МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ МОДЕРНІЗАЦІЇ ЗМІСТУ ОСВІТИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VIII науково-практична конференція

Збірник матеріалів
(Київ, 24 травня 2017 року)

Електронна версія

Київ
2017

УДК 341.123(045)(0.034.2PDF)
А43

Організаційний комітет конференції:

Кудінов С.С. – голова організаційного комітету конференції, ректор Національної академії СБ України, кандидат юридичних наук, доцент;

Пилипчук В.Г. – заступник голови, директор Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки і техніки України;

Ткаченко В.В. – заступник голови, в.о. директора Інституту модернізації змісту освіти Міністерства освіти і науки України, доктор історичних наук, професор;

Фармагей О.І. – проректор з наукової роботи Національної академії Служби безпеки України, доктор психологічних наук, старший науковий співробітник;

Чорний Р.Л. – директор Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук, старший науковий співробітник;

Мамченко С.М. – директор Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України, доктор педагогічних наук, професор;

Муратов О.Є. – заступник директора центру – начальник організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат технічних наук, старший науковий співробітник;

Кащук В.І. – заступник завідувача кафедри Навчально-наукового інституту інформаційної безпеки Національної академії Служби безпеки України;

Давидова Т.О. – старший науковий консультант організаційно-наукового відділу Науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук.

Збірник матеріалів розглянуто та схвалено Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України (протокол № 4 від 22 червня 2017 року).

А43 **Актуальні** проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., (Київ, 24 трав. 2017 р.). – Електрон. дані. – Київ : Нац. акад. СБУ, 2017. – 348 с.

У збірнику висвітлюються актуальні проблеми забезпечення інформаційної безпеки України та науково-практичні підходи до їх вирішення. Розглядаються питання захисту інформаційного простору України, формування системи забезпечення кібернетичної безпеки України, удосконалення вітчизняного законодавства у сфері охорони державної та службової інформації, форми й напрями міжнародної взаємодії у сфері забезпечення інформаційної безпеки, шляхи оновлення змісту вищої освіти фахівців з інформаційної безпеки держави.

Для працівників органів державної влади, науковців, викладачів, фахівців з інформаційної безпеки, широкої громадськості.

Тези доповідей публікуються в авторській редакції. Організаційний комітет залишає за собою право не поділяти думку авторів.

© Національна академія Служби безпеки України, 2017

ВСТУПНЕ СЛОВО

За усталеною традицією Національна академія Служби безпеки України проводить вже VIII щорічну науково-практичну конференцію **«Актуальні проблеми управління інформаційною безпекою держави»** з метою широкого обговорення та вироблення пропозицій щодо вирішення вкрай важливих для нашої держави в умовах зовнішньої інформаційної агресії проблем: захисту інформаційного простору, формування системи кібернетичної безпеки, удосконалення вітчизняного законодавства, міжнародної взаємодії та системи підготовки фахівців з інформаційної безпеки.

Уже більше трьох років триває агресія Російської Федерації проти України, а частина нашої території залишається тимчасово окупованою. Ця гібридна війна поєднує військові, інформаційні, терористичні та інші дії, скоординовані єдиним центром і спрямовані на досягнення визначеної стратегічної мети, якою є втрата нашою державою суверенітету, територіальної цілісності та незалежності.

За цей період Україна зробила певні кроки у напрямку розвитку національного інформаційного простору та захисту свого інформаційного суверенітету, зокрема були реалізовані окремі положення вироблені учасниками конференції у минулому році: створено низку організаційних структур, спрямованих на вирішення завдань з інформаційної безпеки, продовжує удосконалюватися нормативно-правове забезпечення національної безпеки в інформаційній сфері, а також відновлюється система підготовки фахівців з інформаційної безпеки.

Так, Указом Президента України від 15 березня 2016 року №96/2016 затверджена Стратегія кібербезпеки України, яка стала підґрунтям для розбудови національної системи кібербезпеки.

У цьому році Указом Президента України № 47/2017 затверджена нова Доктрина інформаційної безпеки України, яка визначає напрями і пріоритети державної політики в інформаційній сфері, зокрема, повноваження сил безпеки та оборони, покликаних протидіяти зовнішньому агресору.

Разом з тим, потребують вирішення питання тактичного рівня – шляхи реалізації визначених у доктринальних документах стратегічних завдань.

У зв’язку з цим, запрошуємо науковців вищих навчальних закладів, наукових установ і практичних підрозділів, а особливо молодих учених, об’єднати зусилля та використати спільний науковий потенціал у напрацюванні пропозицій щодо вирішення питань розвитку інформаційного суспільства, удосконалення вітчизняної інформаційної інфраструктури, захисту від агресивного інформацій-

ного впливу з боку Російської Федерації.

Існування зазначених вище завдань вказує на важливість підготовки фахівців з інформаційної безпеки. Як відомо, у 2015 році „Інформаційна безпека” не увійшла до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Завдяки зусиллям безпекових відомств, зокрема за участі Служби безпеки України, до цього переліку у листопаді 2016 року включено нову спеціальність 256 “Національна безпека (за окремими сферами забезпечення і видами діяльності)”. Національною академією Служби безпеки України здійснюються сьогодні заходи щодо затвердження в установленому порядку в її рамках окремого виду діяльності – “забезпечення державної безпеки в інформаційній сфері”, що надасть можливість забезпечити сектор безпеки та оборони висококваліфікованими фахівцями зі спеціальною підготовкою. А також Національна академія Служби безпеки України продовжує підготовку здобувачів освіти за трьома спеціальностями: «Менеджмент» (спеціалізація – організація захисту інформації з обмеженим доступом); «Право» (спеціалізація – забезпечення інформаційної безпеки) та «Кібербезпека» (спеціалізація – управління інформаційною безпекою).

Крім цього, наприкінці 2016 року Національною академією Служби безпеки України започатковано курси підвищення кваліфікації співробітників СБ України з питань захисту персональних даних, а також курси зі стратегічних комунікацій, до проведення яких залучались найкращі фахівці-практики, представники провідних наукових установ, вищих навчальних закладів.

Участь у конференції приймають представники Ради національної безпеки і оборони України, Міністерства освіти і науки України, Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної прикордонної служби України, Державної служби спеціального зв’язку та захисту інформації України, Державного агентства з питань електронного урядування України, а також шести провідних наукових установ і двадцяти одного вищого навчального закладу нашої держави, загалом - понад 180 осіб.

Узагальнюючи викладене, наголошуємо, що пропозиції та рекомендації, які формуються спільними зусиллями такого потужного експертного колективу, поступово втілюються у життя. То ж сподіваємося, що активна дискусія та обмін набутим досвідом притаманні конференції сприятимуть подальшому удосконаленню реалізації державної політики в інформаційній сфері та вирішенню проблемних питань забезпечення інформаційної безпеки України.

Організаційний комітет

ДЕРЖАВНО-ПРАВОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

УДК 340:007

Авдошин І.В.
доктор юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ВІДНОСИН В УКРАЇНІ

В Україні інформаційне поле формується під могутнім впливом закордонних чинників. Поряд з безумовністю вимог відкритості інформаційного простору України для інформаційних потоків з-за кордону зрозуміло, що втрата важелів впливу на процеси у ньому призвела та може ще більше призвести до значних негативних наслідків для майбутнього країни. Саме тому надзвичайної актуальності набувають проблеми регулювання інформаційної сфери, створення відповідних умов для випереджаючого розвитку вітчизняного інформаційного виробництва. Провідним інструментом реалізації національних інтересів у такому чутливому середовищі суспільних відносин, як інформаційна сфера, безумовно залишається право.

Аналіз відповідних статей Конституції України та інших законодавчих актів у сфері інформаційних відносин дозволяє дійти висновку про намагання вітчизняного законодавця побудувати інформаційну політику на основі демократичних та ліберальних норм і принципів, одночасно забезпечити їхню адаптацію до українських умов. При цьому експертиза українського інформаційного законодавства, котра неодноразово здійснювалася протягом останніх десятиліть, у тому числі представниками ОБСЄ, свідчить про те, що законодавча та нормативно-правова база функціонування інформаційної сфери України в цілому відповідає європейським нормам.

Проте якщо формальний бік справи не викликає значного занепокоєння, то існує нагальна проблема недотримання встановлених норм усіма суб’єктами інформаційних відносин, зокрема органами державної влади всіх рівнів. До того ж рівень правової культури громадян України змушує розглядати ситуацію із зовсім іншого боку порівняно з країнами ЄС.

Тобто, недостатньо ретельне та чітке дотримання законодавства

складає найважливішу проблему правової політики держави, у тому числі це стосується й інформаційної сфери. Показовим, протягом усього періоду існування незалежної України, є намагання певних сил створити новітні зони недоторканості, сформувати потужні системи пільг та переваг, що діють поза законодавством. Забезпечення єдності та невідворотності дії Закону є провідним завданням держави.

Важливою проблемою залишається певна несистемність вітчизняної правової політики в інформаційній сфері. Значна кількість законодавчих актів ухвалюється з метою вирішення певних тактичних завдань, задоволення кланових інтересів, часто без урахування стратегічних орієнтирів та реальних українських умов. Показовим з цієї точки зору є неодноразові спроби перегляду законодавства щодо дозволу рекламування алкоголю і тютюну.

Значним недоліком чинного законодавства, зокрема в інформаційній сфері, є його неконкретність, певна розмитість формулювань. Фактично відсутні визначення конкретних механізмів оприлюднення інформації, конкретних документів, що мають публікуватися. Не встановлюються терміни цієї діяльності, майже відсутні норми прямої дії щодо фінансового та кадрового забезпечення. Левова частка інформаційних відносин регулюється підзаконними, а подекуди й відомчими нормативними актами. Характерним прикладом останнього є відсутність законодавчого визначення режимів доступу до інформації, окрім державної таємниці. Незважаючи на те, що в законодавстві існують поняття комерційної, лікарської, банківської таємниці, інформації «не для друку» тощо, їхнє чітке визначення відсутнє. Режим доступу до інформації, що належить державі, чомусь встановлюється постановами Кабінету Міністрів України.

В Україні сформовано певну законодавчу базу забезпечення відкритості функціонування органів державної влади. Насамперед йдеться про Конституцію України, закони України «Про інформацію», «Про доступ до публічної інформації», «Про пресу (друковані ЗМІ)», «Про державну службу» тощо. Однак чинна нормативно-правова база не встановлює відповідальності за порушення норм, зокрема затягування термінів відповіді на інформаційний запит. Зазначене певним чином девальвує конституційні норми щодо відкритості.

Вітчизняне законодавство «не встигає» за розвитком сучасних інформаційних технологій та їх нормативного забезпечення. Значну проблему становить фактична відсутність правового регулювання функціонування в Україні міжнародних інформаційних систем. Зокрема відсутність відповідних нормативно-правових актів створює певні проблеми для Інтернет-ЗМІ та сприяє їхньому використанню у деструктивних цілях.

Досить суперечлива ситуація склалася у нормативно-правовому забезпеченні діяльності ЗМІ. Поряд з тим, що за роки незалежності створено розгалужену нормативну базу, влада, дозволивши роздержавлення і приватизацію ЗМІ, «умила руки», зняла з себе відповідальність за розвиток україноцінніснихЗМІ. За переважної наявності неукраїнського бізнесу в економіці й інфраструктурі та без підтримки держави українські ЗМІ не зможуть активно формувати і захищати український інформаційний простір.

Значні проблеми зберігаються і в правовому регулюванні питань інформаційної безпеки. Майже відсутнє законодавче забезпечення формування національних інформаційних ресурсів та міжнародних інформаційних обмінів.

Зрештою, роблячи загальний висновок, можемо поки констатувати що сучасний інформаційний простір України ані за формою, ані за змістовним наповненням не є сприятливим у боротьбі за незалежність з російським окупаційним режимом. Тому хронічне не вирішення чи бездумне «вирішення» окреслених проблем правового регулювання інформаційної сфери унеможливлює створення функціональної системи здатної ефективно протидіяти російській інформаційній агресії як визначальної складової «гібридної війни» проти України.

УДК 004.056.53

Архипов О.Є.
доктор технічних наук, професор
Національний технічний університет України
«КПІ імені Ігоря Сікорського»
Бровко В.Д.
кандидат технічних наук
Національна академія Служби безпеки України

КІБЕРБЕЗПЕКА – ВИНИКНЕННЯ, ФОРМУВАННЯ, РОЗУМІННЯ

Введена в дію указом Президента України П.О. Порошенка в січні 2016 року стратегія кібербезпеки України являє собою базовий документ, що дозволяє почати узгоджену роботу зі створення системи кібербезпеки в Україні. Проте успішному виконанню цієї роботи явно не сприятиме відсутність єдиної термінології у цій сфері, невизначеність ряду понять, які згадуються в стратегії кібербезпеки, зокрема таких базових понять, як кіберпростір, кібербезпека, кібернетична загроза і т.п. На поточний момент у сфері кібербезпеки стрімко зростає кількість публікацій з термінологічної тематики, що

цілком зрозуміло, зважаючи на актуальність цієї проблеми. Автори пропонують різні підходи до її дослідження, причому аналіз змісту публікацій свідчить про іноді абсолютно суперечливе розуміння фахівцями основних термінологічних питань. В цій ситуації для успішного формування загальних уявлень про зміст та базові визначення у сфері кібербезпеки видається доцільним переглянути певні історичні події та факти, пов'язані з процесами виникнення і розвинення інформаційного та кіберпротиборства.

На початку 90-х років минулого століття військово-політичне керівництво США за підсумками оцінки результатів війни в районі Перської затоки прийняло рішення про доповнення традиційної програми захисту інформації у збройних силах США заходами з проникнення в системи державного і військового управління потенційних супротивників і економічних конкурентів. Першим з них стала директива міністра оборони США TS.3600.1, прийнята в 1992 році [7], у якій дано поняття інформаційної війни, поставлені завдання перед міністерством оборони і комітетом начальників штабів (КНШ), визначені питання розвитку форм і способів ведення інформаційної війни. Наступного року з'явилася директива КНШ МОР N 30-93, головний зміст якої склала нова концепція, що отримала назву «боротьби з системами бойового управління» і фактично виділила боротьбу з системами управління в самостійний вид оперативного забезпечення бойової діяльності військ. Теорія боротьби з системами управління отримала свій подальший розвиток у документах КНШ ЗС США «Спільні дії різнорідних сил по боротьбі з системами управління супротивника» та «Єдина перспектива-2020», які визначили основні напрямки розвитку оперативно-стратегічних концепцій застосування збройних сил в XXI столітті, наголосивши, що головною рисою збройної боротьби в наступному столітті буде перенесення акценту в сферу інформаційного протиборства (ІП). Практична реалізація концепції ІП здійснюється шляхом знищення пунктів управління і систем зв'язку з метою позбавлення противника інформації, виведення з ладу або знищення його систем управління при одночасному захисті своїх від аналогічних дій.

В подальшому, в період з 1995 по 2003 рік, корпорацією RAND Corporation на замовлення міністерства оборони США виконано ряд дослідницьких робіт, у звітах про які було визначено роль і місце ІП в збройній боротьбі. Так, у звіті MR-661-OSD (Strategic Information Warfare. A new face of War. 1996) вперше з'являється термін «стратегічне інформаційне протиборство», зміст якого полягає у використанні державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій і змен-

шення сторонніх впливів на власний інформаційний ресурс». У 1998 році в звітах MR-963-OSD (The Day After ... in the American Strategic Infrastructure) і MR-964-OSD (Strategic Information Warfare Rising) відображається тогочасне розуміння стратегії ведення ІП. Стає очевидним виокремлення у ІП кількох тенденцій, зокрема так званого ІП другого покоління, у якому передбачається професійне використання інформації з метою здійснення впливу на емоції, мотиви, поведінку іноземних урядів, організацій і окремих громадян. Вважається цілком можливим досягнення в майбутньому глобальної переваги шляхом інформаційної боротьби в психологічній сфері, без збройного втручання.

Порівняно з цим ІП першого покоління вважається більше орієнтованим на комплексні дії, пов’язані із знищенням або дезорганізацію критичних елементів національної інфраструктури, реалізацію акцій із забезпечення військових операцій, що проводяться традиційними силами і засобами. Саме цей вид ІП, значно розширивши межи свого застосування поза мілітарної сфери, сприяв формуванню нового перспективного напряму, який згодом отримав назву боротьби у кіберпросторі.

Ретроспектива процесу зародження, формування та розвитку кіберпротиборства, дозволяє стверджувати, що боротьба в кіберпросторі - це складова ІП, зміст якої - знищення або дезорганізація діяльності систем управління і зв'язку супротивника (**кіберсистем**), та, відповідно, залежних від них ключових елементів національної інфраструктури.

Киберсистема – це сукупність елементів, що реалізують набір інформаційних технологій, вона є окремим видом більш загального родового поняття - інформаційної системи.

Захисту в кіберсистемі підлягає специфічний вид інформації - управлінська інформація, яка забезпечує вирішення управлінських завдань у різних сферах діяльності. Незахищеність цієї інформації може спричинити погіршення якості управління аж до настання катастрофічних наслідків як для об'єкта управління, так і для його оточення, зокрема персоналу і населення.

Згідно із стандартом ISO/IEC 27032:2012, **кібербезпека, безпека кіберпростору** (cybersecurity, cyberspace security) - збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить в кіберсистему, накопичується та зберігається в ній для подальшої обробки) з метою забезпечення стійкості і безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління. Відповідно, **кіберпростір** - частина інформаційного простору, утворена інформаційними потоками і інформаційними полями, що породжуються в процесі функціонування кібернетичних систем.

Баранов О.А.
доктор юридичних наук
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

НОВА ПАРАДИГМА БЕЗПЕКИ В УМОВАХ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Феномен Інтернету речей (скорочено - IP або Internet of Things - англ., скорочено - IoT), який отримав таку назву понад 15 років тому, потужно увійшов в життя сучасного суспільства, демонструючи вражаючі результати в усе нових і нових сферах людської діяльності. В передових країнах світу активно йде впровадження технологій Інтернету речей. За даними багатьох експертів: до 2025 року 100 мільярдів пристроїв будуть підключені до мережі Інтернет, а ринок IP буде складати $ 7-19 трильйонів. У 2016 році Китай прийняв п'ятирічну Державну програму з загальним фінансуванням $ 127,5 млрд. Німеччина у 2016 році, як і багато розвинених країн, стала виконувати програму «Індустрія 4.0» –багаторічну стратегічну ініціативу для створення всеосяжного бачення і плану дій щодо IP в промисловому секторі.

Приклади у сфері безпілотних автомобілів безсумнівно свідчать про невідворотність настання ери Інтернету речей: Intel витратить 15,3 мільярда $ на покупку Mobileye (виробника компонентів для безпілотних авто); Qualcomm придбала за 47 млрд. $ NXP, найбільшого постачальника автомобільних чіпів; Google, Uber, Ford, Tesla, Nvidia мають власні програми щодо створення власних безпілотних автомобілів.

На основі проведеного аналізу наукових юридичних і технічних джерел, виявлених характерних властивостей IP та результатів роботи [1] запропонуємо наступну дефініцію терміну: «Інтернет речей» – це с сукупність технологій, що поєднують методи, способи і процеси, а також взаємодіючих технічних систем і комплексів, які складаються з мікропроцесорів, сенсорів, виконавчих пристроїв, систем передачі даних, локальних та/або розподілених обчислювальних ресурсів і програмних засобів, призначених для реалізації суспільних відносин, в тому числі, пов'язаних з наданням послуг або проведенням робіт, на основі використання безлічі різноманітних даних і мережі Інтернет при безпосередній участі або без участі суб'єктів цих відносин (юридичних або фізичних осіб).

За 20-25 років стан речей з технологіями IP буде характеризуватись наступним: поширеністю – IP буде пронизувати всі сфери людської діяльності; інтелектуальністю – практично всі комплекси IP будуть функціонувати на базі штучного інтелекту; самоорганіза-

цією, динамічністю і гетерогенністю – різнорідні комплекси ІР будуть самостійно об'єднуватись з іншими комплексами ІР; великими даними – буде мати місце колосальна концентрація різноманітних даних; стрімким розвитком мережі Інтернет – відбудеться колосальне зростання трафіку цифрових даних.

Таким чином, з огляду на те, що комплексі та системи ІР будуть безперервно забезпечувати людську діяльність у будь-який сфері, базуючись на використанні комп'ютерних систем та мережі Інтернет, зокрема, із використання радіотехнологій, можна дійти висновку, що об'єкти з комплексами і системами ІР за визначенням це об'єкти критичної інфраструктури для будь-якої діяльності за участю людини або без її участі.

Розвитку та впровадженню технологій ІР на сучасному етапі притаманні такі основні зони ризиків та бар'єрів: техніко-технологічні; безпеки; конфіденційності; сумісності; стандартизації; правового регулювання.

Це обумовлюється низкою певних факторів. Наприклад, для техніко-технологічної сфери буде характерним дотримання наступного принципу, що забезпечить розвиток: всі технології, які дозволяють надати послугу або здійснити роботи комфортніше, дешевше, швидше, якісніше, безпечніше будуть імплементовані в технології ІР. Зазначене призведе до того, що сфера ІР буде характеризуватись наступним: архітектура ІР – багатозв'язна, багатовимірна, складна, адаптивна, багатофункціональна; ідентифікація – всі складові елементи комплексів та систем ІР, об'єкти, якім надаються послуги або для яких виконуються роботи мають бути ідентифіковані; безшовною роботою технологій передачі даних; максимальною ефективністю користування радіочастотним ресурсом; економним енергоспоживанням і збільшенням часу автономності; транскордонним характером взаємодії; підвищеними вимогами до надійності і стійкості.

Основний принцип для забезпечення в майбутньому безпеки технологій ІР – це забезпечення надійності, стійкості і якості здійснення тієї чи іншої діяльності, що базуються на використанні цих технологій. В умовах широкого використання комплексів та систем ІР потрібно визначати та одночасно забезпечувати наступне: інфраструктурну безпека (надійність, стійкість, резервування); технологічну безпеку; кібернетичну безпеку; багаторівневу систему безпеки; безперервність всіх складових безпеки; інтеграція і взаємодію різноманітних систем безпеки, створення спеціального менеджменту безпеки.

Література

1. Баранов О. «Інтернет речей» як правовий термін // Юридична Україна. 2016. №5-6. С. 96-103.

Благодарний А.М.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія Служби безпеки України

ПРОБЛЕМИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ЮРИСДИКЦІЙНОЇ ДІЯЛЬНОСТІ ОРГАНІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ НА СТАДІЇ ПОРУШЕННЯ СПРАВ ПРО АДМІНІСТРАТИВНІ ПРОСТУПКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З огляду на розбудову в Україні правової держави та громадянського суспільства актуалізуються питання нормативного регулювання адміністративно-юрисдикційної діяльності органів державної влади, зокрема діяльності посадових осіб органів СБ України.

Стосовно участі органів СБ України в юрисдикційних адміністративних провадженнях, слід зазначити, що значну частину діяльності СБ України становлять провадження у справах про адміністративні правопорушення. Так, відповідно до ст. 255 Кодексу України про адміністративні правопорушення (далі - КУпАП), уповноважені посадові особи органів СБ України мають право складати протоколи про такі правопорушення у сфері інформаційної безпеки:

– порушення порядку провадження господарської діяльності (у частині, що стосується правопорушень у галузі господарської діяльності, ліцензії на проведення якої видає СБ України) (ст. 164 КУпАП);

– незаконне зберігання спеціальних технічних засобів негласного отримання інформації (ст. 195-5 КУпАП);

– порушення законодавства про державну таємницю (ст. 212-2 КУпАП);

– порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, що містять службову інформацію (ст. 212-5 КУпАП);

– здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем (ст. 212-6 КУпАП).

Починаючи розгляд проблемних питань провадження в справах про адміністративні правопорушення, слід зазначити, що адміністративно-процесуальне законодавство не має спеціальної норми, в якій в концентрованому вигляді були б відображені приводи та підстави порушення справи про адміністративний проступок. Найчастіше приводами до порушення адміністративної справи є:

– заяви або повідомлення підприємств, установ, організацій, посадових осіб, представників влади, громадськості, громадян (свідків, потерпілих, інших зацікавлених осіб);

– повідомлення, опубліковані в пресі та інших засобах масової інформації;

– безпосереднє виявлення ознак правопорушення уповноваженою особою [1, с. 348]. Досліджуючи такий привід порушення справи про адміністративний проступок, як заяву або повідомлення фізичних або юридичних осіб, слід зазначити, що КУпАП не містить норми, яка б зобов'язувала компетентний орган прийняти заяву чи повідомлення про вчинений адміністративний проступок.

Практика діяльності правоохоронних органів знає випадки, коли повідомлення і заяви не приймалися посадовими особами органів адміністративної юрисдикції [2, с. 93]. Тому вважаємо, що до КУ пАП слід внести зміни, які б закріпили обов'язок уповноваженої особи органу адміністративної юрисдикції або особи, уповноваженої складати протокол про адміністративне правопорушення, прийняти заяву або повідомлення про адміністративне правопорушення.

КУпАП не передбачає терміну, протягом якого після вчинення адміністративного проступку складається протокол про адміністративне правопорушення – основний документ, що фіксує факт порушення адміністративної справи. Такий стан речей, звісно, не узгоджується з короткочасним терміном притягнення до адміністративної відповідальності.

На думку багатьох юристів, протокол повинен бути складений безпосередньо після збору доказів факту вчинення адміністративного правопорушення [2, с. 110]. Зволікання із складанням протоколу можуть призвести до того, що буде важко зібрати докази у справі.

Продовжуючи розгляд питань провадження в справах про адміністративні правопорушення, варто зазначити, що КУпАП недостатньо категорично вимагає від уповноваженої посадової особи складання протоколу у випадку виявлення ознак адміністративного проступку, його положення свідчать скоріше про право, а не про обов'язок уповноваженої посадової особи складати протокол про адміністративне правопорушення.

Враховуючи зазначене, вважаємо, що у КУпАП слід закріпити норму, яка б передбачала саме обов'язок посадової особи складати протокол про адміністративне правопорушення у випадку виявлення ознак адміністративного проступку.

Підсумовуючи викладене, слід зазначити, що правове регулювання адміністративно-юрисдикційної діяльності органів СБ України, зокрема, провадження в справах про адміністративні правопо-

рушення у сфері інформаційної безпеки потребує подальшого вивчення та вдосконалення. Насамперед, вважається за доцільне визначити у чинному законодавстві приводи та підстави порушення справи про адміністративний проступок, а також закріпити у КУ пАП обов'язок уповноважених посадових осіб складати протоколи про адміністративні правопорушення.

Література

1. Колпаков В.К. Адміністративне право України : Підручник. – К.: Юрінком Інтер, 2001. – 752 с.

2. Благодарний А.М. Адміністративна відповідальність за порушення законодавства про державну таємницю: Монографія. – К.: Вид-во НА СБ України, 2008. – 180 с.

УДК 35.078.3

Бондаренко І.Д.

Національна академія Служби безпеки України

НАПРЯМКИ УНІФІКАЦІЇ «КОМП'ЮТЕРНОЇ» ТЕРМІНОЛОГІЇ В СТАТТЯХ РОЗДІЛУ XVI КК УКРАЇНИ

В статтях розділу XVI КК України, якими передбачено відповідальність за так-звані «комп'ютерні» злочини, законодавцем вказано на конкретні типи технічного устаткування (щодо якого або щодо інформації оброблюваній на якому вчиняються злочини), але їх дефініції в тексті кримінального закону відсутні. Тлумачення їх змісту впливатиме на встановлення в конкретному діянні складу злочину та передбачає необхідність здійснення аналізу законодавства в сфері захисту інформації. ЕОМ відповідно до ДСТУ 2938-94 є функціональним пристроєм, що складається з одного або декількох взаємопов'язаних центральних процесорів і периферійних пристроїв і може виконувати розрахунки без участі людини. В статтях розділу XVI КК України слово «комп'ютер» розміщено у дужках після «ЕОМ», що на думку А.С. Білоусова та С.В. Дрьомова свідчить про їх синонімічність. Із достатньо великої кількості наукових визначень поняття «комп'ютер» можна виокремити його характерні ознаки: а) наявність електронного пристрою і програмної складової, що працюють як єдине ціле; б) наявність принаймні одного мікропроцесора, пам'яті, периферійних пристроїв; в) можливість за командою людини та/або програми здійснювати введення, виведення, знищення, копіювання, модифікацію, передачу інформації у системи чи мережі. Таку ознаку як наявність програмного забезпечення у вигляді операційної систе-

ми, яка обумовлює його полі-функціональність завдяки можливості інсталювати нові програми, довгий час називали ключовим ідентифікатором комп'ютера, що відрізняє його від іншої електроніки. Але з огляду на тенденцію до тотального «урозумнення» всієї побутової техніки, вищенаведені ознаки комп'ютера характерні і для «планшетних комп'ютерів», «смартфонів», касових апаратів, банкоматів, платіжних терміналів, телевізорів, тощо. В науці кримінального права питання співвідношення поняття «комп'ютер» з приладами сучасної електроніки є дискусійним. Наприклад, В.А. Мещеряков та М.В. Карчевський аргументували, що будь-яке устаткування з процесором та здатністю здійснювати розрахунки без участі людини є комп'ютером. Протилежну позицію займає А.С. Білоусов. Цілком виправданими є аргументи щодо архаїчності самого поняття «ЕОМ» та необхідності оновлення відповідного термінологічного апарату, перегляду суміжних понять «автоматизована система», «комп'ютерна мережа», «носій (комп'ютерної) інформації», що використані в статтях розділу XVI КК України.

Поняття «автоматизована система (АС)» використовується в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», низці підзаконних актів у значенні організаційно-технічної системи, що об'єднує операційну систему, фізичне середовище, персонал і оброблювану інформацію та за сукупністю характеристик диференціюється на 3 класи. Паралельне використання в кримінально-правовій нормі зазначеного терміну поряд із терміном «комп'ютер» є абсолютно невиправданим, оскільки «автоматизована система» є поняттям абсолютно іншого типу, позначає не технічний, а організаційно-технічний об'єкт, охоплює крім техніки і персонал та оброблювану інформацію, врешті-решт завжди включає в себе принаймні 1 комп'ютер.

Слід зазначити, що в ДСТУ 2226-93 міститься зовсім інше визначення АС – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність (наприклад, «система керування технологічним процесом автоматизована», «лінія виробнича гнучка»). Зазначений ДСТУ 1994 року наразі є суттєво застарілим, наприклад, лише одним із видів автоматизації в ньому визначено комп'ютеризацію. Втім, наразі саме комп'ютерні системи є основою будь-якого автоматизованого процесу. Отже, в даному значенні АС також включає в себе принаймні один комп'ютер, що підтверджує попередній висновок про невиправданість використання поняття «АС» в

статтях розділу XVI КК України.

Відповідно до ДСТУ 2938-94 комп'ютерна мережа (далі – КМ) – це сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів. КМ є продуктом еволюції телекомунікаційних і обчислювальних систем, їм характерні системоутворюючі ознаки (фактично – низка об'єднаних комп'ютерів), а тому цілком аргументованою видається позиція С.О. Орлова про практичну відсутність між ними чіткої грані та, відповідно, невиправданість використання терміну «КМ» в статтях КК України поряд із терміном «комп'ютер».

Суперечливим є застосування поняття «носій такої інформації», яке з контексту ст. 361-2 КК України слід розуміти як носій комп'ютерної інформації (далі – НІ). За аналогією із «носієм інформації з обмеженим доступом» науковці його тлумачать як устаткування, призначене для накопичення, передачі комп'ютерної інформації. Але таке устаткування у вигляді жорсткого диску є конструктивною складовою будь-якого комп'ютера, тому одночасне використання в кримінально-правовій нормі слів «комп'ютер» та «носій інформації» в низці випадків утворює тавтологію. Останній доречно виокремлювати лише коли ним є самостійний засіб збереження інформації (флеш-носій, тощо) або якщо жорсткий диск був спеціально вилучений з комп'ютера.

Отже, проаналізувавши кримінально-правовий зміст понять «ЕОМ», «комп'ютер», «АС», «КМ», «НІ» слід констатувати наявність суттєвих проблем термінологічної невизначеності, що на практиці може створювати передумови для маніпулювання при визначенні ознак злочину. Крім того, наявність у кримінальному законі чіткого переліку комп'ютерних засобів не лише перевантажує норми розділу XVI КК України, але і, фактично, обмежує їх застосування для протидії комп'ютерним злочинам, які можуть бути вчинені із використанням новітніх, не перелічених у диспозиції статті, видів комп'ютерного обладнання. Вирішення даної проблеми можливе шляхом заміни аналізованих термінів універсальним, «комп'ютерна система», який використано в Конвенції Ради Європи «Про кіберзлочинність» у значенні пристрою або групи взаємопов'язаних пристроїв (в мережу), один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних.

УДК 343.3/.7

Волошин О.В.
Національна академія Служби безпеки України

ПРЕВЕНТИВНІ АНТИТЕРОРИСТИЧНІ ЗАХОДИ ЯК МЕХАНІЗМ ПРОТИДІЇ ТЕРОРИСТИЧНИМ ЗАГРОЗАМ В ІНФОРМАЦІЙНІЙ СФЕРІ

Тероризм залишається однією з головних загроз безпеці сучасного світу – разом з організованою злочинністю, екстремізмом, релігійними, етнічними та соціальними конфліктами. Доволі важливо приймати до уваги можливості (пропаганда, радикалізація екстремістів та вербування до терористичних мереж), які відкриті терористам завдяки сучасним інформаційним та комунікаційним технологіям. Терористичні атаки, що відбуваються безпосередньо в кіберпросторі, більш не є футуристичною уявою, а стали реальністю. Вони створюють пряму загрозу як життю та здоров'ю людей, так і інформаційній безпеці.

Терористичні групи взяли на озброєння використання мас-медіа як один з найбільш ефективних підходів для залякування громадян для того, щоб примусити їх виконувати терористичні вимоги. Це може включати використання телебачення, радіо, Інтернету або друкованих видань, таких як книги, газети, журнали та інші періодичні видання. Мас-медіа можуть бути визначені як будь-яка форма комунікації, оскільки вона охоплює широкі та неоднорідні аудиторії [1].

Нова модель тероризму частковою мірою є результатом стрімкого розвитку інформаційних технологій. Особливо яскраво це проявляється в тому, що терористичні групи усвідомили вплив засобів масової інформації (ЗМІ) на виконання своїх цілей. Також терористи використовують Інтернет для поширення терористичної пропаганди, навчальних матеріалів, підготовки своїх членів, уточнення інформації щодо протидіючих сторін (правоохоронних органів) з метою використання її для власних потреб.

Попередження тероризму в європейських країнах – це проблемне питання, яке постійно перебуває в розвитку, оскільки влада не тільки використовує засоби профілактики злочинності, але й також удосконалює свої власні унікальні інструменти, особливо в сфері міжмуніципального діалогу. В цілому, керівні принципи політики у сфері запобігання тероризму для місцевої влади взяті з Конвенції Ради Європи про запобігання тероризму від 16 травня 2005 року, яка базується на двох основних напрямках [2]. По-перше, вона підкреслює необхідність підготовки (тренування) репресивних служб (поліції), а по-друге в ній акцентується увага на розвитку превентивної політики, яка впливає на

освіту, культуру, публічну інформацію, ЗМІ та громадську свідомість.

Превентивні антитерористичні заходи охоплюють значну кількість елементів таких як інформація, інфільтрація, соціальний і міжмуніципальний діалог. Зосереджуючись на середньостроковій і довгостроковій перспективі, ці механізми намагаються знайти витоки тероризму, виявити причини, які змушують людей здійснювати теракти, навіть знаючи, що вони загинуть. У цьому контексті, якщо стримування, як це реалізовано в правовій системі, продовжує бути важливою частиною боротьби з тероризмом, воно повинно бути доповнене превентивною політикою, спрямованою, з одного боку, на скорочення можливостей для організації терористичної діяльності (ситуаційна профілактика), а з іншого боку, на викорінення всіх мотивацій для осіб, які намагаються взяти участь у цих заходах (соціальна профілактика). Ідея вдосконалення превентивних заходів у рамках боротьби з тероризмом не заперечується будь-яким урядом.

Протягом 2016 року Рада Європейського Союзу реалізувала ряд антитерористичних заходів, необхідних для запобігання насильницької радикалізації і підвищення спроможності європейських спільнот відмовитися від усіх форм екстремізму. Офіційне й неформальне навчання, молодіжний рух відіграють важливу роль у цьому напрямку. Неабияке місце у протидії радикалізації посідають вчителі, соціальні працівники, місцева влада, жінки, молодь, представники спорту, релігійні лідери й обмін передовим досвідом між ними триває.

У березні 2017 році була прийнята Директива Європейського парламенту та Ради Європи про боротьбу з тероризмом, заміну рамкового рішення Ради 2002/475/JHA та внесення змін до рішення Ради 2005/671/JHA [3]. У статті 21 Директиви йдеться про те, що держави-члени повинні вживати необхідних заходів для забезпечення швидкого видалення онлайн-контенту, що містить публічні підбурювання до вчинення терористичного злочину, розміщеного на їх території. Вони також прагнутимуть локалізації такого вмісту, розміщеного за межами їх території. Коли його видалення не передбачається можливим – вживати заходів для блокування доступу до нього інтернет-користувачами у межах своєї території.

Отже, подальше поширення терористичних загроз може бути обмежене за допомогою системи ефективних превентивних антитерористичних заходів, спрямованих на розвиток готовності суспільства щодо протидії терористичним ризикам, захист свідомості людей від терористичної ідеології, залучення місцевого населення до комунікації в якості інструменту для боротьби з тероризмом.

Література

1. Terrorism and mass media essay. RL: https://www.ukessays.com/

ssays/media/terrorism-and-mass-media-media-essay.php.
2. Council of Europe Convention on the Prevention of Terrorism. URL: http://www.statewatch.org/news/2005/may/coe-conv-terrorism.pdf.
3. Directive of the European Parliament and of the Council on Combating Terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. URL: https://db.eurocrim.org/db/en/doc/2704.pdf.

УДК 378.016:004.056.5

Воскобойніков С. О.
кандидат педагогічних наук
Національна академія СБ України
Кащук В.І.
Національна академія СБ України

МОДЕРНІЗАЦІЯ ПРОЦЕСУ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ КІБЕРНЕТИЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Необхідність кадрового забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки є актуальною науково-практичною проблемою сучасності, зумовленою глибокими системними перетвореннями в інформаційному суспільстві сучасного світу та викликів інформаційної безпеки та кібербезпеки в умовах прискореного розвитку інформаційного, комунікаційного і кіберпростору, загроз антропогенного і техногенного характеру.

Потреба у вирішенні цієї проблеми визначена у аналітичній доповіді Національного інституту стратегічних досліджень при Президенті України «Кібербезпека: світові тенденції та виклики для України» (Д. Дубов, 2011р.). Зокрема увага фокусується на незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки. Формування професійних компетентностей, визначених діючими Галузевими стандартами вищої освіти у галузі знань 1701 – Інформаційна безпека, відповідно до освітньо-кваліфікаційної характеристики (ОКХ) та освітньо-професійної програми (ОПП) охоплює весь спектр професійної діяльності фахівців захисту інформації і водночас не конкретизує компетенцій застосування методів і засобів забезпечення кібернетичної безпеки. Тому професійна підготовка майбутніх фахівців кібернетичної безпеки у вищих навчальних закладах України потребує модернізації відповідно до найновіших досягнень світового рівня розвитку кібербезпеки й викликів кібернетичного простору.

Спеціальні наукові знання, технічні навички і здатність використовувати технології у галузі кібернетичної безпеки, для захисту інтересів громадян і національних інтересів в інформаційному і кіберпросторі від ризиків стороннього кібернетичного впливу є складовими професійної компетентності майбутніх фахівців кібербезпеки. В свою чергу це пов'язано з тим, що об'єктами їх професійної діяльності в умовах реальних кіберзагроз є: об'єкти інформатизації (комп'ютерні, автоматизовані, телекомунікаційні, інформаційні й інформаційно-аналітичні системи), інформаційні ресурси й інформаційні технології; технології забезпечення кібербезпеки об'єктів різного рівня (система, об'єкт системи, компонент об'єкта); процеси управління інформаційною і кібербезпекою об'єктів, що у певній мірі є інтегрованими.

На думку сучасних науковців (В. Богуша, В. Бурячка, В. Толубка, С. Толюпи) ефективним є введення у процес професійної підготовки майбутніх фахівців кібербезпеки спеціальних навчальних дисциплін: «Кібернетичний простір»; «Інформаційні технології та системи кібернетичного простору»; «Технологія організації збору та добування інформації у кіберпросторі, її обробки, аналізу і синтезу»; «Основи автоматизації процесів інформаційної діяльності у кібернетичному просторі» та ін., що надають підґрунтя для формування готовності до реалізації компетенцій: соціально-особистісних, інструментальних, загальнонаукових та професійних, а також виробничих функцій – дослідницьких, проектувальних, організаційних, управлінських, технологічних, контрольних, прогностичних, технічних та ін., пов'язаних із забезпеченням кібербезпеки особистості, підприємства та держави у цілому.

Вивчення теоретичних основ кібернетичної безпеки, правових та організаційних засад протидії кіберзлочинності, методів та засобів протидії кіберзлочинності, програмного забезпечення систем кібернетичної безпеки, криптографічних механізмів кібернетичної безпеки, кібернетичної безпеки підприємств та кібернетичної безпеки держави є обов'язковими компонентами модернізації структури і змісту професійної підготовки майбутніх фахівців кібербезпеки у вищих навчальних закладах України.

Професійна здатність аналізу потенційних загроз і ризиків кібербезпеки, здатність виявляти ознаки стороннього кібернетичного впливу, моделювати можливі ситуації такого впливу, прогнозувати їх можливі наслідки; реалізувати комплекс заходів кібербезпеки, обґрунтовувати правові, адміністративно-управлінські й технічні рішення для запобігання й протидії кіберзагроз, зовнішніх впливів, протидіяти несанкціонованому впливу на об'єкти економічної та інформаційної діяльності для забезпечення кібербезпеки на національному рівні, а також відновлення їх функціонування після здійснення кібератак; програмної реалізації алго-

ритмів рішення завдань забезпечення кібербезпеки, застосування програмних засобів системного, прикладного й спеціального призначення; здійснювати аналіз інформаційної безпеки об'єктів і систем з використанням вітчизняних і закордонних стандартів; формувати комплекс заходів для управління кібербезпекою – є основою формування і розвитку професійної компетентності майбутніх фахівців кібербезпеки.

УДК 343.346

Гавловський В.Д.
кандидат юридичних наук,
старший науковий співробітник
Міжвідомчий науково-дослідний центр
з проблем боротьби з організованою
злочинністю при РНБО України

ДО ПИТАННЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ДЕСТРУКТИВНИХ ЦІЛЯХ

На сьогодні швидкими темпами зростає кількість користувачів соціальних мереж. Лише соціальна мережа «Facebook» налічує більше 1,94 млрд користувачів у світі. UA-сегмент соціальної мережі «Facebook» налічував близько 7,2 млн. Це третій показник в Україні. На другому місці за кількістю користувачів – російська соціальна мережа «Однокласники», щомісячна українська аудиторія якої становить 9,5 млн чоловік. Лідером є соціальна мережа «Вконтакте», яка встановила в лютому поточного року новий рекорд в Україні – 16 мільйонів унікальних відвідувачів на добу.

Аналізуючи нові загрози та виклики для користувачів соціальних мереж, необхідно констатувати, що соціальні мережі вже тривалий час активно використовуються злочинцями. Масштаби кримінальних проявів у соціальних мережах Інтернет складно оцінити. Об'єктивному аналізу досліджуваного виду злочинності не сприяє як недосконалість статистичної звітності правоохоронних органів, так і труднощі у виявленні, розкритті та розслідуванні злочинів, скоєних із використанням високих інформаційних технологій.

Науковцями Центру проведено кримінологічний аналіз злочинів, учинених із використанням соціальних мереж у 2016 році, у фабулах кримінальних правопорушень яких був присутнім контент, пов'язаний із соціальними мережами (перелік цих кримінальних правопорушень (667 документів) надано Національною поліцією України).

Так, соціальна мережа «Твіттер» була використана для вчинення кримінального правопорушення один раз, «Однокласники» –

3 рази, «Facebook» – 48 разів. Решта кримінальних правопорушень були вчинені з використання соціальної мережі «ВКонтакте».

За результатами опрацювання наданих документів встановлено, що з використанням соціальних мереж вчинено кожне четверте шахрайство та кожне десяте кримінальне правопорушення, передбачене ч.ч. 3,4,5 ст. 301 КК України.

Соціальна мережа «ВКонтакте» також найчастіше використовується спільнотами антиукраїнського змісту. За запитом "Антимайдан" «ВКонтакте» знаходить 2,5 тисячі відповідних груп. У антимайданівській групі близько півмільйона учасників, з яких 163 тисячі зареєстровані в Україні [1].

Нещодавно співробітники Служби безпеки України затримали в різних регіонах країни п'ятьох власників та адміністраторів антиукраїнських угруповань в соціальних мережах. Правопорушники за завданням своїх кураторів із російських спецслужб поширювали напередодні травневих свят заклики до радикалізації суспільних акцій з нагоди 1, 2, 8 і 9 травня, а також намагалися використовувати соціальні мережі для ініціювання масових заворушень [2].

Метою захисту інформаційного простору України від російської пропаганди, на думку окремих політиків, має стати блокування російських соціальних мереж "ВКонтакте", "Одноклассники", які сьогодні повністю керуються російськими спецслужбами. Але власники соціальних мереж знаходяться за кордоном, і на них не поширюється українське законодавство. До того ж це не так просто зробити технічно. Наприклад, в Італії сайт «ВКонтакте» заблокований за піратство, але в мережі нескладно знайти інструкції як мінімум з десятком способів зайти в соціальну мережу з території цієї країни.

Більш виваженою в цьому питання є пропозиція не блокувати соціальні мережі, а визначити спосіб, щоб за законодавством України можливо було б блокувати певний контент, а не саму соціальну мережу [1].

Слід вказати на кардинально різні позиції законодавців щодо правового регулювання, впровадження та розвитку Інтернет–технологій. Так, у США управління Інтернет-простором та контроль за його діяльністю здійснюється завдяки об’єднанню зусиль як уряду, приватного сектору, так і громадянського суспільства. У КНР основним суб’єктом, який здійснює «управління мережею Інтернет», є уряд. У Великобританії вирішення цього питання відводиться громадянському суспільству [3].

Також заслуговує на увагу законопроект, підготовлений Мінюстом Німеччини, який спрямований на боротьбу зі злочинністю на ґрунті ворожнечі й ненависті на таких платформах, як Facebook.

Цим законопроектом передбачається прискорення реагування на скарги користувачів, накладення штрафів як на конкретну особу, так і на всю компанію. Крім того, соціальні мережі, в разі прийняття законопроекту, повинні будуть призначити відповідальну контактну особу в Німеччині, яка буде представляти інтереси компаній і відповідатиме за обробку скарг користувачів [4].

Література

1. ВК і ОК на замок: навіщо українців "рятують" від соцмереж. URL: https://apostrophe.ua/ua/article/society /media/2017-02-22/vk-i-ok-na-zamok-zachem-ukraintsev-spasayut-ot-sotssetey/10361

2. Пятерых пророссийских интернет-пропагандистов задержала. URL: http://hronika.info/videonovosti/226582-pyateryh-prorossiyskih-internet-propagandistov-zaderzhala-sbu-video.html

3. Використання соціальних мереж у виявленні та розслідуванні злочинів: зарубіжний досвід та перспективні напрямки. URL: http://molodyvcheny.in.ua/files/journal/2016/8/21.pdf

4. В Германии хотят усилить давление на социальные сети. URL: http://news.eizvestia.com/news_society/full/

УДК 351.74+004

Гордієнко С.Б.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
Богуш В.М.
кандидат технічних наук, доцент,
Національна академія Служби безпеки України
Настрадін В.П.
кандидат технічних наук, професор,
Національна академія Служби безпеки України

ПРОБЛЕМИ ПІДГОТОВКИ СУСПІЛЬСТВА ДО ВИКЛИКІВ КІБЕРТЕРОРИЗМУ

В останнє десятиліття кібертероризм, загроза кібератак стали достатньо реальними, а їх ризики оцінюються як достатньо високі, реалії їх входження в повсякденну дійсність стали питанням часу та місця. Використання мережевого інструментарію здатне вивести з ладу критичні компоненти національної інфраструктури (енергетичні потужності держави, зв’язок, транспортні, фінансові та інші засоби) і невпинно стає реальною і зростаючою загрозою. Нагальним стає постановка і рішення задач з аналізу і управління ризиками для адекватної оцінки реальності проявів кібертероризму, та підготовки фахівців у цій галузі.

Термінологічно поняття «кібертероризм» означає сукупність дій з дезорганізації інформаційно-комп'ютерних систем (несанкціоноване втручання в комп'ютерні мережі, перепрограмування, порушення роботи серверів та ін.), що становлять небезпеку для людей, призводять до значних майнових та немайнових збитків або інших суспільно небезпечних наслідків, якщо їх здійснено з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішень органами влади, а також загрози здійснення цих дій. Це завжди заздалегідь спланований мотивований напад на інформаційні, комп'ютерні системи, комп'ютерні програми та дані. Проте загальноприйнятого визначення цього поняття наразі не існує. Для кібертероризму характерно наступне: по-перше, використання комп'ютера як інструменту дії; по-друге, наявність Інтернету як інформаційного простору, в якому перебуває об'єкт злочину; по-третє, зловмисна атака з боку зловмисників чи їх угрупувань на специфічні об'єкти (інформаційні системи, програми, комп'ютери, локальні та глобальні мережі). В цьому відношенні найважливішим є протидія саме кібертероризму.

Боротьба з тероризмом як напрям діяльності європейської спільноти набула документального оформлення після терактів у США 11 вересня 2001 року. Високий рівень інформаційно-технологічного розвитку країн Євросоюзу пов'язаний з проблемою забезпечення інформаційної безпеки. Спільна позиція країн – членів Європейського Союзу стосовно змісту поняття «інформаційна безпека» висловлена представником Швеції при обговоренні на 56-й сесії Генеральної Асамблеї ООН з питань міжнародної інформаційної безпеки, згідно з якою інформаційна та мережева безпека означає: 1) захист особистої інформації про відправників і одержувачів; 2) унеможливлення несанкціонованої зміни інформації; 3) контроль доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації.

Положення Конвенції Ради Європи «Про кіберзлочинність» знайшли своє відображення в Законах України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23.12.2004 року, у Стратегії національної безпеки України та Стратегії кібербезпеки України, затверджених Указами Президента України відповідно від 26.05.2015 № 287 та 15.03.2016 № 96. Серед визначених основних завдань суб'єктів національної системи кібербезпеки найбільш функціональними, на наш погляд, є завдання Служби безпеки України.

Важливим в усвідомленні сутності кібертероризму, боротьбі з ним є підготовка відповідного кадрового потенціалу, перш за все у вищих навчальних закладах, які готують фахівців галузі знань «інформаційні технології». Аналіз існуючих підходів до побудови процесу підготовки фахівців в сфері захисту інформації перш за все у США, дозволив виділити домінуючі напрямки і сконцентрувати

увагу на розгляді існуючих підходів до процесу навчання. У США найсерйознішу увагу приділяють проблемі підготовки фахівців для захисту національних інформаційних структур. Ще у 1998 році був створений Національний центр захисту інфраструктури (NIPC), який об'єднав представників органів влади, військових і приватного сектору, для захисту національних інфраструктур. Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS), забезпечує навчання в області комп'ютерних технологій. Успішно функціонує Національна спілка кібербезпеки, створена спільно урядом і промисловцями США. Серед навчальних центрів, що спеціалізуються на підготовці фахівців із захисту інформації можна зазначити: CERT, GIAC, CSI, Cisco Systems. Крім комерційних компаній, підготовку фахівців у галузі інформаційної безпеки здійснює ряд державних структур: аспірантура NAVAL, агентство із захисту інформаційних систем (Defense Information Systems Agency, DISA), коледж управління інформаційними ресурсами (Information Resource Management College). Для вдосконалення методів навчання в Міністерстві оборони створено спеціальний підрозділ - «Управління програм з інформаційної безпеки (Information Assurance Program Office)». Агентство національної безпеки (NSA) сформувало ще в 1999 році ряд центрів післядипломної освіти, а в 2000 році підключило до них 14 провідних університетів США. Одночасно Білий дім розпочав навчання урядових чиновників (до 10 тис. чоловік) в рамках федеральної програми забезпечення безпеки інформаційних технологій з бюджетом 25 млн. доларів на рік.

В багатьох містах США почали регулярно проводитися семінари, конференції, симпозіуми з проблем кіберзлочинності та кібертероризму.

Навчання в США концентрується, в основному, на підготовці та перепідготовці фахівців з технічних аспектів захисту інформації. Водночас спостерігається відставання в підготовці юристів з розслідування комп'ютерних злочинів. Одним з напрямків вдосконалення системи підготовки фахівців із захисту інформації в США вбачається у створенні міжнародних консорціумів. США виступили ініціаторами створення мережі міжнародних консорціумів з підготовки кадрів у галузі захисту інформації, з сертифікації фахівців з інформаційної.

З метою налагодження партнерських зв'язків з навчальними закладами Європи, Близького Сходу та Африки співробітники Стенфордського університету в 1984 році створили фірму системи Cisco. Був створений освітній проект «Мережева академія Cisco», здійснюваний спільно освітніми установами та компанією Cisco, світовим лідером в області мережевих Інтернет-рішень. В даний час Cisco є світовим лідером у мережевих технологіях для Інтернет. Вона забезпечує фундаментальну підготовку фахівців з теорії та практиці проектування, будівництва та технічного супроводу локальних і глобальних мереж з використанням зага-

льновизнаних стандартів і рішень в області інформаційної безпеки.

Програма Мережевої академії Cisco розрахована на 280 годин. Навчальні плани розроблені відповідно до освітніх стандартів США за участю кращих фахівців у галузі освіти і мережевих технологій. Навчання проводиться на 9 мовах. Навчальний матеріал оновлюється кожні 90 днів.

Аналіз сайтів провідних університетів США дозволяє зробити ще ряд цікавих висновків. Наявність одного диплома, виданого 10-15 років тому, у США вже недостатньо. Тому 42% всіх студентів приватних і державних вузів США віком більше 25 років.

Враховуючи досвід США та інших країн, які мають значний досвід в боротьбі з кібертероризмом нагальним завданням є розгортання підготовки та перепідготовки фахівців для Служби безпеки України в Національній академії СБ України зі спеціальностей «національна безпека» та «кібербезпека».

Література

1. Еляков А. Компьютерный терроризм. / Мировая экономика и международные отношения. – 2008. – № 10. – С. 102–105.

2. Макаренко Є. А., Рижиков М. М., Ожеван М. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 916 с.

3. Стратегія національної безпеки України / Офіційний вісник Президента України від 03.06.2015 — 2015 р., № 13, стор. 50, стаття 874

4. Стратегія кібербезпеки України / Офіційний вісник Президента України від 05.04.2016 — 2016 р., № 10, стор. 39, ст.198.

УДК 004.056.5

Грищук Р.В.
доктор технічних наук,
старший науковий співробітник
Житомирський військовий інститут
імені С. П. Корольова

ГІБРИДНА ЗАГРОЗА В КІБЕРПРОСТОРІ: ІНФОРМАЦІЙНА ТА КІБЕРНЕТИЧНА СКЛАДОВІ

Актуальність. Досвід України з питань протидії російській агресії наочно продемонстрував зміну характеру загроз безпеці держави у всіх сферах [1]. Зокрема в інформаційній сфері загрози стають гібридними [2]. Гібридний характер загроз як наслідок характерний і загрозам в кіберпросторі.

Суть гібридної загрози в кіберпросторі полягає в різноманітних проявах небезпеки для всіх складових кіберпростору – його фізич-

ного, логічного та соціального рівнів [3]. Відсутність технологій протидії гібридним загрозам зумовлює нагальну потребу у проведенні наукового дослідження, яке спрямоване на уточнення їх ролі та місця в системі безпеки, визначення їх складових, з'ясування сутності та змісту, знаходження дієвих механізмів запобігання проявам таких загроз та ліквідації наслідків тощо.

Аналіз стану питання показав, що протидії гібридним загрозам в кіберпросторі до сьогодні майже не приділялася увага науково-експертного співтовариства. Вперше в науковий обіг поняття гібридної загрози в кіберпросторі було введено відносно недавно – в 2017 р. [4]. Поряд з тим слід зауважити те, що складові гібридної загрози в кіберпросторі були розглянуті та досліджені у більш ранніх публікаціях, зокрема в [2, 3] та в працях ін. вчених. У практичній площині нині на стадії формування знаходиться Європейський Центр передового досвіду протидії гібридним загрозам. Однак наукові та практичні здобутки даного підрозділу на сьогодні невідомі.

Метою доповіді є формалізація концепції гібридної загрози в кіберпросторі та визначення її складових.

Основний зміст дослідження. До сьогодні загрози в кіберпросторі мали суто технічний характер та націлювалися на його фізичний та логічний рівні. Вони проявлялися у вигляді кібератак таких основних типів DOS, R2L, U2R та PROBE [3].

На фізичному рівні кіберзагрози проявлялися у вигляді блокування (обмеження) роботи інформаційних ресурсів, у тому числі й державних, та самих інформаційно-телекомунікаційних систем. На логічному рівні кіберзагрози проявлялися у вигляді кібератак, які призводили, наприклад, до змін схем маршрутизації трафіку, проходження команд управління, змін даних в базах даних тощо.

Головною відмінністю гібридної загрози в кіберпросторі від "класичних" кіберзагроз є застосування окрім описаних вище рівнів третього його складового рівня – соціального. При цьому основною мішенню в такому разі виступає не фізична інфраструктура інформаційно-телекомунікаційних систем та логіка роботи периферійних пристроїв, а оператор (власник) який її обслуговує або використовує у власних приватних цілях. До сьогодні вже є достатньо велика кількість таких прикладів. Але слід наголосити, що більшість з них не містить ознак прояву гібридної загрози в кіберпросторі.

Гібридна загроза в кіберпросторі не є новою за сутністю але є унікальною за узгодженістю цілей, динамічністю їх досягнення, зростанням ролі інформаційної та кібернетичної складової на усіх рівнях. Її інформаційною складовою виступають інформаційні дії. Під інформаційними діями в кіберпросторі пропонується розуміти

такі дії, які спрямовані на зміну масової та (або) індивідуальної свідомості суб'єктів впливу (соціуму) з метою стимулювання у них (нього) заданого типу поведінки. Другою складовою гібридної загрози є кібернетичні дії. Під такими діями пропонується розуміти дії, які спрямовані на блокування (зрив або обмеження) роботи фізичної інфраструктури інформаційно-телекомунікаційних систем та внесення змін в логіку роботи їх периферійних пристроїв шляхом взяття під контроль в них процесів управління.

У доповіді більш ґрунтовно розкриваються особливості інформаційних та кібернетичних дій, наводяться методи та способи їх реалізації. Особливий акцент зроблено на відмінностях між інформаційною та кібернетичною складовою гібридної загрози в кіберпросторі. Також показано їх спільні ознаки.

У доповіді наводяться приклади гібридних загроз в кіберпросторі та надаються результати аналізу насідків, які мали місце у результаті їх прояву.

Отже, в доповіді показано, що гібридна загроза в кіберпросторі – це новий вид загроз безпеці, прояв інформаційної та кібернетичної складові якої в результаті комплексування узгоджених за завданнями в часі та просторі й здійснюваних за єдиним задумом і планом дій, призводять до тяжких наслідків для людини суспільства та держави.

Література

1. Грищук, Р. В. Актуальні питання забезпечення інформаційної та кібернетичної безпеки у зоні проведення антитерористичної операції IX наук.-практ. конф. ["Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] (Київ, 25 лист. 2016 р.). – К. : ВІТІ НТУУ КПІ, 2016. – С. 83.

2. Грищук, Р. В. Інформаційна та кібернетична безпека: роль та місце в умовах гібридної війни / Всеукр. наук.-практ. конф. ["Кібербезпека в Україні: правові та організаційні питання : матеріали"] (Одеса, 21 жовтн. 2016 р.). – Одеса : ОДУВС, 2016. – С. 16–17.

3. Грищук, Р. В. Основи кібернетичної безпеки : Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

4. Boyer, B. Countering Hybrid Threats in Cyberspace. Cyber Defense Review, 2017, Vol. 2, Ed. 1. [Electronic resource] – Mode of access : http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1134632/countering-hybrid-threats-in-cyberspace.

5. NATO welcomes opening of European Centre for Countering Hybrid Threats, 11 Apr. 2017. [Electronic resource] – http://www.nato.int/cps/en/natohq/ news_143143.htm.

УДК 343.9

Гуцалюк М.В.
кандидат юридичних наук,
старший науковий співробітник, доцент
Міжвідомчий науково-дослідний центр з проблем
боротьби з організованою злочинністю при РНБО України

ЗАХОДИ БОРОТЬБИ З КОНТРАФАКЦІЄЮ І ПІРАТСТВОМ У МЕРЕЖІ ІНТЕРНЕТ

Виробництво контрафактної продукції є одним із найбільш поширених тіньових бізнесів для організованої злочинності, яка вважає його більш прибутковим і менш небезпечним, ніж інші види злочинної діяльності.

Міжнародна торгівля контрафактною продукцією становить до 2,5% світової торгівлі, або приблизно 338 млрд євро. Вплив контрафакції особливо високий в Європейському Союзі, де її частка становить до 5% від загального обсягу імпорту, або 85 мільярдів євро. Контрафактні товари виробляються без урахування норм санітарії і безпеки ЄС, вони можуть бути небезпечними для споживачів. В Україні ця проблема існує навіть у більших масштабах, адже за оцінками Всесвітнього економічного форуму, Україна за рівнем захисту інтелектуальної власності посідає 115-е місце серед 128-и країн [1].

У зв’язку із відсутністю ефективних та системних засобів боротьби з порушеннями авторського права та суміжних прав у мережі Інтернет, недоліками в системі колективного управління авторськими та суміжними правами, широким використанням неліцензійного програмного забезпечення як урядовими, так і приватними установами Офіс торговельного представника США в рамках «Спеціальної доповіді 301» («Special 301» List) присвоїв нашій державі статус «Пріоритетної іноземної країни» («Priority Foreign Country») [2].

Разом із стрімким поширенням мережі Інтернет, збільшенням кількості користувачів розповсюджується й Інтернет-піратство, чому сприяють недосконалість чинного законодавства та відсутність дієвого механізму впливу на порушників авторського права і суміжних прав в Інтернеті.

За даними Української антипіратської асоціації, середній термін у днях між першим виходом фільму в кінотеатрах і появою його піратської копії в Інтернеті в VI кварталі 2016 року становив 8,5 дня, а в VI кварталі 2015 року – 13,5 дня, тобто значно зменшився [3].

Інтернет-піратство має глобальний характер, його неможливо

побороти в окремій країні. Але світова спільнота і кожна країна намагаються розробити дієвий механізм спрощеного та прискореного захисту авторського права в мережі Інтернет.

Активну роль у протидії правопорушенням у цій сфері відіграють правоохоронні органи, які налагоджують тісне міжнародне співробітництво. Більше 4500 доменних імен, які незаконно використовувалися для продажу контрафактної продукції, були вилучені під час спільної глобальної операції «In Our Sites», яка проходила в листопаді 2016 року за сприяння Європолу та Інтерполу. У ній взяли участь представники 27-и країн та Національного Координаційного центру з прав інтелектуальної власності США [4].

Боротьба з торгівлею контрафактною продукцією в Інтернеті є складним завданням для правоохоронних органів. Для того, щоб посилити боротьбу з контрафакцією і піратством в Інтернеті, Європол і Офіс Європейського Союзу з інтелектуальної власності (EUIPO) об'єднали свої зусилля для створення Координаційної коаліції протидії злочинності в галузі інтелектуальної власності (the Intellectual Property Crime Coordinated Coalition – IPC3) в липні 2016 року [5].

Міжнародна промислова палата 26 квітня 2017 року опублікувала Стратегічний план щодо захисту інтелектуальної власності [6]. Серед інших напрямів у плані значна увага приділяється захисту інтелектуальної власності в мережі Інтернет. Зокрема зазначено, що Інтернет ставить перед правоохоронними органами комплекс юридичних та практичних проблем, серед яких розробка інструментів для виявлення порушень он-лайн, збору електронних доказів, а також реальні проблеми, пов'язані з ідентифікацією кінцевого місця перебування підозрюваного порушника.

При цьому необхідно забезпечити дотримання презумпції невинуватості, права на справедливий судовий розгляд, а також належного процесу щодо розкриття конфіденційної інформації.

Сучасна практика європейської протидії контрафакту і піратству передбачає декілька підходів:

– судове переслідування промислових масштабів піратства;

– блокування сайтів Інтернет-провайдерами на основі судового рішення;

– тісна співпраця з посередниками (провайдерами, платіжними системами, рекламодавцями і пошуковими системами).

В Україні Стратегією сталого розвитку «Україна-2020», схваленою Указом Президента України від 12.01.15 р. № 5/2015 передбачено реалізацію Реформи захисту інтелектуальної власності. Для забезпечення реформування у цій сфері передусім необхідно вдосконалити законодавство. Суттєвим кроком у цьому напрямку став Закон Украї-

ни «Про державну підтримку кінематографії в Україні» [7], який набрав чинності 26 квітня 2017 року. Законом внесені зміни в деякі законодавчі акти, у тому числі в Закон України «Про авторське право і суміжні права», які сприятимуть посиленню протидії правопорушенням у сфері інтелектуальної власності, особливо Інтернет-піратству.

Крім реформування законодавства, необхідно приділити увагу налагодженню дієвої взаємодії державних структур та приватного сектору, а також підвищенню обізнаності населення щодо контрафактної продукції.

Слушним буде також використання захищених технологій в Інтернеті, наприклад, ID-web – створення web-ресурсів та користування ними на основі ідентифікації за допомогою біометричних ID-документів [8].

Література

1. The International Property Rights Index 2016. URL: http://internationalpropertyrightsindex.org/countries
2. 2016 Special 301 Report. URL: https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf
3. Що таке Інтернет-піратство? URL: http://apo.kiev.ua/internet.phtml
4. Over 4500 Illicit Domain Names Seized For Selling Counterfeit Products: URL: https://www.europol.europa.eu/newsroom/news/over-4500-illicit-domain-names-seized-for-selling-counterfeit-products
5. Intellectual Property Crime Coordinated Coalition. URL: https://www.europol.europa.eu/about-europol/intellectual-property-crime-coordinated-coalition-ipc3
6. The ICC Intellectual Property Roadmap. URL: https://iccwbo.org/publication/icc-intellectual-property-roadmap-current-emerging-issues-business-policymakers/
7. Закон України Про державну підтримку кінематографії в Україні від 23 березня 2017 року № 1977-VIII. URL:: http://zakon3.rada.gov.ua/laws/show/1977-19.
8. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 18. – С. 265 – 269.

Даник Ю.Г.

доктор технічних наук, професор

Національний університет оборони України

ім. І.Черняховського

ФОРМУВАННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Гібридна війна, яка триває на сході України, є високотехнологі-

чним конфліктом, метою якого з боку Росії є нав'язування Україні своєї волі за допомогою комплексних, адаптивних, асиметричних і синхронізованих впливів у багатовимірному просторі та різних сферах з поєднанням конвенційної і неконвенційної складових, забезпеченням мультиплікативності та синергетичності результатів і високого рівня невизначеності щодо кінцевих цілей і шляхів їх досягнення.

Сьогодні до високих технологій відносять найбільш нові і прогресивні технології сучасності, серед яких не останнє місце займають технології боротьби у кіберпросторі.

Світовий досвід показує, що близько 70 країн світу активно займаються питаннями кібербезпеки держави, в тому числі у військовій сфері. Близько 50 країн мають власні системи кібербезпеки (кібервійська), які створені за останнє десятиріччя. У Російській Федерації 22 лютого 2017 року було створено Війська інформаційних операцій, які, проміж іншим, включають також і кібервійська чисельністю біля 5000 осіб (рис. 1).

Рис. 1. Сили та засоби кіберкомандування військ інформаційних операцій ЗС Російської Федерації

Отже, ефективне протистояння агресії з боку Росії у кіберпросторі потребує адекватної відповіді України на основі створення відповідних органів управління, підрозділів та засобів з використанням існуючих та перспективних технологій.

Для ефективної розробки, створення, супроводження високотехнологічних засобів озброєння боротьби у кіберпросторі доцільним є створення навчально-науково-випробувальних комплексів, де поєднується освітня та наукові складові експериментально-бойові підрозділи, здатні застосовувати навчально-бойове озброєння і техніку, які проходять підготовку на спеціальних (кібер)полігонах і працюють у взаємодії з конструкторськими бюро та експериментально-дослідницьким

виробництвом.

Передбачається, що саме у поєднанні наукової, освітньої та практичної складових може бути досягнуто значного ефекту у протидії високотехнологічним загрозам сьогодення у кіберпросторі.

УДК 351.746.1+004.9: 340.13(043.2)

Довгань О.Д.
доктор юридичних наук,
старший науковий співробітник
Науково-дослідний інститут інформатики і права
Національної академії правових наук України

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ПРОБЛЕМА ДЕРЖАВНОГО РІВНЯ

Застосування країною-агресором по відношенню до України технологій гібридної війни, у першу чергу в інформаційній сфері, сформувало нові виклики та загрози інформаційній безпеці держави. Кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом такої гібридної війни. Тому, забезпечення цілісності, достовірності та конфіденційності інформації в кіберпросторі стало однією з найважливіших проблем нинішнього століття і головним завданням держави, економіки та суспільства, як на державному, так і на міжнародному рівні. Залишаються актуальними на сьогодні питання необхідності створення цілісної та узгодженої системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів у інформаційній сфері, розбудови власних спроможностей надійних та достовірних державних комунікацій та створення тісної взаємодії між органами влади, формування інфраструктури національного інформаційного простору з метою створення умов для його інтегрування у світовий інформаційний простір, налагодження комунікаційного процесу між органами влади та споживачами інформації. Тому питання кібербезпеки, у т.ч. її правового забезпечення, у нашій державі має надзвичайно велике значення.

Інформаційне законодавство відіграє значну роль у подальшому прогресі інформаційного суспільства та інформаційної сфери. Аналіз правових систем показує, що практично всі держави мають численні нормативні акти, спрямовані на врегулювання суспільних відносин в різних сегментах інформаційної сфери: забезпечення і захист свободи слова та свободи використання і поширення інформації; функціонування телекомунікацій; захист інтелектуальної власності; застосування інформаційних комп'ютерних технологій, електронного цифрового підпису, електронного документообігу; забезпечення інформаційної безпеки та кібербезпеки тощо.

Для інформаційної сфери є критично важливою наявність відповідних політико-правових документів, затверджених на найвищому державному рівні. Оскільки такі документи формують бажану модель предметної сфери і є важливим чинником формування наукової правосвідомості.

На сьогодні є ціла низка законів України та інших нормативних документів різних рівнів які загалом охоплюють проблеми забезпечення кібербезпеки держави, але вони не охоплюють всі основні елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Проведемо аналіз прийнятих нормативно - правових документів.

Першим чинним стратегічним документом в межах даної проблематики стала Стратегія національної безпеки України, яка визначила основні загрози кібербезпеці і безпеці інформаційних ресурсів та пріоритети забезпечення: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки. Якщо детально розглянути ці пріоритети, то видно, що фактично був визначений реальний дороговказ, що потрібно робити і куди рухатися вперед.

З набуттям чинності Стратегії кібербезпеки України наша країна підтвердила наміри у напрямі розбудови національної системи кібербезпеки. На державному рівні задекларовано, що пріоритетами й напрямами забезпечення кібербезпеки в сучасних умовах є: розвиток безпечного, стабільного та надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів і критичної інформаційної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю тощо.

Ужиття заходів, визначених Стратегією національної безпеки України та Стратегією кібербезпеки зумовило необхідність змін у

чинному законодавстві, насамперед з метою подальшого унормування суспільних відносин, пов'язаних з реалізацією завдань в оборонній та безпековій сферах.

На розвиток цього за останній рік було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких Концепція розвитку сектору безпеки і оборони України, Стратегічний оборонний бюлетень, Положення про Національний координаційний центр кібербезпеки, Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави та низка інших. Все це є підтвердженням важливості питань, що стосуються кібербезпеки. Але б усе було добре. Однак, на жаль, у нашій державі існує негативна тенденція щодо невжиття окремими суб'єктами, які наділені владними повноваженнями, планових заходів, затверджених на державному рівні. Тому, була відповідна реакція з боку держави і рішенням Ради національної безпеки і оборони України від 29.12.16 р., уведеним в дію Указом Президента України від 13.02.17 р. № 32/2017, в якому акцентовано увагу на необхідності термінової підготовки законодавчих пропозицій щодо кіберзахисту об'єктів критичної інформаційної інфраструктури, посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах тощо.

Окремо потрібно говорити про проект Закону України «Про основні засади забезпечення кібербезпеки України», який було прийнято Верховною Радою України за основу у вересні 2016 р. Проте, зазначений проект далекий від досконалого, на що справедливо було звернуто увагу науковцями.

Загалом, практичне виконання зазначених вище фундаментальних положень щодо забезпечення кібербезпеки неможливе без формування чітко регламентованих поточних і перспективних планових засад державної політики в зазначеному контексті, що передбачає: визначення алгоритму реалізації відповідних скерованих державних планових заходів, установлення конкретних строків їх ужиття, посилення відповідальності за прострочення термінів, прискорення комплексної взаємодії та узгоджених спільних дій суб'єктів забезпечення кібербезпеки.

Тому, прийняття цілого ряду нормативних-правових актів, у т.ч. стратегії кібербезпеки і подальше схвалення закону про кібербезпеку має не просто убезпечити країну та захистити її від ряду нових загроз, але і переформатувати роботу спецслужб і інших державних органів. Звичайно, це стане можливим за наявності політичної волі та комплексного бачення майбутнього розвитку країни. Рішення повинно бути комплексним і комбінованим. Питання кібербезпеки – це питання виживання країни і можливості її розвитку.

Література

1. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.
2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.16 р. № 96/2016 // Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.
3. Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.16 р. № 92/2016// Офіційне інтернет-представництво Президента України. URL: http: //www.president.gov.ua.
4. Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 06.06.16 р. № 240// Офіційне інтернет-представництво Президента України [Електронний ресурс]. − Режим доступу: http: //www.president.gov.ua.
5. Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.16 р. № 242/2016// Офіційне інтернет-представництво Президента України. URL: http: //www.president.gov.ua.
6. Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563. URL: http://zakon0.rada.gov.ua/laws/show/563-2016-%D0%BF
7. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека” // Правова інформатика. – 2014. – № 2(42). – С.54-62.

УДК 355.40

Заєць П.М.
Національна академія Служби безпеки України
Іванова О.С.
кандидат фізико-математичних наук
Національна академія Служби безпеки України
Скубак О.М.
кандидат технічних наук
Національна академія Служби безпеки України

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КІБЕРПРОСТОРІ УКРАЇНИ

В зв’язку з активізацією зовнішніх дій, хакерських атак на інформаційний простір банків, державних структур в світі і в Україні актуальним стає питання інформаційної безпеки кіберпростору країни.

В самому загальному аспекті під інформаційною безпекою ми

розуміємо стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави [1]. В інформаційному праві інформаційна безпека – це одна з сторін розгляду інформаційних відносин в межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобіганню таким загрозам правовими методами [2]. В цьому плані важливою являється концепція інформаційної безпеки держави. Дана концепція являє собою систематизовану сукупність відомостей про інформаційну безпеку України та шляхи її забезпечення. Вона включає в себе проведення системних класифікацій дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільству і державі; обґрунтування основних положень з організації забезпечення інформаційної безпеки держави; розробку пропозицій за способами і формами забезпечення інформаційної безпеки.

Основні загрози кібербезпеці можна розділити на три групи [1]:

1. загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації);

2. загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію та інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

3. загрози інформаційним правам і свободам особистості (право на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т.ін.).

Література

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. –К: «МК- Прес», 2005. – 432с., іл..

2. Цимбалюк В.С., Павловський В.Д., Грищенко В.В. та ін.; За ред. Швеця М.Я., Калюжного Р.А. та Мельника П.В., Навч. посіб. – К.: Знання, 2004. – 274 с.

УДК 351.746.1

Іванов О.Ю.
Національна академія Служби безпеки України

РОСІЙСЬКО-УКРАЇНСЬКЕ ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО З «КРИМСЬКОГО ПИТАННЯ»: ГЕНЕЗИС ТА СУЧАСНИЙ СТАН

Після протиправної анексії Російською Федерацією території АРК у лютому – березні 2014 р. представники її органів влади та управління активно почали займатися фальсифікаціями історії, прагнучи довести «споконвічний російський» статус Криму. Відтак, слід констатувати, що РФ розпочала інформаційну війну проти України через різноманітні засоби масової інформації: телебачення, друковані видання, Інтернет і т. ін. Метою таких дій є також формування позитивного міжнародного іміджу РФ. Проблема російсько-українського інформаційного протиборства з «кримського питання» досліджена недостатньо, що і обумовлює актуальність теми нашої доповіді.

Аналіз історичного досвіду свідчить про те, що в інформаційній війні РФ проти України в аспекті «кримського питання» можна виділити два етапи: до та після протиправної анексії території АРК. У межах першого етапу можна виокремити декілька стадій. На першій стадії, яку умовно відносимо до першої половини 1990-х рр., метою інформаційної війни РФ проти України було заперечити правомірність залишення Криму у складі України після розпаду СРСР у 1991 р. Для цього російські можновладці активно намагались обґрунтувати неправомірність рішення радянського керівництва про передачу Кримської області зі складу РРФСР до УРСР у 1954 р. У 1993 р. навіть була ухвалена Постанова Державної Думи РФ, згідно з якою відповідні законодавчі акти СРСР були нібито визнані нікчемними. Цьому акту передувала активізація проросійських сил у Криму під проводом Ю. Мєшкова, які поширювали через засоби масової інформації псевдоаргументи щодо нібито волюнтаристського характеру рішення М. Хрущова про передачу Кримської області, не обумовленого жодними історичними, економічними та правовими підставами. У межах сепаратистських тенденцій у Криму до та після вказаної Постанови поширювалася пропагандистська література, у якій населення переконували в тому, що Крим був і залишається російською територією, а українській владі пропонувалося «припинити являти світові документи сорокарічної давності», які заперечували основні постулати російської пропаганди.

У цей же період предметом російсько-українського інформа-

ційного протиборства став і правовий статус м. Севастополя. Російська пропаганда поширювала безпідставну інформацію про те, що позаяк після перетворення Кримської АРСР на Кримську область у 1945 р. статус м. Севастополя було визначено як статус міста обласного підпорядкування, то при передачі Кримської області до складу УРСР у 1954 р. статусу цього міста нібито змінено не було і воно залишалося російським. З цього приводу існує дві постанови – Верховної Ради РФ 1992 р. та Держдуми РФ 1993 р., – у яких закріплено статус м. Севастополя як міста республіканського підпорядкування у складі РФ. Однак при цьому не враховано того факту, що правовий статус м. Севастополя, наданий йому у 1945 р., передбачав лише порядок його фінансування напряму із загальносоюзного бюджету, не вносячи при цьому змін до його статусу як адміністративно-територіальної одиниці. У зв'язку з цим фактом як відповідь у межах інформаційного протиборства Верховною Радою України у 1993 р. було прийнято текст звернення до Держдуми РФ із вимогою про скасування протиправних рішень. У світлі зазначених подій до Верховної Ради України та до Президента України стали масово надходити звернення громадян із реакцією на такі дії РФ та пропозиціями щодо дій України у відповідь. Це можна розглядати як свідчення реакції громадянського суспільства на дії РФ у вигляді несприйняття поширюваної нею пропаганди.

Наприкінці 1990-х рр. можна виділити другу стадію першого етапу російсько-українського інформаційного протиборства. У цей час набули поширення дослідження з історії Криму, автори яких намагалися довести «споконвічну» приналежність Криму Росії. Ці дослідження охоплювали вже не лише радянську добу, а і більш ранні періоди (Кримське Ханство, перебування Криму у складі Російської імперії). Характерною рисою цих праць є те, що в них викривлено передумови включення території Кримського Ханства до складу Російської імперії у 1783 р. та характер національної політики російського самодержавства на новоприєднаних територіях. Наведено хибні причини формування переважно російського складу населення Криму через приховування фактів добровільно-примусової еміграції кримських татар. Більше того, у передмові до одного з таких питань піддано критиці позицію української влади щодо беззаперечної належності Криму Україні та мало не злочинним називалося недопущення відокремлення «Республіки Крим» від України. Там же окремо наголошено на тому, що українська влада нібито безпідставно заперечувала «споконвічний» російський статус Криму та намагалася виключно силовими методами втримати Крим у складі України. Наслідком цієї стадії першого етапу інформаційного протиборства стала

активізація сепаратистських тенденцій в АРК на початку 2000-х рр., які були відвернені завдяки зусиллям співробітників СБУ.

Другий етап російсько-українського інформаційного протиборства, який розпочався після згаданих подій 2014 р., характеризується посиленням історичної аргументації стратегічного значення території Криму для Росії. Основним вектором сучасної російської пропаганди є намагання обґрунтувати нібито сприятливість перебування Криму у складі Росії для його соціально-економічного розвитку та забезпечення національних прав кримських татар. Такі тези неодноразово звучали з боку органів влади та управління РФ, так і від її представників на засіданнях різноманітних міжнародних інституцій. Аргументами у цих випадках слугують переважно перекручення фактів історико-правової дійсності Криму під час його перебування у складі Російської імперії (1783 – 1917 рр.) та у складі РРФСР (1921 – 1954 рр.). Причому об'єктами такої пропаганди стали не лише українська та міжнародна спільнота, а і населення РФ, яке у такий спосіб переконують у необхідності беззаперечно вірити своїй владі та підтримувати всі її рішення.

З метою формування системи ефективної протидії інформаційній пропаганді РФ Указом Президента України від 25 лютого 2017 р. було затверджено Доктрину інформаційної безпеки України. У ній, зокрема, зазначено, що СБУ має здійснювати моніторинг вітчизняних та іноземних засобів масової інформації та Мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері. На нашу думку, з огляду на наведений вище аналіз змісту етапів російсько-українського інформаційного протиборства вказане положення Доктрини слід доповнити вказівкою на необхідність моніторингу також і наукової та науково-популярної літератури, оскільки, як свідчить практика, там також можуть міститися значні перекручення фактів історичної дійсності з пропагандистською метою.

Таким чином, російсько-українське інформаційне протиборство було розв'язане представниками РФ на початку 1990-х років для обґрунтування своїх нібито історичних прав на Крим шляхом поширення фальсифікацій історичних відомостей. Для забезпечення ефективної протидії української влади російській пропаганді з «кримського питання» має бути вдосконалена наявна правова база, у тому числі у напрямі розширення повноважень СБУ в цій сфері та способів їх здійснення.

УДК 341.824:338.46

Касперський І.П.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

ВІТЧИЗНЯНЕ ТА ЄВРОПЕЙСЬКЕ РЕГУЛЮВАННЯ СТРАТЕГІЧНИХ ПІДХОДІВ У ГАРАНТУВАННІ КІБЕРБЕЗПЕКИ

Стратегією кібербезпеки України [1] одним із принципів забезпечення кібербезпеки України визначено міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам.

У цьому контексті досить цікавим є досвід ЄС у сфері кібербезпеки з огляду на необхідність досягнення стандартів ЄС для забезпечення євроінтеграційних процесів.

За даними Європарламенту, технічні помилки та помилки персоналу в сфері мережевої безпеки, а також кібератаки призводять до €288 млрд. збитку щороку. Згідно з щорічним звітом Європейського агентства із мережевої та інформаційної безпеки (ENISA) основними мережевими загрозами залишається активність шкідливих програм, мережеві атаки, атаки із використанням стандартних додатків та ботмереж.

Стратегія кібербезпеки ЄС була прийнята у 2013 році [2] і у її розвиток у 2016 році Європейський парламент прийняв закон тобто Директиву із мережевої та інформаційної безпеки [3];.

Згідно з положеннями цієї директиви кожна держава-член ЄС зобов’язана розробити власну стратегію кібербезпеки та співпрацювати з ЄС та урядами країн-членів ЄС через спеціально створену директивою Групу співробітництва, офіційну підтримку якій зобов’язано надавати Європейське агентство із мережевої та інформаційної безпеки (ENISA), яке делегує до складу групи своїх представників разом із членами ЄС та представниками єврокомісії.

Також члени ЄС зобов’язані:

- визначити які саме суб’єкти будуть визнані складовими критичної інфраструктури;
- визначити один або декілька державних органів відповідальними за кібербезпеку та наділити їх достатніми повноваженнями;
- створити єдиний центр взаємодії усіх учасників процесу безпеки на базі уповноваженого органу;
- створити і забезпечити роботу груп реагування на інциденти інформаційної безпеки.

Закон встановлює зобов'язання по забезпеченню кібербезпеки підприємств критичної інфраструктури, таких як транспортні, енергетичні, фінансові і медичні компанії. Під його вплив також потрапляють інтернет-фірми, такі як Google і Amazon, які будуть зобов'язані повідомляти про інциденти ІБ владі ЄС. Таким чином закон допоможе зміцнити довіру користувачів до інтернет-сервісів, особливо закордонних. Відмова від надання інформації про інциденти спричинить санкції з боку уряду.

Директива ЄС наполягає на залученні ресурсів приватного сектору для виконання завдань безпеки, водночас встановлюючи обмеження спрямовані на захист інтелектуальних прав бізнесу.

З цього досвіду ми у нашій стратегії перейняли створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів.

Що одразу впадає в очі при порівнянні двох стратегій:

- європейська будується на стандартах ISO тому оперує загальноприйнятою термінологією і загальновизнаними підходами до вирішення задач інформаційної безпеки, чого у нас немає (загального стандартизованого розуміння у термінології та підходах);
- другим опорним пунктом є існуюче регулювання в ЄС щодо доступу до банківської та фінансової інформації, яке береться до уваги, не модифікується і не звужується новим актом;
- європейська стратегія апріорі розглядає державу, суспільство і бізнес як єдине ціле, а основна задача – вільне функціонування бізнес процесів та забезпечення прав споживачів (про такі речі як у нас, де цілями стратегії кібербезпеки визнаються зокрема посилення спроможностей суб'єктів сектору безпеки та оборони та забезпечення кіберзахисту державних електронних інформаційних ресурсів, про що в ЄС навіть мови немає);
- роль держави в основному в обов’язках перед громадянами забезпечити належне функціонування електронних способів надання адміністративних послуг в тому числі забезпечення електронного урядування та електронного цифрового підпису, створення безпекової структури, контроль за дотриманням стандартів.

У нашому контексті на виконання завдання Стратегії кібербезпеки України, яке полягає у упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти пропонується:

- забезпечити чіткі критерії визначення меж втручання держави у телекомунікаційний простір;

- розробити прозорі правила залучення суб'єктів приватного права до вирішення завдань безпеки кіберпростору;
- створити спільний консультативний орган взаємодії між державою та іт-спільнотою;
- формувати на базі цього органу шляхом домовленостей меморандуми щодо протидії загрозам у кіберпросторі за участі обох сторін.

Література

1. Стратегія кібербезпеки України: затв. Указом президента України №96 від 15.03.16р. // Офіційний вісник України від 29.03.2016. 2016. № 23.стор. 69, стаття 899, код акту 81164/2016

2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7.2.2013 [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1493795785820&uri=CELEX:52013JC0001

3. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

УДК 35.078.3

Климчук О.О.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України
Ткачук Н.А.
Служба безпеки України

ФОРМУВАННЯ ДЕРЖАВНОЇ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ

Термін «політика кібернетичної безпеки (кібербезпеки)» (англ. National cyber security strategy – NCSS) увійшов до сталого обігу завдяки активній діяльності у цьому напрямі американських, європейських науковців і політиків. При тлумаченні терміну ключовим смисловим компонентом виступає розуміння кіберполітики як інструмента поліпшення кібербезпеки, що є структурою високого рівня, яка базується на принципі «зверху донизу» й дозволяє встановити і підтримувати національні цілі й пріоритети [1].

За О.Мандзюком [2, с. 29], кібербезпекова політика - це цілеспрямована, науково обґрунтована діяльність державних органів, ор-

ганів місцевого самоврядування, недержавних структур (зокрема аналітичних центрів), окремих фахівців з формування і реалізації правових норм, концепцій, що дозволяють здійснювати управлінські, організаційні, технічні заходи з метою забезпечити інформаційний суверенітет України, а також убезпечити функціонування юридичних і фізичних осіб у кібернетичному просторі.

Стратегією кібербезпеки України завдання із формування та реалізації державної політики у сфері кіберзахисту покладено на Держспецзвязку [3]. Водночас, на сьогодні в державі чітко не визначено орган, який би відповідав за формування та реалізацію політики держави саме у сфері кібербезпеки. Окремі завдання щодо державної політики у сфері забезпечення кібербезпеки покладені на Національний координаційний центр кібербезпеки:

- опрацювання питань щодо визначення шляхів, механізмів та способів вирішення проблемних питань, що виникають під час реалізації державної політики у сфері забезпечення кібербезпеки;
- здійснення аналізу стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України;
- розроблення і внесення Раді національної безпеки і оборони України, її Голові в установленому порядку пропозицій щодо пріоритетних напрямів, концептуальних підходів до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [4].

Державна політика у сфері кібербезпеки, перш за все, повинна бути спрямована на створення ефективної системи кібербезпеки держави, здатної забезпечити протидію кіберзагрозам національній безпеці України. Формування кібербезпекової політики потребує комплексного підходу, та має базуватися на ретельному вивченні стану, проблемних питань та перспектив розвитку національної системи кібербезпеки; сукупності існуючих та потенційних кіберзагроз; вивченні міжнародного досвіду у сфері кібербезпеки; наявних сил та засобів у кіберпросторі спецслужб, правоохоронних органів та збройних сил іноземних країн; механізмів використання кіберпростору терористичними організаціями, а також в ході міждержавного протистояння.

Крім того, при формуванні кібербезпекової політики України необхідно враховувати особливості та тенденції розвитку геополітичної ситуації та міжнародних кібербезпекових трендів. Ґрунтовне дослідження геостратегічних чинників впливу на кібербезпекову політику України було здійснене Д. Дубовим. Науковець виокремлює наступні кібербезпекові тренди, з яких повинна виходити Україна, формуючи власну зовнішньо- та внутрішньополітичну страте-

гію в новому цифровому світі:

1. Протистояння у кіберпросторі між США та КНР, двох найбільш могутніх кібердержав, що може призвести до «холодної війни» оновленого формату.

2. Перетворення кіберпростору на нове поле геополітичного суперництва, що призводить до його подальшої мілітарізації, яка супроводжується посиленням недовіри між акторами, несформованістю міжнародного нормативно-правового поля та відчуттям нового протистояння.

3. Реалізація гонки озброєнь у кіберпросторі, що спонукатиме держави вкладати значні сили і кошти в кібербезпеку та власні кіберозброєння.

4. Неприйняття у майбутньому жодних дієвих міжнародних договорів щодо заборони кіберозброєнь через неможливість контролю за їх створенням.

5. Сплеск шпигунської активності, базованої на використанні кіберпростору.

6. Пріоритет національного виробника IT-продукції та створення суто національних продуктів, що їх уповноважені безпекові структури могли б ідентифікувати як дійсно безпечні.

7. Тенденція до сегментування кіберпростору та виникнення «національних інтернетів», а також збереження головної ролі держави, що має реальний контроль над фізичним рівнем кіберінфраструктури [5, с. 219-221].

У цілому погоджуємося щодо визначених кібербезпекових тенденцій, водночас, вважаємо, що не обов’язково саме протистояння США та КНР у кіберпросторі стане визначальним чинником впливу на кібербезпекову сферу та може перетворитися на своєрідну «холодну війну». Адже останнім часом фіксується значне потепління у відносинах між США та КНР у кібербезпековому домені та переорієнтування як китайських так і американських хакерів на інші країни, в т.ч. РФ.

Так, у вересні 2015 року між США та КНР було досягнуто домовленості щодо заходів протидії кібершпигунству. Країни зобов'язалися не здійснювати і не підтримувати діяльність, спрямовану на викрадення інтелектуальної власності за допомогою кібернетичних засобів, а також створити спільну робочу групу для подальшого регулювання зазначеної проблеми.

Опублікований у червні 2016 року звіт компанії FireEye про шпигунську діяльність хакерів, які діють з території Китаю або підтримуються китайською владою, засвідчив, що за минулий рік хакерські атаки з боку КНР проти США суттєво зменшилися. У цей період також були зафіксовані атаки з боку китайських хакерів на відомчі ресу-

рси в Росії і Азії [6]. У свою чергу, зі зміною геополітичного середовища, значно посилилося протистояння у кіберпросторі між США та РФ [7]. Саме ця тенденція може стати вирішальним трендом, що впливатиме на подальший розвиток глобальної кібербезпекової сфери.

Крім того, при формуванні кібербезпекової політики України необхідно враховувати ще одну сталу тенденцію – розширення меж використання кіберпростору терористами (сьогодні більшою мірою використовується терористичними угрупованнями для здійснення інформаційно-організаційного та фінансового забезпечення власної діяльності). Лише питанням часу залишається перетворення кіберзброї на зброю терористів, яка буде націлена на об'єкти підвищеної небезпеки та критичну інфраструктуру держави.

Ця тенденція є особливо актуальною для нашої держави у контексті проведення триваючої антитерористичної операції на сході України та вимагає вжиття відповідних заходів протидії, що забезпечать готовність нашої держави до її можливої реалізації.

Література

1. EU Launches First European Public-Private Partnership on Cybersecurity, Plans $2B Investment. URL: http://www.circleid.com/posts/20160706_eu_launches_first_european_public_private_partnership/.

2. Мандзюк О. Роль аналітичної діяльності й аналітичних центрів у формуванні та реалізації кібербезпекової політики // Підприємництво, госп-во і право. — 2015. — № 5. — С. 27-31.

3. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: http://www.president.gov.ua/documents/962016-19836.

4. Указ Президента України від 7.06.2016 р. №242/2016 «Про Національний координаційний центр кібербезпеки». URL: http://www.president.gov.ua/documents/2422016-20141.

5. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д.В. Дубов. – К.:, 2014. – 328 с.

6. China Recalculates its Use of Cyber Espionage: Special Report of Fireeye. URL: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

7. U.S. Considers Sanctions Against Russia in Response to Hacks of Democratic Groups [Електронний ресурс]. – Режим доступу : http://www.wsj.com/articles/u-s-considers-sanctions-against-russia-in-response-to-hacks-of-democratic-groups-1470946133.

Ковбан А.В.
кандидат юридичних наук, доцент
Національний університет
«Одеська морська академія»

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЕЛЕМЕНТ ГЛОБАЛЬНИХ ПРАВ

Демократизація міжнародно-правових відносин і лібералізація внутрішньодержавних процесів приводить до глобальних змін та нового переосмислення сучасного міжнародного права. Адже в контексті захисту прав людини більша увага приділяється розробці групових прав, таких як права народів, права нації тощо. Проте зазначені спільноти мають схожі права, які можна виділити в окрему групу – глобальні права.

Глобальні права (право народу, право нації) не є природним, оскільки вони формуються в міру становлення інтересів народу як населення держави. Європейська традиція розглядає права народу як колективні права та асоціює з правами умовного «третього покоління». Глобальні права, на нашу думку, беруть свій початок з ст. 1 Міжнародного пакту про громадянські і політичні права від 16 грудня 1966 р., де вказується, що всі народи мають право на самовизначення. У силу цього права вони вільно встановлюють свій політичний статус і вільно забезпечують свій економічний, соціальний і культурний розвиток. При цьому народи для досягнення своїх цілей можуть вільно розпоряджатися своїми природними багатствами і ресурсами без шкоди для будь-яких зобов'язань, що випливають з міжнародного економічного співробітництва, заснованого на принципі взаємної вигоди, та з міжнародного права. Одним з важливих елементів розвитку суспільства є право на безпеку та безпечне співіснування. Жодне суспільство та держава не є ізольовані та автономні в своєму розвитку та знаходиться під впливом багатьох зовнішніх чинників. Право на безпеку сьогодні розвивається не лише в контексті воєнного протистояння та дипломатичних розв’язань конфліктних ситуацій, але й у використанні інформаційних важелів для впливу на суспільство та громадську думку. Тому сьогодні активно вживається стан сучасного розвитку суспільства як інформаційного суспільства.

Основою такого суспільства є інформація та знання, які поєднуються в єдиному інформаційному просторі. Характерними ознаками інформаційного суспільства є збільшення ролі інформації і знань в житті суспільства, використання інформаційних технологій та комунікаціями, створення глобального інформаційного простору

для ефективної інформаційної взаємодії людей та доступ до світових інформаційних ресурсів.

Проте процес становлення інформаційного суспільства потребує й захисту, який можна використовувати не лише в межах судового та позасудового, але й в установленні самої безпеки – інформаційної безпеки. Інформаційну безпеку в сучасному інформаційному суспільстві можна розглянути стан захищеності особистості, суспільства і держави від внутрішніх і зовнішніх інформаційних загроз. Також інформаційна безпека забезпечує реалізацію конституційних прав і свобод людини та громадянина, гідний рівень життя громадян, суверенітет, територіальну цілісність та сталий соціально-економічний розвиток держави, оборону та безпеку держави.

В якості моделі інформаційної безпеки можна розглянути її такі обмежувачі: конфіденційність (інформація з обмеженим доступом суб'єктів, що мають на неї право), цілісність (уникнути незаконної зміни інформації), доступність (вільне володіння і розпорядження інформацією користувачем з правом доступу), підконтрольність (простежування дій суб'єкта по маніпуляції з об'єктом), достовірність (відповідність інформації поводженню чи результату), справжність (суб'єкт або інформація ідентичні заявленим). Аналізуючи інформаційну безпеку як невід’ємний елемент розвитку не тільки суспільства, але і держави як гаранта такого розвитку, можна стверджувати, що інформаційна безпека є елементом глобальних прав.

При виконанні гарантування інформаційної безпеки зі сторони держави, остання повинна виконувати певні зобов’язання. Загальні вимоги, які характеризують гарантування інформаційної безпеки суспільства і держави, повинні бути як організаційні, так і юридичні. Напрямками реалізації інформаційної безпеки повинно бути: забезпечення та захист громадянських прав і свобод людини і громадянина щодо отримання та використання інформації, приватності, недоторканності приватного життя при використанні інформаційних технологій, забезпечення інформаційної підтримки демократичних інститутів держави та громадянського суспільства; застосування інформаційних технологій задля збереження культурних, історичних і духовно-моральних цінностей держав; забезпечення сталого розвитку інформаційної інфраструктури; сприяння формуванню системи міжнародної інформаційної безпеки, як протидія загрозам використання інформаційних технологій з метою порушення міжнародного порядку.

Розглядаючи приватність як категорію інформаційного суспільства, слід наголосити на її напрямках – інформаційна приватність (встановлення правил збору та обігу персональних даних, таких як інформація кредитних установ та медичні записи), тілесна приват-

ність (захист від втручань стосовно фізичного стану людей, наприклад, тестування щодо вживання наркотиків та обстеження порожнин тіла), комунікаційна приватність (безпека та приватність поштових відправлень, телефонних розмов, електронних повідомлень та інших видів комунікації), територіальна приватність (встановлення обмежень на втручання в домашнє та інше навколишнє середовище, наприклад, робоче місце чи громадське оточення).

При досягненні позитивних показників в інформаційній безпеці, держави повинні обмежити загрози міжнародній інформаційній безпеці та створити інформаційний простір з рисами співпраці і гармонії на виконання резолюції Генеральної Асамблеї Організації Об'єднаних Націй A / RES / 65/41 від 8 грудня 2010 року "Досягнення у сфері інформатизації та комунікацій в контексті міжнародної безпеки», резолюції Генеральної Асамблеї Організації Об'єднаних Націй A / RES / 55/29 від 20 листопада 2000 «Роль науки і техніки в контексті міжнародної безпеки та роззброєння», резолюції Генеральної Асамблеї Організація Об'єднаних Націй A / RES / 64/211 від 21 грудня 2009 року "Створення глобальної культури кібербезпеки і оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур». Отже, міжнародні організації мають правову базу для функціонування інформаційної безпеки. Також з боку держав є необхідність.

посилення координації і зміцнення співпраці між в боротьбі з злочинним використанням інформаційних технологій і в даному випадку, велику роль можуть зіграти Організація Об'єднаних Націй та інші міжнародні та регіональні організації.

Отже, інформаційна безпека відіграє величезну роль у становленні такого глобального права як право на розвиток. Інформаційна безпека як елемент глобальних прав використовується як стан захищеності інтересів особистості, суспільства і держави від загроз деструктивних та інших негативних впливів в інформаційному просторі. Можна стверджувати, що інформаційна безпека є проблемою не лише однієї держави, а людства взагалі та є необхідним для подальшого розвитку в сучасному міжнародному праві та закріпленні в конституціях держав.

Література

1. Степко О. М. Аналіз головних складових інформаційної безпеки держави // [Електронний ресурс] – Режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/download/3172

2. В.Ю.Світлична, Т.І.Світлична. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення. URL: http://economy.kname.edu.ua/images/files/publishing/360-369_%D0%A1%D0%B2%D1%96%D1%82%D0%BB%D0%B8%D1%87%D0%BD%D0%B0_2.pdf

УДК 343.3

Ковтун Ю.В.
Служба безпеки України

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ ПРОСТОРУ ДЕРЖАВИ В УМОВАХ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

В умовах військової агресії Російської Федерації одну з найбільших загроз національній безпеці нашої держави становить антиукраїнська інформаційна експансія, яка на сьогодні набула ознак систематичного, спланованого і тривалого у часі процесу, що впроваджується і фінансується країною-агресором, та спрямований на залишення нашої держави в орбіті геополітичних інтересів Кремля, обмеження суверенітету та, як наслідок, руйнування України як незалежної держави.

Основним елементом масштабної інформаційної агресії у вітчизняному та світовому інформаційних просторах є проведення Російською Федерацією спеціальних інформаційних операцій, які передбачають поширення деструктивного контенту, повідомлень тенденційного характеру, викривленої інформації про процеси в Україні для маніпулювання суспільною свідомістю громадян України, дестабілізації суспільно-політичної обстановки, дискредитації євроінтеграційної політики нашої держави, інспірування сепаратистських настроїв, міжетнічної та міжконфесійної ворожнечі, висловлення недовіри до центральної влади з метою підбурення населення України до радикальних та екстремістських дій, спрямованих на антиконституційну зміну центральної влади в Україні, а також акції кібернетичного впливу.

При цьому, для реалізації базованих на сфальсифікованих інформаційних матеріалах масштабних кампаній інформаційно-психологічного впливу використовується ієрархічно-побудована система відповідних суб'єктів: державні та неурядові організації, аналітичні, дослідницькі центри, ЗМІ, журналісти, блогери, науковці, експерти, публічні особи, мережеві спільноти тощо.

Основними механізмами проведення російською стороною спеціальних інформаційних операцій через мережу Інтернет є:

- використання підконтрольних загальнодоступних Інтернет-ресурсів (новинні сайти, блоги, сайти громадсько-політичних структур, та ін.) для розміщення відверто антиукраїнського контенту, розрахованого для сприйняття проросійські налаштованими громадянами України, а також громадянами РФ, При цьому, широко поширеним є механізм «територіального» (фізичне знаходження сайту домена «.ua» на закордонних хост-майданчиках) та/або «іменного»

(назва сайту містить українські слова) маскування;

- створення та супроводження проросійських груп у соціальних мережах («ВКонтакте», «Одноклассники», «Фейсбук»). Адміністрування таких груп здійснюється з території РФ, тимчасово окупованих територій України (АР Крим, ОРДЛО) або невизнаних територіальних одиниць (ПМР). При цьому, переважна більшість учасників таких спільнот мають IP-адреси російського діапазону. На цьому напрямку спецслужбами РФ активно використовується механізм створення псевдоукраїнських груп з метою формування громадської думки про начебто невдоволення громадянами України соціально-економічною політикою вищого керівництва держави;

- залучення представників експертного середовища з числа громадян РФ та України, представників вітчизняних громадсько-політичних структур проросійського спрямування, маловідомих або взагалі «фейкових» (вигаданих) політологів та соціологів західноєвропейських країн, які за фінансову винагороду оприлюднюють матеріали антиукраїнського характеру.

Збільшення кількості деструктивних коментарів та антиукраїнських сайтів створює ілюзію підтримки населенням України та світовою спільнотою квазідержавних утворень на території ОРДЛО.

Окремим елементом «гібридної війни» є акції кібернетичного впливу, метою яких є завдання фінансової та матеріальної шкоди об'єктам критичної інфраструктури нашої держави, зокрема, фінансовим установам, підприємствам енергетики і транспорту, а також демонстрація можливостей з подальшим створенням негативного інформаційного фону, що оперативно використовується російськими ЗМІ.

З метою протидії зовнішній інформаційній агресії РФ Службою безпеки України проводиться системна робота, спрямована на виявлення, попередження і припинення загроз в інформаційному просторі України з боку російських спецслужб. Пріоритетними напрямками такої протидії є:

припинення антиукраїнської діяльності на території України представників російських та підконтрольних РФ іноземних ЗМІ та навколомедійних структур;

протидія негативним інформаційно-пропагандистським впливам, впроваджуваним країною-агресором;

протидія кібератакам російських спецслужб, які загрожують сталому функціонуванню важливих для держави електронних інформаційних ресурсів;

сприяння органам влади у розробці і впровадженні нових якісних механізмів протидії зовнішній інформаційній та кібернетичній агресій з боку іноземних країн та їх спецслужб.

Водночас, існує низка проблемних питань, вирішення яких дозволить більш ефективно протидіяти країні агресору в інформаційному та кіберпросторі.

Так, потребує нагального вирішення питання визначення на державному рівні порядку експертного оцінювання деструктивного інформаційного контенту, а також розроблення механізму видалення інформаційних повідомлень і матеріалів, які поширюються в мережі Інтернет та містять заклики до насильницької зміни або повалення конституційного ладу, посягання на територіальну цілісність і недоторканність, пропагують війну, тероризм тощо.

УДК 351.741

Комісаров О.Г.
доктор юридичних наук, професор
Дніпропетровський державний
університет внутрішніх справ

ТЕОРЕТИКО-ПРАВОВА МОДЕЛЬ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА, ЩО РЕГУЛЮЄ ІНФОРМАЦІЙНО-АНАЛІТИЧНУ ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ

Повноваження правоохоронних органів визначено у відповідних законодавчих актах та, як правило, розділено на основні (перелік переважно вичерпний) та додаткові, виконання яких може бути покладено на ці органи спеціальним законом. З метою реалізації вказаних повноважень утворюються системи вказаних органів, які, у свою чергу, складаються з територіальних підрозділів та міжрегіональних територіальних підрозділів. Кожна з утворених складових, виключно у межах визначених у положеннях (статутах) про такі підрозділи, з метою забезпечення діяльності керівника підрозділу, а також виконання покладених на підрозділ завдань здійснює інформаційно-аналітичну діяльність.

Керівні принципи інформаційно-аналітичної діяльності правоохоронних органів та їх структурних підрозділів визначено у: Резолюції 34/169 Генеральної асамблеї ООН «Кодекс поведінки посадових осіб по підтриманню правопорядку»; Рекомендаціях Комітету міністрів Ради Європи державам-членам від 09.09.2003 № Rec(2003)14 «Про можливість взаємодії інформаційних систем у сфері правосуддя»; Рекомендаціях Комітету міністрів Ради Європи державам-членам від 10.07.2003 № Rec(2003)13 «Щодо порядку надання інформації про розгляд кримінальних справ засобам масової інформації»; Декларації Рада Європи про європейську політику в

галузі нових інформаційних технологій 06.05.1999; актах інформаційного законодавства України, Державних та галузевих стандартах України з інформаційної діяльності.

Інформаційне законодавство та інформаційно-правова наука одностайно визначають основними видами інформаційної діяльності створення, збирання, одержання, зберігання, використання, поширення, охорону та захист інформації, що дозволяє сформувати предмет інформаційно-аналітичної роботи у правоохоронній діяльності – вивчення закономірностей практично всіх процесів і явищ суспільного життя, які тією чи іншою мірою впливають на діяльність відповідного правоохоронного органу та держави загалом, використанні здобутих відомостей і знань для забезпечення їх ефективності діяльності.

Інформаційно-аналітична робота є цілеспрямованою, творчою, дослідницькою, спеціально організованою діяльністю, яка здійснюється на основі методів пізнання й призначена здійснювати збір, накопичення й обробку даних; пошук, аналіз й узагальнення інформації про стан правопорядку та діяльність правоохоронних органів; отримання нових спеціальних знань щодо підвищення ефективності боротьби з кримінальними правопорушеннями й спрямована на якісне забезпечення управлінської діяльності на різних рівнях щодо забезпечення охорони прав і свобод людини, протидії злочинності, підтримання безпеки і порядку. Інформаційно-аналітичне забезпечення являє собою комплекс заходів із збору, опрацювання та використання інформації, необхідної для виконання підрозділами окремих правоохоронних органів покладених на них функцій та завдань. Інформаційно-аналітична робота та інформаційно-аналітичне забезпечення є «обов’язковими», спеціально організованими процесами управління, невід’ємними складовими частинами організаційної діяльності, функцією усіх ланок усіх правоохоронних систем, що функціонують постійно та із обсягами обробки даних кількість яких незмінно збільшується.

За цільовими властивостями інформаційно-аналітична робота є безперервним процесом вивчення оточуючого середовища, який складається з етапів: 1) збору, накопичення й обробки даних; 2) пошуку, аналізу й узагальнення інформації; 3) отримання спеціальних знань.

Здійснення інформаційно-аналітичної діяльності структурними підрозділами правоохоронних органів розглядається переважно з огляду на операційні процедури організації та функціонування інформаційно-пошукових систем (баз даних), їх інтеграції до інформаційного середовища правоохоронних органів, систем міжнародного інформаційного обміну тощо.

Ведення баз даних – це діяльність, спрямована на оновлювання, підтримування, перебудову структури бази даних, щоб забезпечити її цілісність, збереженість і ефективність. При цьому «операційні процедури» обумовлені інформаційними потребами самого правоохоронного органу, його функціями та обов'язками його персоналу. Більшість баз (банків) даних, якими користуються правоохоронні органи містять інформацію обмеженого доступу (конфіденційну, таємну та службову інформацію), яка може поширюватися за бажанням (згодою) відповідної особи у визначеному спільно з нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Необхідне оснащення правоохоронних органів технічними та технологічними засобами базується на використанні сучасних інформаційних технологій, засобів комп'ютерної техніки, телекомунікаційного обладнання, загальносистемного та прикладного програмного забезпечення й здійснюється в єдиному порядку інформатизації визначеному у законі.

Створюючи бази даних правоохоронний орган стає власником інформаційної продукції (цих баз даних) у відповідних відносинах, але власником інформації залишається фізична або юридична особа, якій належить право власності на відповідну інформацію. При цьому інформація, яка обробляється в інтегрованих системах є власністю держави і підлягає захисту відповідно до чинного законодавства.

УДК 351.74:007

Кудінов В.А.
кандидат фізико-математичних наук, доцент
Національна академія внутрішніх справ

ДО ПРОБЛЕМИ ЩОДО СТВОРЕННЯ НАДІЙНИХ ПАРОЛІВ КОРИСТУВАЧІВ ІНТЕГРОВАНОЇ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ МВС УКРАЇНИ

Відповідно до Указу Президента України від 20 жовтня 2005 року № 1497/2005 передбачено створення інтегрованих інформаційно-аналітичних систем органів державної влади та органів місцевого самоврядування, правоохоронних органів [1]. Тому в системі Міністерства внутрішніх справ (далі – МВС) України вживаються заходи щодо створення та впровадження різноманітних інтегрованих інформаційних систем. Станом на сьогодні найбільш потужною серед них є Інтегрована інформаційно-пошукова система (далі – ІІПС)

МВС України («АРМОР») [2].

МВС України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними базами даних ІІПС у порядку, визначеному у статтях 26, 27 Закону України «Про Національну поліцію» (ст. 28) [3]. Інформація про доступ до баз даних фіксується та зберігається в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. Чинним законодавством передбачено, що поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації [3]. При цьому виникає актуальна проблема щодо уникнення неправомірного використання зловмисниками правами доступу поліцейських до баз даних ІІПС. Одним з шляхів її вирішення є створення надійних паролів користувачів даної системи.

Пароль, згідно відомчої Інструкції з організації функціонування ІІПС, – це послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж він почне обробку інформації в ІІПС.

В Інструкції зазначені такі правила формування атрибуту «Пароль»:

1. Пароль визначається та використовується користувачем особисто і розголошенню не підлягає.
2. Довжина повинна бути не менше 5 символів.
3. Використовується тільки поєднання літер та цифр.
4. Початковий пароль формується адміністратором безпеки ІІПС під час реєстрації нового користувача (пароль співпадає з ім'ям користувача); користувач зобов'язаний змінити зазначений пароль під час першого сеансу роботи з ІІПС (доступ до об'єктів обліку ІІПС новому користувачеві надається тільки після зміни початкового паролю, до цього моменту користувачеві заборонено будь-який доступ).
5. Користувач зобов'язаний змінювати пароль тільки особисто. Термін зміни пароля визначається адміністратором безпеки ІІПС відповідного рівня, але не рідше одного разу на місяць.

На наш погляд, для створення надійних паролів користувачів ІІПС правила формування атрибуту «Пароль» необхідно розширити, а саме:

1. Довжина повинна бути не менше 12 символів.
2. Повинен містити літери верхнього та нижнього регістру.

3. Повинен містити окремі спецсимволи (!@#$%^&*()_+?|).

4. Використовувати заміну окремих символів в паролі на символи, які схожі за написанням.

5. Набирати пароль кирилицею у латинській розкладці.

6. Повинен значно відрізняється від попереднього паролю.

7. Не повинен містити персональні дані користувача.

8. Не використовувати паролі зі сфери своєї діяльності.

9. Не повинен співпадати з логіном.

10. Не повинен складатися з цілого слова.

11. Не використовувати стандартні паролі, засновані на повторенні, словникових словах, літерних або числових послідовностях.

12. Пароль можливо запам'ятати (не записуйте та не залишайте пароль на видному місці).

При вимаганні від користувачів створювати надійні паролі необхідно враховувати також те, що складні паролі можна легко забути, і їх з більшою ймовірністю будуть записувати на папері, що передбачає собою певний ризик. З іншого боку, якщо зажадати у користувачів запам'ятовувати паролі напам'ять, то вони будуть придумувати більш легкі паролі, що серйозно збільшить ризик злому.

Таким чином, у роботі запропоновано розширити правила формування атрибуту «Пароль» користувача Інтегрованої інформаційно-пошукової системи МВС України новими обов'язковими вимогами, що дозволить користувачам створювати надійні паролі та майже уникнути можливість неправомірного використання зловмисниками правами доступу поліцейських до баз даних.

Література

1. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20.10.2005. № 1497/2005. URL: http://zakon3.rada.gov.ua/laws/show/1497/2005.

2. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12.10.2009 № 436. URL: http://zakon3.rada.gov.ua/laws/show/z1256-09/conv.

3. Про Національну поліцію: Закон України. URL: http://zakon3.rada.gov.ua/laws/show/580-19/page.

УДК 351.86(477)

Карпенко О.В.
доктор наук з державного управління
Національна академія державного управління
при Президентові України

СУЧАСНІ БЕЗПЕКОВІ ІМПЕРАТИВИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

Необхідний рівень національної безпеки країни забезпечується шляхом впровадження вітчизняної інноваційної системи освоєння нових ресурсних джерел та модернізації державної влади. Першочерговим завданням є реалізація новітніх правових, інституційних та інформаційних механізмів забезпечення національних інтересів України. Національна безпека є базовим гарантом розвитку будь-якої держави. В умовах зростання зовнішніх викликів та хронічної соціальної кризи, яка спостерігається в українському суспільстві, особливої актуальності набуває проблема забезпечення національної безпеки у такій специфічно важливій сфері, як інформаційна безпека держави. Сьогодні все українське суспільство чинить активний спротив руйнівним діям деструктивної пропаганди Російської Федерації, натомість інформаційна інфраструктура органів державної влади та особовий склад державних військових формувань все частіше стають об’єктом застосування інформаційної зброї під час здійснення агресором спеціальних інформаційних операцій.

Однією з актуальних загроз національним інтересам та національній безпеці в інформаційній сфері, яку визначено у Доктрині інформаційної безпеки України [1, с. 8], є неефективність державної інформаційної політики та недосконалість законодавства стосовно регулювання взаємодії в інформаційній сфері, що гальмує можливості усього українського суспільства єдиним фронтом протистояти зовнішньому ворогу. Під державною інформаційною політикою в жодному разі не мається на увазі виключно регулююча діяльність державних органів. Необхідність зміни змісту системи публічного управління визначається змінами нових інформаційних технологій парадигми відносин "надавач – споживач", що означає перегляд взаємодії держави з громадянами як з клієнтами і партнерами [2, с. 105].

Ефективна взаємодія органів публічної влади та громадянського суспільства в процесі формування та реалізація державної інформаційної політики сприятиме залученню новітніх засобів ведення інформаційної війни проти руйнівних впливів Російської Федерації. Так, разом із заходами оборонного характеру проти агресора, що

намагається домінувати в інформаційному просторі України, необхідно використовувати наступальні інформаційні операції. На нашу думку, внутрішня і зовнішня вітчизняна інформаційна політика у сфері захисту державних (національних) інтересів повинна радикально змінитись шляхом відмови від виключно оборонних засад.

Сучасні геополітичні реалії України свідчать про неефективність методів офіційного спростування представниками влади тієї чи іншої інформації що потрапляє у ЗМІ. Необхідно проводити заходи активної протидії інформаційним кампаніям проти України шляхом застосування наступальних інформаційних операцій (інформаційних атак та інформаційних диверсій).

Інформаційна атака є актом агресивного застосування інформаційної зброї під час проведення інформаційної операції. За типологією інформаційних операцій інформаційна війна має наступальний та оборонний характер та несе безпосередню або опосередковану інформаційну загрозу безпеці та інтересам її учасників [3, с. 310].

Прикладом інформаційних атак, які успішно може застосовувати Україна є так звані "мем-технології" в процесі реалізації певної інформаційної кампанії. Так, наприклад, загальновідомий у всьому світі мем-слоган "Хто не скаче, той…" (зокрема, в Боснії – "… не боснієць", в Чілі – "… не чилієць", у Франції – " … не француз", в Португалії – "… іспанець", в Україні "… москаль") відтепер використовується і в Російській Федерації як "… той ведмідь", що відверто спрямовано проти діючого режиму та поширюється опозицією для згуртування в конфліктах із владою. В умовах стрімкого розвитку інформаційно-комунікативних технологій, наступальні інформаційні операції в рамках спрямованих інформаційних кампаній повинні стати дієвим інструментом ведення сучасної інформаційної війни проти будь-яких супротивників, які намагаються дезорганізувати державне управління, загрожують національній безпеці, зазіхають на територіальну цілісність та незалежність України.

Література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" : Указ Президента України від 25 лют. 2017 р. № 47/2017 // Офіц. вісн. України. – 2017. – № 20. – Ст. 554. – С.8.

2. Куйбіда В.С. Муніципальне управління: аспект інформатизації / В.С. Куйбіда – К.: Знання, 2004. – 357 с.

3. Карпенко О.В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : дис... д-ра наук з держ. упр.: спеціальність 25.00.02 "Механізми державного управління" / Карпенко Олександр Валентинович; Нац. Акад. держ. упр. при Пре-

зидентові України. – К., 2016. – 466 с.

УДК 35.078

Куроєд В.В.
Державна прикордонна служба України

ЗАСОБИ МАНІПУЛЯЦІЙ В ІНФОРМАЦІЙНІЙ ВІЙНІ

Явище інформаційної війни являє собою надзвичайну зацікавленість і широке поле для вивчення спеціалістами різних галузей. Інформаційна війна – дії, спрямовані на досягнення інформаційної переваги, підтримку національної воєнної стратегії шляхом впливу на інформацію і інформаційні системи супротивника при одночасному забезпеченні безпеки і захисту власника інформації [1, с. 216]. Досягнення інформаційної переваги безпосередньо пов'язане з впливом на масову свідомість і суспільну думку.

Важко сказати, хто коли вперше використав сам термін інформаційної війни і прирівняв інформаційне протиборство до низки інших війн. Ще в Древньому Китаї даний підхід був включений до мистецтва таємного управління супротивником. Це мистецтво передавалось від покоління до покоління і ретельно від усіх приховувалось. Зміст порад китайського полководця і стратега Сунь-Цзи, спрямованих до представників влади, полягав у тому, що супротивника потрібно вводити в оману за допомогою різноманітних прийомів, а після цього нападати на нього [3, с. 43]. Також неможливо сказати, коли саме інформацію стали використовувати в якості «зброї», але якщо враховувати початком перший задокументований випадок, то один з таких – події часів Кримської війни, коли після Синопської битви 30 листопада 1853 року англійські газети писали, що росіяни дострілювали тих поранених турків, що плавали у морі [2, с. 273].

Для ведення успішної інформаційної війни потрібні два важливих атрибути – «зброя» і той, хто буде ефективно управляти нею. В якості першого атрибута виступають різні засоби маніпуляції і прийоми впливу на свідомість. В якості другого – джерела (суб'єкти), які доносять інформацію до адресата (об'єкта). Як правило суб'єктом другого атрибута виступають засоби масової інформації.

С.Г. Кара-Мурза узагальнив основні засоби маніпуляцій, які, як правило, використовуються в інформаційній війні. До них, зокрема, належать: 1) використання переконання; 2) штучне затемнення «картинки реальності» в ЗМІ, подання суперечливої, недостовірної і за-

відомо упередженої інформації; 3) перенесення приватного факту в сферу загального, в систему; 4) використання чуток, домислів, тлумачень в незрозумілій політичній чи соціальній ситуації; 5) метод під назвою «потрібні трупи»; 6) метод «страшилок»; 7) замовчування одних фактів і висвітлення інших; 8) метод фрагментації; 9) багаторазові повтори або «метод Гебельса»; 10) метод абсолютної брехні – «чим жахливіша брехня, тим легше в неї вірять»; 11) створення неправдивих подій, містифікація; 12) підміна фактів гарними гаслами; 13) метод дисонансу: просунення альтернативних фактів, цінностей і уявлень, що порушують механізм трансляції історичної пам'яті, загальні символи і цілісність цільової групи [2, с. 364].

Водночас, метою будь-яких дій в інформаційній війні є вкидання інформації і переконання суспільних мас в її достовірності, тож кожен акт ведення таких інформаційних війн завжди передбачає використання першого методу – переконання.

Також популярним є метод підміни фактів гаслами, який активно використовувався і використовується для підтримки революцій. Самими відомими прикладами є Велика Французька революція з всесвітньо відомим гаслом «Свобода, рівність, братерство» і Революція 1917 року з гаслами «Мир – народам», «Земля – селянам», «Фабрики – робітникам».

Отже, інформаційна війна існувала з найдавніших часів, хоча на той час і не мала таких масштабів, яких набула в XXI столітті. Сьогодні інформаційна війна стала невід'ємною частиною будь-якого конфлікту або зіткнення інтересів політичних еліт. Прийоми маніпуляцій, що в них застосовуються мають бути використані грамотно, бо інакше вони можуть бути спрямовані проти того, хто їх використовує.

Література:

1. Борисов А.Б. Большой юридический словар. Москва, 2012. 848 с.

2. Кара–Мурза С.Г. Революция на експорт. Москва, 2006. 525 с.

3. Сунь-Цзы. Искусство войны / пер. с англ. Н. Рыбальченко; под ред. Т. Клири. София, 2008. 192 с.

УДК 004.5

Ланде Д.В.
доктор технічних наук,
старший науковий співробітник
Інститут проблем реєстрації інформації НАН України
Бойченко А.В.
Інститут проблем реєстрації інформації НАН України

ПОБУДОВА МОДЕЛІ РОЗВИТКУ СИТУАЦІЇ НА ОСНОВІ АНАЛІЗУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Важливою складовою аналітичної діяльності є сценарний аналіз, який дає можливість дослідити, наскільки істотними виявляється вплив того чи іншого показника на кінцеву ситуацію. Для вирішення задачі пропонується наступна методика:

1 Формування репрезентативного текстового корпусу із вибраного для аналізу масиву інформаційних повідомлень.

2 Виявлення термінологічної основи моделі. Отримані терміни складаються з одного, двох (біграм) чи трьох (триграм) слів. Мережа термінів описується за допомогою матриці інцидентності [1].

3 Зважування термінів за допомогою модифікованого алгоритму HITS.

Для всіх термінів обраховуються взаємопов'язані показники авторства (auth) та портальності (hub) з використанням модифікованого алгоритму HITS [2]. Оскільки у отриманій мережі можуть існувати двонаправлені зв'язки між вузлами, які можуть мати як додатний так і від'ємний показник ваги ребра, оригінальний HITS застосовуватися не може. Модифікація алгоритму передбачає при розрахунку значення ваги кожного вузла враховувати вагу ребер, а для зниження впливу нерівномірності розподілу значень ваги на результат множити на монотонно-зростаючою та менш круту за лінійну функцію. Прикладом такої функції є функція логарифма, обчислення показників відбувається наступним чином:

$$hub(A_i) = \sum_{A_i \to A_j} auth(A_j) f(w_{ij}),$$
$$auth(A_i) = \sum_{A_j \to A_i} hub(A_i) f(w_{ij}).$$

Тут w_{ij} – вага зв'язків між вузлами A_i та A_j, відповідно w_{ji} –між A_j та A_i.

4 Ранжирування слів та організація мережі природних ієрархій або Language-network. Автоматизований аналіз термінів, включення важливих термінів до моделі у якості вузлів мережі. Для цьому етапі, для отримання необхідним є залучення експертів для побудови зв'язків між термінами отриманої мережі.

Визначення напрямків зв'язків, побудова моделі когнітивної карти.

5 Зважування вузлів мережі. Інтеграція ваги термінів. (HITS, Gephi). Візуалізація мережі та обчислення основних характеристик (довжина шляху) , виконується за допомогою засобів програмного продукту Gephi.

6 Надання власної семантики мережі та її подальше корегування виконується за допомогою Protégé - сучасного програмного пакета з відкритим вихідним кодом, призначений для розробки онтологій і систем управління знаннями. Опис об'єктів мережі використовується засобами OWL (Ontology Web Language). OWL використовує ширшу систему типів порівняно з попередніми подібними мовами. Це дозволяє визначати унікальність та визначати еквівалентність термінів предметної області.

Отримана когнітивна карта являє собою знаковий орієнтований граф:

G = <V, E >, де V — множина вершин $V_i \in V$, i = 1, 2,..., k, які є елементами досліджуваної системи; E — множина дуг $e_{ij} \in E$, i, j = 1, 2,..., N, які відображують взаємозв'язок між вершинами V_i та V_j; вплив V_i на V_j може бути позитивним, негативним, чи бути відсутнім [3, 4].

7 Розрахунок взаємного впливу вузлів мережі виконується наступним чином: $S_{\alpha\beta} = \frac{1}{d_{\alpha\beta}} \langle V \rangle$.

Для перевірки методики було проведене формування текстового корпусу з інформаційних Інтернет за темою brexit. За результатами досліджень було виявлено терміни з більшим значення auth, зокрема: "minister theresa may", "british prime minister", "comey confirms fbi", "minister david cameron", "leader nigel farage", "pull brexit trigger". Терміни з найбільшим значенням hub: "brexit", "eu", "uk", "may", "european", "minister".

За результатами описаних досліджень побудовано сценарну модель інформаційного простору. Запропонована методика дозволяє в автоматизованому режимі, на базі аналізу вхідного пакету документів, вирішити задачу розробки та дослідження сценаріїв інформаційного впливу на об'єкти, які відповідають вибраним ключовим поняттям. Методика може використовуватись для виявлення різноманітних аспектів інформаційної безпеки.

Література

1. Додонов А.Г., Ландэ Д.В., Коваленко Т.В. Модели предметных областей в системах поддержки принятия решений на основе мониторинга информационного пространства. Открытые семанти-

ческие технологии проектирования интеллектуальных систем (OSTIS-2016): материалы VI междунар. науч.-техн. конф. (Минск 18-20 февраля 2016 года) - Минск: БГУИР, 2016. - С. 171-176.

2. Kleinberg J. Authoritative sources in a hyperlinked environment // Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, Philadelphia, PA, 1998. – P.668–677.

3. Снарский А.А., Ланде Д.В., Зоринец Д.И. Ранжирование понятий, извлекаемых из потоков сетевых новостей. Информационные технологии и безопасность. Материалы XVI Международной научно-практической конференции ИТБ-2016. - К.: ИПРИ НАН Украины, 2017. - С. 130-131.

4. Ландэ Д. В. Подход к созданию терминологических онтологий / Д. В. Ландэ, А. А. Снарский // Онтология проектирования, 2014. – № 2 (12). – С. 83–91.

УДК 354.42

Левченко О.В.
кандидат військових наук, професор
Житомирський військовий інститут ім. С. П. Корольова

ВИЗНАЧЕННЯ СТРУКТУРИ МЕТОДИКИ ВИЯВЛЕННЯ, АНАЛІЗУ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ ДЕРЖАВІ У ВОЄННІЙ СФЕРІ

Оцінка інформаційних загроз національній безпеці України у воєнній сфері передбачає:

виявлення негативного іноземного інформаційного впливу (далі – ІВ) на особовий склад Збройних Сил нашої держави, його аналіз за якісними і кількісними показниками, визначення на основі базових показників цього впливу (інтенсивності, тривалості, поширеності джерел, масштабності об’єктів впливу) форми інформаційної боротьби;

виявлення наявності інформаційних загроз державі у воєнній сфері та визначення рівня цих загроз.

Виходячи з цього, розроблена Методика виявлення, аналізу та оцінювання інформаційних загроз державі у воєнній сфері (далі – Методика) складається з двох блоків (часткових методик): блоку виявлення негативного інформаційного впливу (рис. 1) і блоку аналізу інформаційних загроз державі у воєнній сфері та оцінювання їх рівня (рис. 2).

Виходячи з того, що до виникнення інформаційних загроз інформаційно-психологічного характеру призводить цілеспрямований,

ЕТАП 1.
Виявлення ознак негативного ІВ:
- виявлення фактів поширення повідомлень з ознаками маніпулювання щодо об'єктів впливу;
- визначення об'єктів впливу;
- встановлення першоджерел розміщення та авторів матеріалів з ознаками маніпулювання;
- уточнення переліку критичних тем

↓

ЕТАП 2.
Формування інформаційного потоку за:
- критичними темами;
- темами, визначеними під час поточного моніторингу;
- об'єктами, на які спрямований ІВ;
- повідомленнями з різко негативною тональністю, лінгвістичними ознаками маніпулювання;
- джерелами, які раніше використовувалися для проведення заходів ІВ;
- авторами, які раніше залучалися для проведення ІВ;
- датами, часом перебігу подій, які потребують подальшого аналізу

↓

ЕТАП 3.
Виявлення змістовних ознак маніпулювання у досліджуваному потоці:
- аналіз критичних тем;
- вивчення тональності (позитивна, негативна, нейтральна) повідомлень;
- виявлення лінгвістичних ознак маніпулювання

↓

ЕТАП 4.
Виявлення організаційних ознак маніпулювання:
- аналіз дублікатів;
- аналіз взаємозв'язків між об'єктами, темами, джерелами, авторами повідомлень, що містять змістовні ознаки маніпулювання

↓

ЕТАП 5.
Визначення заходів негативного ІВ:
- узагальнення інформації, отриманої на попередніх етапах, зіставлення з невербальною інформацією, відомими фактами, подіями;
- формулювання переліку заходів ІВ;
- визначення початку (закінчення) заходів ІВ

Рис. 1. Блок виявлення негативного інформаційного впливу

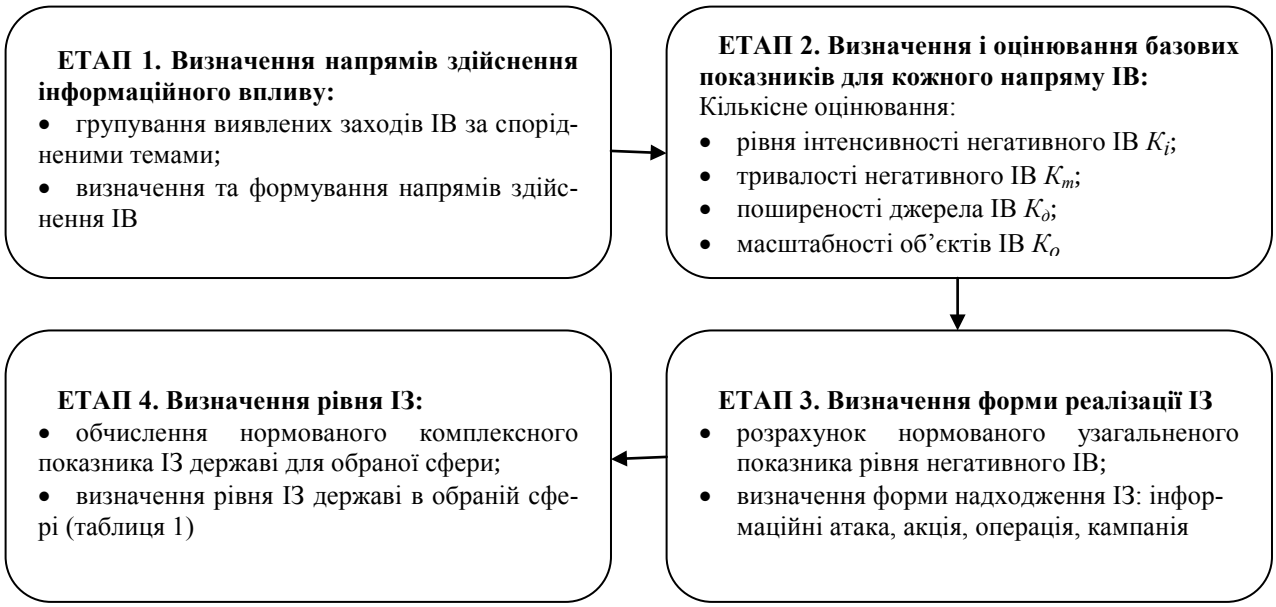

Рис. 2. Блок аналізу інформаційних загроз державі у воєнній сфері та оцінювання їх рівня

тобто спеціально організований, інформаційний вплив з боку супротивної держави [1], слід вважати, що такий організований вплив може проводитись лише за заздалегідь визначеними планами у вигляді певних форм ведення інформаційної боротьби. Тому у Методиці прийнято, що інформаційна загроза інформаційно-психологічного характеру може надходити у формі інформаційної атаки, інформаційної акції, інформаційної операції, інформаційної кампанії.

У підсумку для визначення рівня ІЗ у воєнній сфері спочатку обчислюється нормований комплексний показник ІЗ державі $\overline{Z_k^c}$, який потім зіставляється зі значеннями, наведеними нижче у таблиці 1.

Таким чином, у Методиці рівень інформаційної загрози вимірюється дискретно від 0 до 1 з кроком 0,25 і має такі значення: низький, підвищений, високий, критичний.

Таблиця 1. Значення показників рівня інформаційної загрози

Межі значень показника рівня ІЗ	Показник рівня ІЗ
0 – 0,25	низький
0,26 – 0,5	підвищений
0,51 – 0,75	високий
0,76 – 1,0	критичний

Література

1. Панченко В.М., Полевий В.І. Методика виявлення ознак інформаційного впливу в засобах масової інформації // Інформаційна безпека людини, суспільства, держави. 2011. № 3(7). С. 70–77.

УДК 378(477)(094)

Мамченко С.М.
доктор педагогічних наук, професор
Національна академія Служби безпеки України

ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА СУЧАСНОМУ ЕТАПІ РЕФОРМУВАННЯ СИСТЕМИ ВИЩОЇ ОСВІТИ УКРАЇНИ

Революційні події, що відбулися у нашій державі з осені 2013 року призвели до кардинальних змін різних сфер суспільного життя. Впровадження європейського досвіду побудови правового базису, державних інституцій та економіки закономірно призводять до змін на ринку праці, а відповідно й сфери академічної і професійної освіти. У цьому напряму зроблено багато новацій, починаючи від прийняття та впровадження нового Закону України «Про вищу освіту», Національної рамки кваліфікацій тощо. Природним наслідком нормотворчих напрацювань стало прийняття у 2015 році нового переліку освітніх галузей та спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах України (Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266 (далі – Перелік-266).

У період з початку 2000-х років до 2015 року в системі вищої освіти України існувала галузь знань “Інформаційна безпека”, в рамках якої здійснювалася підготовка фахівців у сфері забезпечення інформаційної безпеки. Основними завданнями професіонала з інформаційної безпеки (Національний класифікатор України “Класифікатор професій” ДК 003:2010, Довідник кваліфікаційних професій працівників “Безпека господарської діяльності підприємства, установи, організації”, погоджений Міністерством соціальної політики України від 11.10.2011 року) є забезпечення безпеки інформаційного простору (комунікативних каналів впливу на масову та індивідуальну свідомість, психологічний та психічний стан громадян), а також забезпечення безпеки інформаційних ресурсів, що містять інформацію з обмеженим доступом.

Ставлячи собі за мету привести Перелік спеціальностей до положень Міжнародної системи кваліфікації освіти автори, на жаль, забули врахувати досвід вітчизняної системи вищої освіти, яка на той час вже розвивалася 24 роки і мала власні напрацювання. Механістичне застосування міжнародної класифікації без врахування вітчизняного ринку праці та освіти, призвело до звуження освітньої га-

лузі «Інформаційна безпека», яка складалася з трьох різнорідних спеціальностей, до одної – «Кібербезпека», включеної до освітньої галузі «Інформаційні технології». Ці зміни, на жаль, призводять до втрати зв'язку із ринком праці та оманою користувачів освітніх послуг, оскільки назва «кібербезпека» не відповідає фактичному змісту спеціальності. Названа спеціальність, що розкривається через визначені у проекті стандарту вищої освіти, відображає професійну діяльність з кіберзахисту. Кібербезпека як діяльність значно ширша та включає, наприклад, таку сферу як контррозвідувальна безпека кіберпростору. З огляду на проекти відповідних стандартів вищої освіти (www.mon.gov.ua), зорієнтовано на підготовку фахівця суто технічного спрямування, що не повною мірою відповідає професійно-кваліфікаційним характеристикам фахівців з інформаційної безпеки та вимогам сьогодення.

Поза нововведеною спеціальністю залишилися питання нормативно-правового регулювання побудови систем захисту інформації та вельми актуальних сьогоденних питань інформаційного спротиву, що включалися до спеціальності «Управління інформаційною безпекою». Таким чином, на нашу думку, була розірвана єдність професійної підготовки, яка існувала в освітній галузі «Інформаційна безпека». Гуманітарна складова інформаційної безпеки була втрачена як цілісна підготовка, а отже питання інформаційного спротиву та інформаційно-психологічного протиборства, побудови комплексних систем захисту інформації та систем управління інформаційної безпеки стали другорядними у підготовці фахівців за іншими спеціальностями.

Водночас, державою проведено низку законодавчих заходів щодо розмежування інформаційної та кібернетичної безпеки. Указами Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" та Указом Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» визначено основні завдання у цих сферах.

Національна академія Служби безпеки України накопила великий досвід із підготовки випускників із здатністю вирішувати завдання у сфері інформаційної безпеки саме гуманітарної складової із добре сформованими компетентностями для побудови як інформаційного, так і комп'ютерного просторів за сучасними моделями свобідного світу із повагою до честі, гідності особи.

Одним із перспективних напрямів підготовки фахівців із кібернетичної безпеки у напрямку її менеджменту Академія розглядає

навчання за спеціальністю «Кібернетична безпека» за спеціалізацією «управління інформаційною безпекою». Наші випускники на основі ґрунтовної підготовки за визначеними у стандарті вищої освіти компетентностями формуватимуть системи захисту критичної інфраструктури кіберпростору, спроможні організувати її безпекову діяльність.

Другий напрям розвитку нашого досвіду підготовки випускників Академії за проблематикою інформаційна безпека є формування фахівців із захисту інформації, інформаційного протиборства, формуванню інформаційних наративів та контентів тощо. Разом з тим, намагання перенести вказаний досвід підготовки шляхом впровадження спеціалізації «захист інформації з обмеженим доступом» спеціальності «менеджмент» показує значні складнощі синергії через різнорідні об'єкти діяльності, що зумовлено різним історичним розвитком спеціальностей, орієнтацією на суттєво різні сфери, об'єкти та суб'єкти діяльності.

Зокрема, події останніх років засвідчили, що прогалини в системі забезпечення інформаційної безпеки та охорони державної таємниці, у тому числі брак висококваліфікованих фахівців, значною мірою сприяли російському агресору в реалізації планів щодо впливу на соціальні, економічні та політичні сфери розвитку нашої держави, а також анексії українських територій, що зумовило прийняття керівництвом держави низки першочергових стратегічних рішень. Так, у Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.2015 № 287, Воєнній доктрині України, затвердженій Указом Президента України від 24.09.2015 № 555, рішенні РНБО України від 28.04.2014 "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", введеному в дію Указом Президента України від 01.05.2014 № 449/2014, рішенні РНБО України від 06.05.2015 року "Про стратегію національної безпеки України", введеному в дію Указом Президента України від 26.05.2015 № 287/2015, наголошується на зростанні впливу інформаційних сил і засобів на воєнно-політичну обстановку в регіоні довкола України та необхідності вдосконалення професійної підготовки фахівців із забезпечення інформаційної безпеки як одного з пріоритетів забезпечення національної безпеки.

Сучасний світ передових комунікаційних технологій, які дозволяють формувати єдину світову спільноту, за гуманістичними принципами отримав виклик темного минулого, коли людина стає лише сірою масою. Маніпуляційний вплив на демократичні вибори шляхом використання технологій «BIG DATA», накопичення вели-

кого обсягу персональних даних потребують напрацювань із протидії. Саме тому підтримуємо заборону на використання соціальних мереж, що контролюються країною агресором.

Ситуація, що склалася, зумовила ініціативу Служби безпеки України перед Міністерством освіти і науки України на введення нової спеціальності «Національна безпека» (за сферами та видами діяльності) у галузі «Військова освіта, національна безпека, безпека державного кордону». У лютому 2017 року Постановою КМУ названа спеціальність і введена до Переліку спеціальностей. Обрана назва спеціальності була компромісом між потребою збереження підготовки фахівців з інформаційної безпеки та потребою у підготовці спеціалістів різних міністерств та відомств безпекового сектору України.

Звісно, намагання об‘єднати в одній спеціальності подібні за сферою діяльності вже є суттєвий позитивний крок вперед, однак залишається питання узгодження в одному стандарті вищої освіти різних об’єктів та суб’єктів діяльності.

На нашу думку, виклики, що стоять перед нашою державою у захисті територіальної цілісності, державного суверенітету та боротьби з агресором призведе до формування потреби у фахівцях-професіоналах із стратегічних комунікацій, побудови та захисту інформаційного простору держави, кібернетичного захисту й кібернетичної безпеки тощо. Враховуючи наміри МОНУ розробити до 2021 року проекту нової редакції ЗУ «Про вищу освіту» на основі Стратегії розвитку вищої освіти (до 2030 року), перед нами стоять завдання із включення до названої Стратегії окремим розділом підготовку фахівців із інформаційної та кібернетичної безпеки.

УДК 351.86: 004

Марутян Р.Р.
кандидат історичних наук, доцент
Національна академія державного управління
при Президентові України

БІО-ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В КОНТЕКСТІ БЕЗПЕКИ ЛЮДИНИ: ДЕРЖАВНО-ПРАВОВИЙ ВИМІР

Глобалізаційний розвиток світу стає причиною появи нових технологій, які здійснюють вплив на всі сторони життя сучасної людини. Але революційні прориви в галузі нових біо-та інформаційних технології не тільки облегшують життя людини, але й ставлять питання щодо її безпеки.

Держава використовує такий інструмент біотехнології, як біомет-

рія - розпізнавання особи по її природним біологічним характеристикам, які є індивідуальними для кожної людини (наприклад, голос, почерк, відбитки пальців, малюнок веселкової оболонки ока, ДНК).

Згідно з Технічним звітом Міжнародної організації цивільної авіації (ІКАО) «Про включення засобів біометричної ідентифікації в машино розраховані проїзні документи» поняття «біометрія» або «біометрична ідентифікація» означає автоматизовані засоби розпізнавання живої людини за допомогою виміру фізіологічних або поведінкових характеристик».

Біометрія як інструмент державно-правової управлінської технології має внутрішньополітичний та зовнішньополітичний виміри: біо-паспорти, біометричні візи, біометричні водійські права, чипізація мігрантів, ID-картки тощо.

Перш за все, використання нових технологій ідентифікації людини було покликане забезпечити національну безпеку держав від нових викликів і загроз - транснаціонального тероризму, нелегальної міграції і організованої злочинності.

В той же час, слід визнати, що впровадження біометричних технологій у візової політиці країн не стало запобіжником до актів міжнародного тероризму.

У 2016 році Білл Ґейтс в своєму виступу в Royal United Services Institute, розташованому в Лондоні, виступив з попередженнями щодо небезпеки біологічного тероризму. Він заявив, що терористи за допомогою штучно створених в лабораторіях мікробів і вірусів здатні знищити близько 30 мільйонів осіб менше, ніж за рік.

У листопаді 2016 року Рада президента з науки і техніки США (PCAST) направила лист президенту Бараку Обамі з попередженням про появу нових форм біотероризму. «У той час, як розвиток біотехнологій є великим благом для суспільства, воно також має серйозний потенціал для деструктивного використання», - написали члени Ради. Вчені були стурбовані тим, що нова техніка під назвою CRISPR тепер дешева і широко доступна. Ця техніка може редагувати код ДНК і замінювати його новими генами. Є побоювання, що в неправильних руках процедура може породити небезпечні штами бактерій або інших організмів.

Таким чином, сьогодні ефективність біометричних технологій в контексті забезпечення зовнішньополітичної безпеки представляється спірною. Розвиток сучасних інформаційних технологій дозволяє обійти систему безпеки нових біометричних паспортів, що ставить перед інформаційною безпекою нові завдання.

Внутрішньополітичний вимір біометрії має наступні характеристики та несе таки загрози особистої безпеки та правам людини та

громадянина:

– **тотальний контроль та стеження за людиною.** На думку правозахисників, біометричні технології загострюють питання щодо прав людини.

– **втручання в приватне життя громадян.**

– **проблема збереження баз біометричних даних громадян**. Уряди держав вводячи біометрію в умовах відсутності законодавчого регулювання даної сфери діяльності не несуть відповідальності за зберігання даних.

– **вплив біометричних технологій на здоров'я людини.**

– **управління людиною через чіпізацію.**

Сьогодні, на законодавчому міжнародному рівні практично відсутні спеціальні нормативні акти, регулюючі правові принципи вживання біометрії відносно прав і свобод людини. Звернення громадян до суду щодо порушення їх прав в цьому питанні є поодинокими та завершуються не на користь останніх. Так у жовтні 2013 р. громадянин Німеччини М.Шварц звернувся до суду ЄС, після того, як йому відмовили у видачі паспорта без обов'язкової процедури здачі відбитків пальців. Суд визнав, що здача і зберігання відбитків йде врозріз з основними правами і свободами, представляє загрозу для приватного життя і збереження персональних даних, проте мета підвищення рівня безпеки виправдовує подібні заходи.

Слід зауважити, що у біометрії є свої прихильники, які вважають що біометричні ID-картки дисциплінують людей і служать громадській безпеці.

Висновок. Постіндустріальне суспільство породжує нові інформаційні виклики і загрози безпеці людини. Однією з таких загроз стає використанням біометричних технологій в управлінської практиці сучасних держав. Саме тому актуальним завданням сьогодення є контроль інститутів громадянського суспільства на національному та міжнародному рівнях над процесами використання біометричних технологій. Це повинно бути партнерство представників науки, бізнесу, громадських об’єднань, яке дозволить контролювати дії держави у цієї сфері та врахує питання особової безпеки людини та громадянина.

Література

1. Білл Ґейтс попередив про загрозу нового виду тероризму. – Режим доступу: http://tyzhden.ua/News/190667

2. Opinion on Ethical Aspects of Patenting Inventions Involving Human Stem Cells. URL: http://europa.eu.int/comm/ european_group_ethics/docs/avis16_en.pdf.

УДК 681.3

Меленті Є.О.
кандидат технічних наук
Білецький С.В.
кандидат технічних наук, доцент
Інститут підготовки юридичних кадрів для СБУ Національного юридичного університету імені Ярослава Мудрого

РЕКОМЕНДАЦІЇ ЗІ ЗМІЦНЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аналіз війн та військових конфліктів останніх десятиліть свідчить, що для вирішення політичних амбіцій, територіальних претензій суміжних держав дедалі більше ворогуючі сторони разом з традиційними способами веденням бойових дій застосовуватимуть політичні, економічні, інформаційні заходи. В сучасній теорії військового мистецтва таку концепцію ведення бойових дій називають «гібридною війною», кінцеві цілі якої досягаються шляхом проведення інформаційних, кібернетичних операцій в поєднанні з діями збройних сил, спеціальних служб та інтенсивним політичним й економічним тиском. Відбувається трансформація класичного поняття поле бою в бойовий простір, в якому противник може з’явитися в будь-якому місці та застосувати непередбачувану технологію нападу. Найімовірніше на початковому етапі домінуватимуть інформаційні спеціальні операції щодо дестабілізації внутрішньої суспільно-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в країні (окремої території), атаки в кібернетичному просторі спрямовані на порушення роботи автоматизованих систем державного та військового управління, об'єктів критичної інформаційної інфраструктури.

Досвід останніх суспільно-політичних подій, що відбувалися в Україні, досить яскраво показав, що для забезпечення національної безпеки в інформаційній сфері слід більше приділяти уваги захисту важливих інформаційних ресурсів, баз даних держави, що містять інформацію з обмеженим доступом, зокрема технічному захисту.

До однієї з основних загроз безпеці інформації належить виток інформації технічними каналами. При цьому відбувається поширення інформативного сигналу через фізичну середовище від джерела корисного сигналу до приймача технічного засобу розвідки, що здійснює перехоплення інформації.

Постає актуальним питання адекватної відповіді сучасним викликам та загрозам в інформаційному просторі. Саме тому, для зміцнення інформаційної безпеки в оборонній, науково-технічній та

економічній сферах нашій державі доцільно розвивати наступні напрямки діяльності:

1) врегулювання національної нормативно-правової бази, яка б відповідала вимогам, що висуваються сучасним рівнем розвитку технологій; адаптація вітчизняного законодавства до правового поля провідних країн світу;

2) участь у міжнародних організаціях по боротьби з кіберзлочинністю, кібершпигунством;

3) якісна підготовка та забезпечення висококваліфікованими фахівцями підрозділів по боротьби з кіберзлочинністю в правоохоронних органах України;

4) підвищення рівня кваліфікації користувачів інформаційно-телекомункаційних систем, в яких циркулює інформація з обмеженим доступом;

5) організація взаємодії і координація зусиль правоохоронних органів та військових формувань, судової системи, забезпечення їх необхідною матеріально-технічною базою;

6) удосконалення технічного захисту інформації з обмеженим доступом в інформаційно-телекомункаційних системах, розголошення якої загрожує національній безпеці та обороні країни; розробка (модернізація) та виробництво на державних підприємствах сучасних спеціальних технічних та програмних засобів з технічного захисту інформації.

УДК 354.42

Небава М.І.
кандидат економічних наук, професор,
Вінницький національний технічний університет
Міронова Ю.В.
кандидат економічних наук,
Вінницький національний технічний університет

ІНТЕГРАЛЬНИЙ ПІДХІД ДО ОЦІНЮВАННЯ РІВНЯ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Сучасні глобалізаційні та динамічні процеси розвитку цивілізації, посилення зовнішньої інформаційної агресії, а також жорстка конкуренція у контексті євроінтеграції вимагають забезпечення від служб безпеки посиленої охорони інформаційного простору [1]. Також визначальним є організація режиму безпеки та здійснення всіх видів діяльності, які забезпечують інформаційну та кібербезпеку.

Мета дослідження полягає у розробці інтегрального методично-

го підходу до оцінювання рівня захисту інформаційного простору, що уможливить покращення якості управлінського процесу.

Рівень інформаційної безпеки залежить від спроможності уникати загроз і ліквідовувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища [2]. Ефективним управлінським рішенням передує глибокий аналіз та оцінка предмету дослідження [3]. Отже, необхідною задачею для кожного управлінського апарату є оцінювання рівня власної безпеки. Процес оцінювання безпеки представляє собою систему реалізації ряду функцій. Задача полягає у знаходженні ряду показників та функцій перетворення, на основі яких буде складена система оцінки.

Основна проблема оцінки безпеки полягає у тому, що її неможливо оцінити, враховуючи вузьке коло початкових показників, або на основі єдиного показника. Оцінка має відображати усі сторони загроз і ризиків для суб'єкта. Також вхідні показники мають бути зрозумілими та доступними для відображення у моделі.

Враховуючи представлені критерії було розроблено алгоритм оцінювання безпеки інформаційного простору (рис 1).

I етап: Вибір множини *T* лінгвістичних термів, які складаються з сукупності лінгвістичних змінних

↓

II етап: Вибір графіків функцій належності $\mu^{Б}$ μ^{Ej}, $j=\overline{1,J}$

↓

III етап: Визначення математичних формул, які описують функції належності $\mu^{Б}$ μ^{Ej}, $j=\overline{1,J}$

↓

IV етап: Побудова таблиці значень для оцінювальних параметрів ($x_{11},\ldots,x_{nm}$,)

↓

V етап: Опис логічних рівнянь функції належності для параметрів ($x_{11},\ldots,x_{nm}$,)

↓

VI етап: Розробка матриці знань для оцінки груп $f_1,\ldots, f_n$ параметрів оцінки та для визначення підсумовуючої оцінки

↓

VII етап: Опис розроблених матриць логічними рівняннями, які встановлюють зв'язок між $f_1,\ldots, f_n$

Рисунок 1 − Етапи оцінювання безпеки інформаційного простору
Джерело: авторська розробка

Згідно представленої схеми, початком процесу є вибір лінгвістичних термів, які будуть відображати рівень безпеки. Далі, використовуючи математичний апарат нечітких множин [4, 5], було складено графіки функції належності, визначено математичні формули опису функції належності. Відбір показників здійснено на основі критеріїв повноти, дієвості та мінімальності. Наступним етапом є формування матриць знань для обраних показників – здійснюється на основі методу експертних оцінок. Розроблені матриці описуються логічними рівняннями, на основі яких і отримується остаточне значення або характеристика рівня безпеки.

Отже, розроблений інтегральний методичний підхід на базі математичного апарату нечітких множин дає змогу оцінити рівень безпеки інформаційного простору, враховуючи технологічну, ресурсну, фінансову та соціальну безпеку [6]. Головна особливість розробленої моделі – обчислювальна ефективність і гарантованість результатів.

Література

1. Небава М. І. Глобалізаційні процеси та головні виклики для національного середовища України / М. І. Небава, В. О. Денисенко // Materials of the XI International scientific and practical conference, «Modern European scienze», – 2015. Volume 3. Economic science. Covernance. Political science. 2015. – С.60-61.

2. Архірейська Н. В. Економічна безпека в контексті державної стратегії України / Н. В. Архірейська // Сучасні тенденції розвитку фінансових та інноваційно-інвестиційних процесів в Україні: Матеріали міжнародної науково-практичної конференції. – Вінниця: ВНТУ, 2013. – С. 8−10.

3. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення ОВС України / О. В. Бойченко // Форум права. – 2009. – № 1. – С. 50–55.

4. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений. Москва: Мир,1976. – 167 с.

5. Ротштейн А. П. Інтелектуальні технології ідентифікації: нечіткі множини, генетичні алгоритми, нейронні мережі. Монографія / А. П. Ротштейн. – 1999. – 320 с.

6. Небава М. І. Забезпечення енергетичної, економічної та екологічної безпеки України в контексті сталого розвитку / М. І. Небава, О. В. Стрелюк // V-ий Всеукраїнський з’їзд екологів з міжнародною участю (Екологія / Ecology -2015), 23-26 вересня 2015. Збірник наукових праць. – Вінниця: ТОВ «Нілан ЛТД», 2015. – С. 277.

УДК 351:311.312

Николаєнко Г.В.
Науково-дослідний інститут
інформатики і права НАПрН України

ПРАВОВІ ЗАСАДИ РЕГУЛЮВАННЯ ПРОФЕСІЙНОЇ КОНФІДЕНЦІЙНОСТІ В ДЕРЖАВНІЙ СТАТИСТИЧНІЙ ДІЯЛЬНОСТІ

Сучасна державна статистика є складовим елементом системи державного регулювання, її інтегруюча функція значно посилюється у створенні інформаційної інфраструктури загальнонаціонального масштабу. Офіційна статистична інформація є основою для прийняття багатьох державних рішень, а тому діяльність в галузі державної статистики носить міжгалузевий характер і призначена для забезпечення державного управління в адміністративно-політичній, економічній і соціально-культурній сферах.

Необхідність збереження професійної конфіденційності первинної інформації постає перед національною статистичною практикою у зв'язку з існуючою тенденцією до систематичного використання макро- та мікроданих. Їй приділено значну увагу в статистичному законодавстві Євросоюзу, оскільки забезпечення конфіденційності даних респондентів значно підвищує рівень довіри до державної статистики, а, отже, і якість первинної інформації. Ця досить нова для національної статистики вимога може бути витримана за наявності юридичного, методологічного, організаційного та технічного забезпечення.

Законом України «Про інформацію» [1] визначається, що залежно від порядку доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом, причому будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом (ст. 20 Закону). Відповідно до Статті 21 Закону інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному порядку відповідно до передбачених ним умов, а також в інших випадках, визначених законом. У на практиці у більшості випадків конфіденційною прийнято називати інформацію комерційного, професійного або ділового характеру, незалежно від форми та способу її вираження, яка стосується, як

правило, інтересів особи і не може бути розголошена без її згоди.

Статистична конфіденційність – це особлива форма професійної конфіденційності, що стосується працівників галузі статистики. Її головний принцип полягає у переконанні осіб, котрі надають дані, які застосовуються для виробництва статистики, у тому, що ці відомості не будуть використані їм на шкоду. Статистична конфіденційність позбавляє можливості передачі третій стороні особистих даних, що збираються під час статистичних спостережень, а також розголошення даних, наданих лише з метою підготовки статистичної інформації [2, с. 57].

Принципи діяльності органів державної статистики України – це звід стандартів у галузі статистики, дотримання яких гарантує державі та суспільству, що офіційна статистична інформація розробляється і поширюється на основі професійної незалежності, неупередженості, об’єктивності, надійності, економічності та статистичної конфіденційності [3]. Відповідно до цих принципів органи державної статистики гарантують конфіденційність первинних статистичних даних, отриманих від респондентів, а також статистичної інформації, на підставі якої можна визначити інформацію щодо конкретного респондента, і адміністративних даних, що використовуються для статистичних цілей.

Згідно з Концепцією забезпечення статистичної конфіденційності [4] в органах державної статистики розрізняють такі типи конфіденційної інформації по відношенню до зовнішніх і внутрішніх суб'єктів:

- конфіденційною інформацією по відношенню до зовнішнього суб'єкта, що виступає джерелом статистичної інформації, є дані про конкретного респондента, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються згідно з їх бажанням і на передбачених ними умовах, а також інших випадках, визначених законодавством;

- конфіденційною інформацією по відношенню до внутрішнього суб'єкта є первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, які охороняються Законом України «Про державну статистику» і використовуються виключно в статистичних цілях, тобто для виробництва статистичної інформації;

- конфіденційною інформацією по відношенню до зовнішнього суб'єкта, що виступає користувачем статистичної інформації, є ста-

тистична інформація, яка дозволяє прямо або опосередковано встановити конкретного респондента та/або визначити первинні дані щодо нього.

Таким чином, проведене узагальнення правових основ регулювання професійної конфіденційності в державній статистичній діяльності дало змогу уточнити поняття «статистична конфіденційність», під яким розуміється забезпечення захисту даних стосовно статистичних одиниць, що отримуються або безпосередньо з статистичних спостережень, або з адміністративних та інших джерел, від будь-якого порушення права на конфіденційність. Це означає унеможливлення їх нестатистичного використання та незаконного оприлюднення.

Література

1. Закон України «Про інформацію». URL: http://zakon3.rada.gov.ua/laws/show/2657-12/print1493666179580645.

2. Гончар О. В. Нормативно-правове забезпечення гарантування конфіденційності в Європейській статистичній системі / О. В. Гончар, О. В. Кузьміна. // Статистика України. – 2011. – №1. – С. 57–61.

3. Наказ Державного комітету статистики України від 14.06.2010 №216. «Про затвердження принципів діяльності органів державної статистики». – [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/prc_dk/prc_ddos.htm.

4. Концепція забезпечення статистичної конфіденційності. Наказ Державної служби статистики України 28 липня 2015 року №180. URL: https://docs.dtkt.ua/download/pdf/1157.3353.1.

УДК:351.746

Остроухов В.В.
доктор філософських наук, професор
Національна академія Служби безпеки України
Величко М.В.
кандидат біологічних наук,
старший науковий співробітник
Національна академія Служби безпеки України
Салагор І.М.
Національна академія Служби безпеки України

ПРИРОДНИЙ ТА ШТУЧНИЙ ІНТЕЛЕКТИ: ЦИВІЛІЗАЦІЙНІ БЛАГА ТА ПРОБЛЕМИ

В ході еволюційного розвитку приматів - людина розумна (Homo sapiens L.) в числі шести, а то можливо, і більше підвидів

людей, (серед яких денисівці, неандертальці, еректуси та інші близькі наші філогенетичні родичі), будучи в порівнянні з іншими підвидами людини низькорослою, голою, не володіючи особливою фізичною силою, зате розумною і кмітливою знищила в конкурентній боротьбі їх всіх. Природний інтелект дав ту перевагу Homo sapiens, завдяки, якій вона пройшла кровопролитний доісторичний міжвидовий відбір, будучи на даний час єдиним представником в своєму роді. Після перемоги над іншими підвидами homo собі подібних почався етап внутрівидової боротьби sapiensa за виживання, за матеріальні, духовні та інші блага. Як історичний приклад - рабство, релігійні конфлікти, світові війни, геноцид, терор — все це витівки розуму людини. Оцінивши свою перевагу серед інших живих істот на планеті, людина протягом 70000 років розвиває і вдосконалює власний інтелект. Її постійне прагнення до фізичного та інтелектуального самовдосконалення є тим адаптаційним інструментом до протидії не тільки викликам природного середовища, але і соціального, а в майбутньому і віртуального. Вона зрозуміла, що мозок людини хоч і має великий потенціал до навчання (формування у індивіда соціальної спадковості, бо біологічну передали її батьки), і якщо «персональний людський комп'ютер» не загружати направленого характеру інформацією, то індивід залишиться десь трохи вище сучасного примата типу "мауглі". Примусове завантаження людського індивідууму суспільством (сім'я, садочок, школа тощо) мова, культура та інші знання про світ відбувається у перші 20 років життя. А потім людина, в залежності від сформованих у неї суспільних потреб, у найкращому випадку протягом всього життя самовдосконалюється. Людина зрозуміла, що не слід переоцінювати власний мозок, адже із часів першого африканського предка його розміри та і можливості особливо еволюційно не змінилися. Тому на сучасному етапі свого як еволюційного, так і соціального розвитку глобальною метою людини стало створення штучного інтелекту та його підкорення у власних цілях. Step by step (крок за кроком), опановуючи і розвиваючи нові інформаційні технології, людина наблизилася до його створення. Спочатку це були перші прості кібернетичні машини, потім комп'ютер взагалі і персональний, який динамічно гібридизується в окремі інформаційні системи. Першим вагомим етапом у створенні штучного інтелекту можна віднести протистояння із шахів в 1997 році чемпіона світу Гаррі Каспарова проти комп'ютера Deep Blue, де вперше природний інтелект програв штучному [1]. В 2011 році Девід Феруччі створює суперкомп'ютер IBM Watson, який оперує практично всією відкритою інформацією, має доступ до інтернету та навчився розуміти мовні питання людини: розрізняти підтекст,

метафору, мовну гру, тощо [2].

Це стало першим справжнім шоком для думаючої частини людства. Але самовпевненість, на думку Андрія Курпатова, людська самовпевненість взяла верх: тобто, ці машини прекрасно аналізують, але ,на відміну від людини, не думають [3]. Є ще старокитайська гра в го, де відсутні закорузлі математичні алгоритми, а гра вимагає інтуїції і бачення стратегії. Рахувалося, що перемогти в цій грі не думаючи по аналогії з людиною, неможливо і комп'ютер так думати ніколи не зможе. І ось наступив березень 2016 року. В Сеулі чемпіон світу в го Лі Седоль зіграв турнір із 5 ігор в го , в якому з рахунком 4:1 програв гугловській комп'ютерній системі AlphaGo [4]. Тобто, вперше штучний інтелект навчився думати краще ніж природний. Адже проти Лі Седоля грала не просто комп'ютерна програма, яка створена людьми, а дійсний цифровий інтелект. Все, що зробили розробники із Google для створеної ними системи AlphaGo, загрузили інформацію про ігри раніше зіграні людьми на турнірах і дали можливість йому опрацювати і потренуватися. AlphaGo зіграв мілліони партій із своїми власними копіями, поетапно вибраковуючи нежиттєздатні. В результаті цього він створив власні стратегії бачення гри в го. Так, що ніхто, включаючи і розробників, не знає, як і чому AlphaGo приймав ті чи інші рішення, і якими правилами він користувався. А звідси можливі перспективи для людства.

Це самий дійсний «чорний ящик», але уже не Скиннера, а Дугласа Лената, який першим розробив технологію цифрового природного відбору, а потім засекретив свої розробки з опаскою за наслідки власного відкриття. Фахівці із Google лиш пішли його шляхом і розробили на прикладі системи AlphaGo щось подібне [5].

Справа в тому, що вчені у сфері інформаційних технологій підійшли до передбаченого «інтелектуального вибуху». Тобто, як вони вважають наближення інформаційного апокаліпсиса. «Інтелектуальний вибух» - це розробка видатного вченого Ірвінга Джона Гуда. Гуд працював над проблемами "штучних нейронних мереж" – штучним інтелектом який програмує сам себе [6]. І на початку він вважав, що повноцінний, незалежний в саморегуляції від волі людини, штучний інтелект, до якого людство прийде, буде великим благом. Потім він усвідомив, що майбутнє людства, носія природного інтелекту після створення ним же повноцінного конкурента штучного інтелекту не таке вже і радужне. Вирішувати відповідні проблеми буде не людина, а машина, яка стане набагато розумніша за неї. І якщо штучний інтелект розвивається шляхом самоосвіти то його вже виключити як вважає Азімов, бачиться проблематично [7]. Адже, що генетичне або нейронне програмування передбачає ціль, ради якої даний інтелект

створюється. Розумна система, чи природна чи штучна, рухома своєю ціллю, зробить все від неї можливе для самозбереження. Тобто, штучний інтелект обов'язково і дуже швидко виявить в собі інстинкт самозбереження а потім буде постійно самовдосконалюватися, щоб чинити опір природному інтелекту в його стримуванні або ліквідації. Справа в тому, що інстинкт самозбереження примусить власний штучний суперінтелект ставити перед собою нові цілі, для досягнення яких необхідні будуть нові ресурси, які уже незалежно від нашої волі він буде черпати на власний розсуд із навколишнього середовища. І, як вважав Алан Тьюрінг, коли ми захочемо його зупинити, то зробити це вже не зможемо [8]. І коли штучний розум по всім параметрам випередить можливості природного (людського), виникнуть два інформаційних світа природного і штучного інтелектів. Ці інтелекти не будуть ідентичними. Хоча природний інтелект (людини) також є програмний продукт, але уже еволюції або іншого творця. Тобто є робота мільярдів нервових клітин (система програмних хімічних реакцій та електричних біоімпульсів в півкілограмовій біомасі, яка складається із води, білків, жирів і катехоламінів). На відміну від штучного , людина вважає, що за природним інтелектом залишаться такі духовні властивості як особистість, культура, душа. Штучний інтелект майбутнього - це самоосвітня, само налаштована і само розвиваюча інформаційна система. Після цього є загроза регресивного розвитку природного інтелекту. Адже не треба буде знати, наприклад, арифметичні дії чи знання іноземних мов, працювати на полі чи в цеху тощо. За нас все це буде робити роботизований інтелект. А оскільки ми не будемо напружувати свій інтелект і м'язи, то вони разом із нами швидко деградують. І настане момент повної залежності природного інтелекту від штучного.

Ілон Маск характеризує створений до цього часу існуючий штучний інтелект як "екзистенціальну загрозу" людству і в 2015 році засновує некомерційну компанію OpenA.I [9]. Її ціль – це створення відкритого і дружнього штучного інтелекту на противагу "злонаміренному штучному інтелекту" над яким, на його думку, працюють всі інші, включаючи Сергія Бріна, Реймонда Курцвейла та інших. Ілон Маск, як технолог і бізнесмен, впевнений, що скоро контролювати нас почне уже сам штучний інтелект через розгалужену інформаційну мережу створену нами самими.

Тепер припустимо, що якщо не зверх розумний, а середнього рівня штучний інтелект попаде у власність інформаційних імперій типу Google або Facebook, то усі наші з вами персональні дані (які у цих компаній уже є і продовжують рости) перетворяться в ідеальний спосіб управління нашою поведінкою. На думку соціолога Зей-

непа Тюфекчі соціальні мережі уже тепер володіють можливістю "формувати нашу особистість і наші слабкі місця" формують наші думки, бажання і мрії" [10]. І необхідно в майбутньому буде тільки невеликі зусилля штучного інтелекту, і передбачення Олдоса Хакслі про виробництво "потрібних суспільству людей" стане реальністю [11]. Уже зараз технологією так званої "когнітивної архітектури" володіють такі компанії, як AGIRI, Cycorp, Google, IBM, Novamente, Numenta, Self-Aware Systems, Vicarious Systems, і список можна продовжувати. Окрім цього, до зазначених компаній можна додати і державну структуру DARPA – " Агенство по перспективним науково-дослідним оборонним розробкам", якому людство уже вдячне за інтернет і тисячі інших цифрових речей типу Siri. Стрімко відбувається «гібридизація» інформаційних та біотехнологій. Юваль Ной Харарі вважає, що людство само себе модифікує за допомогою штучного інтелекту і біотехнологій [12]. Невідворотність кіборгізації також визнає і Ілон Маск, вважаючи, що штучний інтелект і біотехнологія створять новий вид людини, і ця трансформація відбудеться уже в 2100-і роки [9]. Україна також в авангарді досліджень штучного інтелекту. Як приклад, з нового навчального року для студентів "Львівської політехніки" введуть спеціальну навчальну програму, яка навчатиме працювати зі штучним інтелектом.

Отже, чим динамічніше розвивається технологічно людство в галузі створення і удосконалення штучного інтелекту, тим швидше ми наближаємо час власної цивілізаційної катастрофи протистояння за «панування» природного і створеного ним штучного інтелектів. Тому на погляд авторів можлива і біологічна загроза прямого та опосередкованого знищення штучним як природного (людського) інтелекту , так і біоти на землі в цілому. Незважаючи на існуючі міжнародні етичні принципи дослідника штучного інтелекту, вважаємо за доцільне також розробити і впровадити міжнародну та національні системи нормативно-правового контролю за зазначеними науковими дослідженнями, передбачивши кримінальну відповідальність за правопорушення. Тільки спільними зусиллями міжнародних безпекових організацій, включаючи і спецслужби, можна ефективно превентивно протидіяти новим загрозам біологічного характеру – при подальшому розширенню можливостей та автономізації штучного інтелекту.

Література

1. Електронний ресурс - режим доступу: http://startupline.com.ua/bignames/era-shtuchnoho-intelektu-blyzko-dokazy-vid-svitovykh-hihantiv.

2. Електронний ресурс - режим доступу: http://

www.dailytechinfo.org/infotech/8437-iskusstvennyy-intellekt-superkompyutera-ibm-watson-samostoyatelno-sozdal-svoy-pervyy-treyler-k-hudozhestvennomu-filmu.html.

3. Електронний ресурс - режим доступу: tsn.ua/blogi/themes/politics/chetverta-svitova-scenariyi-7.

4. Електронний ресурс - режим доступу: http://dt.ua/TECHNOLOGIES/chempion-z-gri-v-go-z-chetvertogo-razu-zmig-obigrati-shtuchniy-intelekt-202334_.html.

5. Lenat D. Harnessing Cyc to Answer Clinical Researchers' ad hoc Queries. /D. Lenat, M. Witbrock, D. Baxter, E. Blackstone, C. Deaton, D. Schneider, J. Scott, and B. Shepard// AI Magazine, 31 (3), Fall, 2010.

6. Електронний ресурс - режим доступу: www.dailytechinfo.org/np/4249-kembridzhskie-uchenye-nachin...

7. Електронний ресурс - режим доступу: http://vido.com.ua/article/14645/shtuchnii-intieliekt-spasinnia-chi-zaghroza-dlia-liudstva-stivien-khokingh-ta-ilon-mask-pro-zakhist-liudiei-vid-robotiv/

8. Електронний ресурс - режим доступу: http://universum.lviv.ua/magazines/universum/2016/6/shtuch-int.html

9. Електронний ресурс - режим доступу: http://dt.ua/TECHNOLOGIES/ilon-mask-poperediv-pro-nebezpeku-rozvitku-shtuchnogo-intelektu-223854_.html.

10. Електронний ресурс - режим доступу: stud.com.ua/31819/menedzhment/komunikatsiya.

11. Електронний ресурс - режим доступу: vsiknygy.net.ua/shcho_pochytaty/48065/.

12. Електронний ресурс - режим доступу: http://news.eizvestia.com/news_technology/full/575-chelovek-kak-vid-perestanet-sushhestvovat-cherez-stoletie.

13. Електронний ресурс - режим доступу: https://gazeta.ua/articles/science/_ukrayinskih-studentiv-vchitimut-shtuchnogo-intelektu/767507.

УДК 343.3

Павлючук С.О.
Національна академія Служби безпеки України
Скіцько О.І.
кандидат технічних наук,
старший науковий співробітник
Національна академія Служби безпеки України

ІНФОРМАЦІЙНЕ ЗАКОНОДАВСТВО УКРАЇНИ: ПРОБЛЕМИ ТА НАПРЯМКИ РОЗВИТКУ

У сучасних умовах розвитку інформаційного суспільства активно розвивається інформаційна сфера, яка поєднує в собі інформацію, інформаційну інфраструктуру, інформаційні мережі, інформаційні відносини між суб'єктами, що складаються у процесі збирання, формування, розповсюдження і використання інформації. Інформаційна сфера дає можливість для розвитку здібностей, покращення знань та розширення кола інтересів, але й містять у собі реальні загрози. Одна з таких загроз – комп’ютерна злочинність. Для України комп’ютерна злочинність є відносно новим видом злочинності. На сьогоднішній день в країні є низка нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави. Однак вони лише частково охоплюють елементи, які потрібні для протидії кіберзагрозам.

Правову основу кібернетичної безпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти [1].

Необхідність створення ефективної системи кібернетичної безпеки України відбулася після подій 2014 року. Інформаційна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібернетичних атак. Виклик та загрози національній безпеці України в кібернетичному просторі призвели до створення Стратегії кібербезпеки України (далі - Стратегія), затвердженою Указом Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», в якій визначені принципи, пріоритети

та напрями забезпечення кібербезпеки України. Зважаючи на комплекс проблем у сфері забезпечення кібербезпеки та констатуючи її кризовий стан, що загрожує національній безпеці, Указом Президента України від 13 лютого 2017 року №32/2017 уведено в дію рішення Ради національної безпеки і оборони України (далі - РНБО України) від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» та Указом Президента України від 25 лютого 2017 року № 47/2017 уведено в дію рішення РНБО України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [2,3,4].

Стратегія і введенні в дію рішення РНБО України є важливим кроком на шляху розбудови системи кібербезпеки України та являють собою програму дій, за якою мають слідувати державні органи та в яких описано заходи, які покладені на органи виконавчої влади та деяких військових формувань. Метою даної стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Вона складається з загальних положень, основних загроз кібербезпеці, основних суб'єктів забезпечення кібербезпеки, пріоритетів та напрямів забезпечення кібербезпеки України та прикінцевих положень.

Кіберзлочинами, згідно чинного законодавства України є передбачені Кримінальним кодексом України суспільно небезпечні діяння і закріпленні в окремому Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. На думку науковців в рамках криміналістики доцільно включити до даного поняття інші злочини, для скоєння яких застосовується комп'ютерна техніка та використовується глобальна мережа Інтернет. Проте у зазначеному розділі зовсім відсутні поняття пов'язані з кібербезпекою, є лише деякі поняття злочинів, які вчиняються за допомогою електронно-обчислюваних машин (ЕОМ), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Розділ XVI складається з трьох статей:

ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;

ст. 362 «Викрадання, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем»;

ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем» [5].

Зважаючи на нормативно-правову базу у сфері регулювання кі-

бербезпеки України, можна виокремити наступні проблеми:

- відсутні норми, щодо кваліфікації комп'ютерних злочинів;
- відсутні у державі інститути програмно-технічної та судово-кібернетичної експертизи як одного з механізмів у процесі документування злочину та відповідних методик їх проведення;
- відсутність координації та взаємодії між відповідними підрозділами правоохоронних структур;
- малорозвинена державна система протидії кіберзлочинності.

Отже пріоритетами у вдосконаленні нормативно-правової бази сфери кібербезпеки є:

- розвиток та удосконалення державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки;
- розроблення нових способів та методів запобігання кібератакам та поширенню інформації про них;
- технологічних процесів на об'єктах критичної інфраструктури, від несанкціонованого втручання у їх роботу;
- вдосконалення державної системи протидії кіберзлочинності.

Виходячи з вищезазначеного побудова національної системи кібербезпеки повинна складатися з двох напрямків: захист інформаційного простору України та протидія кіберзлочинності.

Література

1. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення/ Шеломенцев В.П. – К. : наук.-практ. журнал «Боротьба з організованою злочинністю і корупцією (теорія і практика)», 2012. –324 с.

2. Указ Президента України. «Про Стратегію кібербезпеки України». – Відомості Верховної Ради – 2016. – №96/2016.

3. Указ Президента України. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». – Відомості Верховної Ради – 2017. – №32/2017.

4. Указ Президента України. «Про Доктрину інформаційної безпеки України». – Відомості Верховної Ради – 2017. – № 47/2017.

5. Кримінальний кодекс України. Розділі XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» – Відомості Верховної Ради (ВВР) – 2001. – №25-26, ст. 131.

Овсянніков В.В.
Військовий інститут телекомунікацій та інформатизації
Паламарчук Н.А.
Військовий інститут телекомунікацій та інформатизації
Паламарчук С.А.
Військовий інститут телекомунікацій та інформатизації
Пеньков В.І.
Військовий інститут телекомунікацій та інформатизації

ДЕЯКІ ПИТАННЯ ЩОДО ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

З прийняттям Стратегій національної та кібернетичної безпеки України, визначені актуальні загрози національній безпеці, дещо змінено пріоритети забезпечення національної безпеки у різних сферах держави, визнана неефективність системи забезпечення національної безпеки і оборони України [5, 6].

Після прийняття Закону України "Про вищу освіту" у 2015 році, підготовка фахівців здійснюється у галузі знань "Інформаційні технології" за спеціальністю "Кібербезпека" [4]. Для порівняння, раніше, відповідно до Постанови Кабінету Міністрів України від 13.12.2006 № 1719 "Про перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра", підготовка здійснювалася у галузі знань "Інформаційна безпека" (за 3 напрямами: Безпека інформаційних і комунікаційних систем, Системи технічного захисту інформації; Управління інформаційною безпекою).

Згідно Постанови Кабінету Міністрів України від 27.08.2010 № 787 "Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра", підготовка здійснювалася у галузі знань "Національна безпека", напрям підготовки "Інформаційна безпека" (за 5 спеціальностями: Захист інформації з обмеженим доступом та автоматизація її обробки (в комп'ютерних системах); Захист інформації з обмеженим доступом та автоматизація її обробки; Системи захисту від несанкціонованого доступу; Адміністративний менеджмент в системах захисту інформації з обмеженими доступом, Захист інформації в комп'ютерних системах і мережах).

Зрозуміло, що Україна вступає у світовий інформаційний простір, адаптує свою нормативну правову базу у відповідність до міжнародної та в умовах стрімкого розвитку ІТ, ведення інформаційної

війни проти України, спеціальність “Кібербезпека”, як ніколи, актуальна для нашої країни, але не потрібно звужувати сферу, втрачати той потенціал та здобутки, які були напрацьовані роками з підготовки фахівців із захисту інформації (в тому числі, з обмеженим доступом), і в цілому інформаційної безпеки як складової національної безпеки держави. До того ж, наразі галузь знань національна безпека (за окремими сферами забезпечення і видами діяльності) входить до галузі “Воєнні науки, національна безпека, безпека державного кордону”. Види діяльності затверджуються відповідним державним органом, який забезпечує виконання завдань у сфері національної безпеки, за погодженням з Міністерством освіти та науки [4].

Про неможливість об’єднання або ототожнення галузей інформаційної та кібернетичної безпеки, в тому числі і в підготовці фахівців, йдеться в [1, 3].

Слід звернути увагу, що згідно [2], у 2013 році Американська національна академія наук, на своїй конференції визнала: “професії/спеціальності фахівця з кібернетичної безпеки бути не може, так як, кібербезпека дуже об’ємна та різнопланова щоб об’єднати її під однією “парасолькою”. Вперше визнали, що дії направлені на уніфікацію та універсалізацію професії безперспективні. Не потрібно концентруватися на розвитку кібербезпеки, як єдиної дисципліни. Потрібно розбивати на різні дисципліни з чіткими межами”. Це визнала держава, яка фактично є одним із лідерів у світі стосовно забезпечення кібербезпеки, Україні не потрібно ігнорувати цей факт.

Безперечно, якісні зміни, які постійно відбуваються в сферах життєдіяльності особи, суспільства, держави та супроводжуються стрімким зростанням ролі ІТ, також будуть потребувати своєчасного перегляду та відповідного коригування державної політики в сфері підготовки фахівців із кібербезпеки та національної безпеки. Доречно було б, при цьому, брати до уваги світовий досвід.

Література

1. Козубцов І.М. Стратегічні напрямки підготовки спеціалістів інформаційної та кібернетичної безпеки / Козубцов І.М., Куцаєв В.В., Срібний С.П., Ткач В.В Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф.(19 березня 2015 р.) К.: Центр навч., наук. та період. видань НА СБУ, 2015. – с. 49-51.

2. Лукацький А.В. Американцы отказываются от специалистов по кибербезопасности. Бизнес без опасности. URL: http://lukatsky.blogstop.com/2013/12/blog-post_5.html .

3. Мальцева І.Р. Проблемні питання побудови системи кібернетичної безпеки України / Мальцева І.Р., Паламарчук С.А., Черниш

Ю.О., Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф.(19 березня 2015 р.) К.: Центр навч., наук. та період. видань НА СБУ, 2015. – с. 65-67.

4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29 квітня 2015 р. №266. URL: http://zakon5.rada.gov.ua/laws/show/266-2015-п.

5. Стратегія національної безпеки України: Указ Президента України від 26.05.2015 №287/2015. URL: http://zakon3.rada.gov.ua/laws/show/287/2015/paran7#n7

6. Стратегія кібернетичної безпеки України: Указ Президента України від 15.03.2015 №96/2016/ URL: http://www.president.gov.ua/documents/962016-19836.

УДК 340:007

Пальчик М.Л.
кандидат юридичних наук
Національна академія Служби безпеки України

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У КІБЕРЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Посилення негативних процесів, пов’язаних зі зростанням кількості кібератак на підприємства та інфраструктурні об’єкти, які в практиці іноземних держав відносять до об’єктів критичної інфраструктури (далі – КІ), виявило наявність системних проблем в забезпеченні їх кібербезпеки, актуалізувало, поряд з іншими, питання удосконалення вже існуючих та створення нових механізмів кіберзахисту.

З метою вирішення ситуації, що склалася на загальнодержавному рівні прийнято низку документів стратегічного та доктринального характеру, направлених на: уточнення засад формування та реалізації державної інформаційної політики [1]; створення умов для безпечного функціонування кіберпростору [2]; комплексного вдосконалення правової основи захисту критичної інфраструктури [3]. І хоча прийняті нормативні акти по суті не вирішують існуючих проблем інформаційної та кібербезпеки, а їх окремі положення є доволі дискусійними, цими документами визначено основні напрями, завдання та пріоритети державної політики в інформаційній сфері, кіберпросторі та захисті критичної інфраструктури.

Зазначимо, що одним із пріоритетних завдань забезпечення інформаційної та кібербезпеки критичної інфраструктури, вказаними нормативно-правовими актами визначено розвиток державно-приватного

партнерства. Вказане, на наш погляд, потребує додаткової наукової уваги та наукової розробленості проблеми взаємодії державних та приватних партнерів у сфері кіберзахисту критичної інфраструктури.

На сьогодні правові та організаційні засади взаємодії державних та приватних партнерів визначені Законом України «Про державно-приватне партнерство України». Законом сформовано поняття та ознаки державно-приватного партнерства, закріплено його основні принципи та форми, визначено сфери застосування державно-приватного партнерства [4].

Водночас питання пов'язані з функціонуванням та створенням державної системи захисту критичної інфраструктури; визначенням прав та обов'язків основних суб'єктів; запровадженням критеріїв віднесення до об'єктів критичної інфраструктури, формуванням їх переліку; оцінкою загроз КІ та реагуванням на них до сьогодні залишаються нормативно невизначеними.

Така невизначеність сфери критичної інфраструктури, на нашу думку, є стримуючим чинником формування практики взаємодії державних та приватних партнерів у забезпеченні кібербезпеки КІ. Разом з тим, компанії, які здійснюють діяльність у сфері інформаційних технологій та інформаційної безпеки, мають можливості, що значно переважають можливості державних установ. До таких відносимо кадровий потенціал, підготовлені рішення попередження та реагування на кібератаки, комплексні програмні продукти забезпечення кібербезпеки. Фахівці приватних компаній вже давно залучаються правоохоронними органами до проведення комп'ютерних експертиз, збору інформації, розслідування та попередження кіберінцидентів, організації та реалізації спільних освітніх проектів з питань кібербезпеки.

Проаналізувавши сформовану практику взаємодії правоохоронних органів та приватних компаній, а також положення названих вище нормативно-правових актів можемо визначити основними напрямами державно-приватного партнерства кіберзахисту критичної інфраструктури:

- розроблення та впровадження програмного забезпечення з контролю та моніторингу кіберпростору;
- використання експертного потенціалу для проведення комп'ютерно-технічних експертиз;
- здійснення збору та аналізу значних масивів інформації у тому числі як доказів в рамках кримінальних проваджень;
- залучення до нормотворчої діяльності з проблем кібербезпеки та кіберзахисту критичної інфраструктури;
- надання освітніх послуг у сфері забезпечення кібербезпеки та підвищення рівня обізнаності населення про кіберзагрози.

Вказані напрями не є вичерпними та потребують подальшого наукового дослідження. Здійснення ж наукової розробки проблем державно-приватного партнерства сфери кіберзахисту критичної інфраструктури, на наш погляд, дозволить сформувати ефективну загальнонаціональну систему її захисту, а також подолати існуючі негативні тенденції взаємовідносин правоохоронних органів та приватних компаній, що здійснюють діяльність у сфері електронних комунікацій.

Література

1. Указ Президента України про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року № 96/2016 / Офіційний Вісник України від 29 березня 2016 року. – Офіц. вид. – К., 2016. – № 23. – Ст. 899.
2. Указ Президента України про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 року № 47/2017 [Електронний ресурс].– Режим доступу : http://www.president.gov.ua.
3. Указ Президента України про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» від 16 січня 2017 року № 8/2017 [Електронний ресурс].– Режим доступу : http://www.president.gov.ua.
4. Закон України «Про державно-приватне партнерство» від 01 липня 2010 року № 2404-VI [Електронний ресурс].– Режим доступу : http://zakon0.rada.gov.ua/laws/show/2404-17.

УДК 343.326

Петрик В.М.
кандидат наук з державного управління, доцент
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПОНЯТЬ «РАДИКАЛІЗМ», «ЕКСТРЕМІЗМ», «ТЕРОР», «ТЕРОРИЗМ», «ТЕРОРИСТИЧНИЙ АКТ», «ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ», «ДИВЕРСІЯ»

Радикалізм – це ідеологія, яка передбачає спосіб мислення, що послідовно і прямолінійно йде до наміченої мети, відкидаючи всякий компроміс. Радикалізм виявляється у різних ділянках: філософії, етиці, релігії, як напрям, який повністю не погоджується з панівними поглядами.

Екстремізм (від лат. extremus — крайній) — схильність до крайніх поглядів і дій переважно в політиці, ідеологічному протиборстві. Відокремлюючи тероризм від екстремізму, пропонується ряд ознак, що відбивають суть як особливого суспільно-політичного явища, але не відмінних стосовно екстремізму, оскільки екстремізм як соціально-політичне явище є сукупність різних крайніх форм політичної боротьби, одна з яких - тероризм.

Тероризм - суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей.

Інформаційний (медіа) тероризм це використання інформаційних засобів у терористичних цілях — загрози застосування або застосування фізичного насильства в політичних цілях, залякування і дестабілізації суспільства і таким чином впливаючи на населення і державу.

Отже можна вивести таке співвідношення «радикалізм» більш ширше поняття чим «екстремізм», а «екстремізм» більш ширше ніж «тероризм». Будь який терорист є екстремістом і радикалом. Тероризм проявляється у двох формах: терористичний акт та інформаційний тероризм.

Терор (у перекладі з латинської (terror) означає страх) це діяльність державної, що характеризується особливо репресивною, жорстокою діяльністю державної влади стосовно своїх політичних противників як усередині країни, так і поза її межами, тому державний терор можна поділити на внутрішній і зовнішній.

Від тероризму терор відрізняється наступним.

По-перше, тероризм – це одноразово здійснюваний акт або серія подібних актів, тоді як терор має тотальний, масовий, безперервний характер.

По-друге, суб’єкти тероризму, на відміну від суб’єктів терору, не те, щоб безмежної, а взагалі ніякої офіційно встановленої (виборним шляхом, внаслідок військової інтервенції і т.ін.) влади над соціальним контингентом тієї місцевості, де розгортаються їх дії, не мають.

По-третє, суб’єктами терору виступають суспільно-політичні структури, а суб’єктами тероризму – фізичні осудні особи, які досягли віку кримінальної відповідальності.

По-четверте, якщо терор – соціально-політичний фактор дійсності, то тероризм – явище кримінально-правової властивості і насильство при тероризмі має не загальне, а локальне застосування.

Диверсія - вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій [1].

Основною метою будь-якого теракту є, як відомо, зовсім *не сам факт здійснення того чи іншого злочинного діяння*, (вбивства, руйнування, захоплення заручників) та його матеріальні збитки, а насамперед *інформаційний вплив* на якомога ширшу аудиторію (залякування, привертання уваги громадськості, провокування до певних дій чи бездіяльності). Таким чином, тероризм – засіб інформаційно-психологічного впливу. Його головний об'єкт – не ті, хто став жертвою, а ті, хто залишився живим. Його мета – не вбивство, а залякування і деморалізація живих. Жертва − інструмент, вбивство – метод. *Цим тероризм відрізняється від диверсійних дій, мета яких – зруйнувати об'єкт (міст, електростанцію) чи ліквідувати противника у перекладі з латинської (terror) означає страх* [2, с. 169].

Література

1. Кримінальний Кодекс України : Закон України від 05.04.2001 №2341-III. URL: http://zakon.rada.gov.ua

2. Інформаційна безпека держави: підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. – Т. 2. / за заг. ред. В.В.Остроухова. – К.: Вид-во ІСЗЗІ НТУУ. – 328 с.

УДК 004.62+004.77

Платоненко А.В.
Державний університет телекомунікацій
Лазаренко С.В.
Державний університет телекомунікацій

АКТУАЛЬНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕРЕД УКРАЇНСЬКИХ КОРИСТУВАЧІВ МОБІЛЬНИХ ПРИСТРОЇВ

Кожен третій житель України має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – кожен другий. З використанням сучасних мобільних пристроїв та високошвидкісних мереж, загрози інформаційної безпеки для державних та приватних установ збільшуються, оскільки працівники частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування, що

відкриває для зловмисників більші технічні можливості.

Таким чином постає питання захисту мобільних пристроїв, які можуть використовуватись за межами офісу компанії та створювати нові загрози витоку інформації. Причиною хакерських атак зазвичай стають ненадійні паролі користувачів. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі підключені до мережі пристрої піддаються ризику можливої атаки. Хакерська група, яка раніше інфікувала пристрої зі сфери Інтернету речей, цілеспрямовано заразила 3,2 мільйони домашніх Wi-Fi-маршрутизаторів за допомогою шкідливого програмного оновлення, що призвело до неможливості відновлення їх роботи.

Знання користувачів в області інформаційної безпеки дуже обмежені. Третина всіх паролів, що використовуються, зламуються шляхом банального перебору варіантів зі словника, а майже 17% облікових записів захищені паролем «123456». Рівень розкриття кіберзлочинів в Україні становить в середньому 50%, при цьому 80% постраждалих вдається відшкодувати збитки, яких вони зазнали внаслідок дій злочинців. Основною перешкодою для захисту компаній від кіберзагроз 65,1% фахівців вважають дефіцит бюджету, брак фахівців з IT-безпеки – 47%. Основні загрози інформаційній безпеці організацій несуть забезпечення мобільності співробітників (51%) та Інтернет речей (20%).

В Україні за останній рік відбулись хакерські атаки на міжнародні організації з контролю за правами людини, антитерористичні центри та об'єкти критичної інфраструктури. В результаті атак кіберзлочинцям вдалося викрасти великі обсяги конфіденційної інформації, включаючи записи розмов користувачів через вбудовані мікрофони ноутбуків, скріншоти документів, різні файли і паролі. Якщо співробітники нехтують прийнятими в компанії правилами інформаційної безпеки, намагаються отримати доступ до корпоративних даних з будь-якого місця і з будь-якого пристрою, то це ставить під загрозу інформаційні ресурси будь-якого рівня. Оскільки велика кількість компаній дозволяє використовувати мобільні пристрої для віддаленої роботи, а завдяки соціальним мережам спілкуються зі своїми клієнтами, то необхідно забезпечити певний рівень захисту користувачів від можливих загроз.

Користувачі повинні бути уважнішими, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування мобільного пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати. Важливо поєднувати зусилля в підвищенні обізнаності користувачів фахівцям у галузі інформаційної безпеки, виробникам мобільних пристроїв, провайдерам послуг та

технічного забезпечення, адже більшість користувачів, нажаль, навіть не замислюється над можливістю того, що їх пристрої можуть піддаватись загрозам.

Література

1. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко. // Сучасний захист інформації. – 2015. – №4. – С. 86–90.

2. Використання смартфонів в Україні [Електронний ресурс] – Режим доступу: http://lead9.com/slide/slide.pdf

3. Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers [Електронний ресурс] – Режим доступу: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious-firmware-update-to-32-million-home-routers

УДК 378 (477)(094.5)

Погребняк В.П.
кандидат технічних наук, професор
Інститут модернізації змісту освіти
Дашковська О.В.
кандидат хімічних наук, доцент
Інститут модернізації змісту освіти
Солоденко А.К.
Інститут модернізації змісту освіти

ІНТЕРНАЦІОНАЛІЗАЦІЯ ВІТЧИЗНЯНОЇ ВИЩОЇ ОСВІТИ

Глобалізація світу і пов’язана з нею інтернаціоналізація суспільної діяльності розповсюджується на всі сфери соціальних відносин, економіку, освіту і науку. Ці процеси реалізуються і у вищій освіті України, сприяючи рівноправній інтеграції вітчизняної вищої школи у світовий і європейський освітній простір.

Першим серйозним кроком до інтернаціоналізації європейської освіти стало запровадження в 1987 році програми ERASMUS, метою якої було удосконалення обсягів мобільності студентів та викладачів у країнах Європейського Союзу, розвиток багатосторонньої міжуніверситетської кооперації, поглиблення співпраці між університетами та підприємствами, поширення технологій навчання. В рамках ERASMUS також було створено інструмент перезарахування навчальних досягнень, отриманих студентом в іншому університеті за програмами мобільності - Європейську кредитно-трансферну систему (далі – ЄКТС).

Наступним кроком стало створення єдиного Європейського просто-

ру вищої освіти (ЄПВО, European Higher Education Area), ініційоване Сорбонською декларацією [1] та сформульоване у Болонській декларації [2], підписаній у червні 1999 року, до якої Україна приєдналась у 2005 році.

У контексті глобальних процесів в освіті, розглянемо, які зміни відбуваються у вітчизняній вищій освіті за останні роки.

Основним законодавчим актом, який повністю відповідає європейським зразкам і акцентований на євроінтеграцію є Закон

Відповідно до положень Закону України «Про вищу освіту» 2014 року (далі – Закон) [3] у вищій школі реалізується комплекс заходів в контексті інтернаціоналізації вищої освіти:

упроваджено Національну рамку кваліфікацій (далі - НРК) [4], приведено рівні та ступені вищої освіти у відповідність з кваліфікаційними рівнями НРК. Законом відповідно до НРК встановлено 9 кваліфікаційних рівнів, 5 з яких відносяться до вищої освіти;

затверджено новий перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти [5]. Замість 48 галузей знань, 144 напрямів та понад 500 спеціальностей попередніх переліків введено 29 галузей знань і 122 спеціальності. При цьому вищі навчальні заклади самостійно обирають спеціалізації, що дає їм можливість гнучко реагувати на потреби ринку праці;

упроваджується стандарт вищої освіти (далі - СВО), який базується на компетентнісному підході, закладеному в Болонському процесі та міжнародному проекті TUNING;

розроблено та впроваджено Додаток до диплома про вищу освіту Європейського зразка (Diploma Supplement), який сприяє академічній мобільності;

розширюється академічна автономія вищих навчальних закладів. Університети отримали право самостійно розробляти і затверджувати освітні програми, присвоювати наукові ступені, здійснювати нострифікацію дипломів, отриманих у закордонних закладах освіти;

створено Національне агентство із забезпечення якості вищої освіти (далі – НАЗЯВО) [6], як постійно діючий колегіальний орган, уповноважений на реалізацію державної політики у сфері забезпечення якості вищої освіти. Передбачається його включення до Європейського реєстру агентств забезпечення якості вищої освіти;

створюється Національний репозитарій академічних текстів, ефективне функціонування якого підвищить рівень академічної доброчесності в освіті і науці;

розширена можливість стажування вітчизняних молодих вчених у міжнародних освітніх та наукових інституціях [7].

Література

1. Harmonization of the architecture of the European higher

education system (Sorbonne Declaration). – Paris, Sorbonne, 25 May 1998.

2. The European Higher Education Area. Joint Declaration of the European Ministers of Education. – Bologna, Italy, 19 June 1999.

3. Закон України «Про вищу освіту», 1 липня 2014 р. №1556-VII.

4. Постанова КМУ від 23.11.2011 р. № 1341 «Про затвердження національної рамки кваліфікації».

5. Постанова КМУ від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».

6. Постанова КМУ від 15.04.2015 р. № 244 «Про утворення Національного агентства із забезпечення якості вищої освіти».

7. Постанова КМУ від 12 серпня 2015 № 579 «Положення про порядок реалізації права на академічну мобільність».

УДК 342.951; 343.9 (477)

Половніков В.В.
кандидат юридичних наук, доцент
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

ДО ПРОБЛЕМИ ВИЗНАЧЕННЯ ПОНЯТТЯ КРИМІНАЛЬНОГО АНАЛІЗУ ТА ЙОГО ЗАСТОСУВАННЯ

До питання про роль і місце кримінального аналізу в оперативно-розшуковій діяльності (далі – ОРД) оперативних підрозділів Державної прикордонної служби (далі – ДПС), Національної поліції, Служби безпеки та інших правоохоронних органів України щодо протидії злочинності останнім часом прикуто велику увагу як науковців, так і практиків.

Загальні теоретичні і практичні положення, що стосуються інформаційно-аналітичної діяльності, інформаційного і оперативно-аналітичного пошуку, поліційної (кримінальної) розвідки, тактико-криміналістичних і процесуальних основ розслідування злочинів відображено у багатьох наукових працях. Разом з тим, їх аналіз свідчить про те, що поза достатньою увагою авторів залишились питання про застосування кримінального аналізу. Це поняття вже давно використовується правоохоронцями інших країн і лише віднедавна увійшло у лексику правоохоронців України.

Досвід розвинутих країн світової спільноти свідчить про ефективність використання його можливостей у протидії злочинності. Певний досвід застосування кримінального аналізу вже накопичено

оперативними підрозділами ДПС України. Вона беручи за взірець досвід поліції та прикордонних служб інших країн, першою з інститутів системи охорони правопорядку в Україні започаткувала процес запровадження міжнародних стандартів управління інформацією у сфері боротьби зі злочинністю.

З огляду на те, що система кримінального аналізу характеризується однаковими аналітичними процедурами, принципами та умовними символами візуального представлення, вона є своєрідною міжнародною мовою інтерпретування кримінальних подій аналітиками у всьому світі. Цей беззаперечний аргумент створює також нові можливості для розвитку результативної взаємодії і співпраці між національними і міжнародними органами правопорядку.

Відтак, знання у галузі кримінального аналізу – його видів, форм, сфер, умов і можливостей застосування, мають бути широко пропаговані, а особливо серед осіб, які безпосередньо та опосередковано залучені до процесу боротьби зі злочинністю. Знаннями, компетентністю і кваліфікаціями у сфері кримінального аналізу повинні, у різній мірі, володіти як кримінальні аналітики та їх керівництво на всіх рівнях управління, так і особи, які здійснюють розшукові, оперативні дії, проводять дізнання і слідство [1, с. 4].

Разом з тим, на сьогодні залишається чимало проблемних питань, що стосуються єдиного розуміння і визначення поняття кримінального аналізу, законодавчого регулювання його застосування в ОРД і, відповідно, в практичній діяльності оперативних підрозділів, використання результатів кримінального аналізу в кримінальному процесі, визнання продуктів (результатів) кримінального аналізу доказами і т. ін. Так, наприклад, в чинному Законі України «Про оперативно-розшукову діяльність» про аналіз та інформаційно-аналітичну діяльність оперативних підрозділів взагалі не згадується.

На думку М. Яніцкі, кримінальний аналіз є оперативно-слідчою дією, яка полягає в ідентифікації і якомога точному визначенні внутрішніх зв’язків між інформаціями (відомостями), що стосуються злочину та будь-якими іншими даними, які були отримані з різних джерел і їх використанні для цілей оперативно-розшукової, дізнавальної і слідчої діяльності.

Інше визначення, на яке він посилається, було представлене у Інтернет-енциклопедії, згідно з якою – кримінальний аналіз – це пошук взаємозв’язків між інформаціями (відомостями), які стосуються подій злочинного характеру, осіб, пов'язаних з ними та даними, що походять з інших джерел та їх використання правоохоронними органами і судами [1, с. 9].

Розглядаючи поняття кримінального аналізу, перш за все, необ-

хідно визначити його складові: «кримінальний» і «аналіз».

Згідно з словником іншомовних слів, кримінальний (лат. criminalis) – той, що стосується вивчення злочинів і злочинності, боротьби і запобігання злочинам [2, с. 370]. Відповідно до цього ж словника, аналіз (від грец. ἀνάλυοις – розклад, розчленування) – 1) Метод дослідження, що полягає в мисленому або практичному розчленуванні цілого на складові частини. Протилежне – *синтез.* 2) Уточнення логічної форми (будови, структури) міркування засобами формальної логіки. Аналітичний – одержаний в результаті розчленування об'єкта й аналізу одержаних внаслідок цього частин [2, с. 47].

Логіка (від грец. λογική – наука про умовивід) – 1) Наука про закони, форми та прийоми людського мислення, застосування яких у процесі міркування й пізнання забезпечує досягнення об'єктивної істини. 2) Формальна логіка – наука, що вивчає форми мислення (поняття, судження, умовиводи) та структури наукового знання (дедуктивні системи, схеми доведення тощо)… 4) Розумність, правильність, внутрішня закономірність [2, с. 398].

Ґрунтуючись на вищезазначеному можна дати таке визначення кримінального аналізу – це один із сучасних засобів і заходів протидії оперативних підрозділів злочинності, що передбачає застосування системи методів логіки (міркування й пізнання), інформаційного пошуку й використання наявних інформаційних баз даних з метою виявлення та встановлення внутрішніх закономірностей у зв'язках між об'єктами і подіями у сфері протиправної діяльності з метою їх візуалізації з використанням програмного аналітичного забезпечення або інших загальнодоступних комп'ютерних програм. Особливу роль при цьому відіграє особистість того, хто здійснює кримінальний аналіз, його креативність, кмітливість, логічне мислення тощо.

У нинішній ситуації належне використання кримінального аналізу є необхідним обов'язком усіх інститутів з боротьби з незаконною діяльністю [1, с. 10].

Література

1. Яніцкі Мірослав. Оперативний кримінальний аналіз: Пер. Ігоря Родюка / За ред. Міжнародної організації з міграції (МОМ). Проект МОМ «Розвиток систем аналізу ризику та кримінального аналізу для Державної прикордонної служби України відповідно до європейських стандартів (АРКА)» – К, 2009. – 86 с.

2. Словник іншомовних слів: Головна редакція УРЕ / За ред. Чл. кор. АН УРСР О.С. Мельничука. – К.: Київська книжкова фабрика, 1974. – 776 с.

УДК [323.28+327]:351.746.1(477)

Присяжнюк М.М.
кандидат технічних наук,
старший науковий співробітник
Національна академія Служби безпеки України

МІЖНАРОДНИЙ ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Одним із найбільш небезпечних і важко прогнозованих явищ сучасності, що відрізняється динамізмом та здатністю до адаптації й модернізації в умовах глобалізації та інформатизації є тероризм, що набув міжнародного характеру.

Атрибутивною ознакою тероризму на нинішньому етапі його розвитку стало активне використання інформаційних технологій, здатних перетворити цільову аудиторію на об'єкт маніпулювання.

Осмислення в цьому відношенні феномену інформаційного тероризму є передумовою формування більш чітких уявлень щодо сутності сучасного міжнародного тероризму, запобігання загроз, здатних зруйнувати державні інститути, основи державної стабільності, як і основи національної безпеки демократичних країн взагалі.

Аналіз положень Закону України «Про боротьбу з тероризмом» свідчить, що інформаційний тероризм є видом технологічного тероризму, і це злочини, що вчиняються з терористичною метою із застосуванням засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля, або створюють умови для аварій і катастроф техногенного характеру.

Інформаційний тероризм, під яким розуміється використання сучасних інформаційних технологій і, в першу чергу мережі Інтернет, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур, стає реальною загрозою для національної безпеки нашої держави.

Особливістю сучасного тероризму є активне використання інформаційно-психологічного впливу як важливого елемента маніпуляції свідомістю людей.

Серед основних зовнішніх загроз для національної безпеки України слід виділити інформаційну експансію з боку інших держав і можливість витоку інформації, яка становить державну та іншу передбачувану законом таємницю, а також конфіденційної інформації, що є власністю держави.

Протидія даному виду злочинної діяльності відстає від потреб правоохоронної практики, а саме знаходиться на стадії становлення і потребує належного організаційно-правового забезпечення.

Україна, що поступово вливається в інформаційний простір світу, намагається боротися з міжнародним інформаційним тероризмом у зв'язку з постійними зовнішніми загрозами. Боротьба з інформаційним тероризмом вимагає насамперед відповідної правової бази, функціонування спеціальних підрозділів по боротьбі з інформаційним тероризмом, широкого співробітництва з громадськістю, тісної міжнародної взаємодії.

Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 р. №287/2015, наголошує на тому, що найбільш актуальними загрозами національній безпеці України є «... агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території». Це, зокрема, розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму.

Для нейтралізації цих загроз у Стратегії визначає основні напрями державної політики у сфері забезпечення національної безпеки України, серед яких важливе місце займає забезпечення державної безпеки у сферах боротьби з тероризмом, економічної, інформаційної, кібернетичної безпеки та розвиток спроможностей щодо запобігання і боротьби з тероризмом, а також спільної боротьби з тероризмом [1].

Успішна реалізація державної політики напрямами потребує належного законодавчого регулювання діяльності суб'єктів відповідних правовідносин.

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Найбільшу небезпеку представляє кібертероризм, а саме – тероризм спланований, вчинений чи скоординований у кіберпросторі. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави. Це й атомні електростанції і системи керування польотами, комп'ютерні системи правоохоронних органів тощо.

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Указом Президента України від 16.03.2016 р. №96/2016 затверджена Стратегія кібербезпеки України. Її метою є створення умов для безпечного функціонування кіберпростору в інтересах особи, суспільства і держави.

Для досягнення цієї мети Стратегія визначає необхідним:

- створення національної системи кібербезпеки;
- посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;
- забезпечення кіберзахисту критичної інформаційної інфраструктури, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України [2].

Література

1. Стратегія національної безпеки України. – Режим доступу: https://www.president.gov.ua.
2. Стратегія кібербезпеки України. URL: https: //www.president.gov.ua.

УДК 316.776.33

Процюк Ю.О.
Військовий інститут телекомунікацій та інформатизації
Островський С.М.
Центральний науково-дослідний інститут Збройних Сил України
Штонда Р.М.
Військовий інститут телекомунікацій та інформатизації

ШЛЯХИ РОЗВИТКУ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ У ВІЙСЬКОВІЙ СФЕРІ

В 2012 році провідні військові експерти визначали, що наступним театром ведення операцій (бойових дій) буде космічний простір, але виявилось все не так. На початку 2014 року на перший план в Україні виходить протистояння в інформаційному просторі, яке триває й на сьогоднішній день. Агресія проти України, що проявилась у «гібридній» війні, потребує сучасних та дієвих заходів та способів протидії. Бажаною ціллю ворога є не тільки фізичний простір країни, а й серця та розум українців, та ставлення до України світової спільноти. В цій війні переможе той, чия розповідь буде більш переконлива.

Стратегічні комунікації є тим інструментом перемоги, який застосовується в сучасній практиці провідних країн світу. В новій редакції Воєнної доктрини України зазначено, *стратегічні комунікації* – скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [1]. Також про пріоритети стратегічних комунікацій у військовій сфері зазначається в:

- Указі Президента України № 92/2016 від 4 березня 2016 року «Про концепцію розвитку сектору безпеки і оборони України».

- Указі Президента України № 96/2016 від 15 березня 2016 року «Про Стратегію кібербезпеки України».

- Указі Президента України № 240/2016 від 6 червня 2016 року «Про Стратегічний оборонний бюлетень України».

- Дорожній карті Партнерства у сфері стратегічних комунікацій між РНБО та Міжнародним секретаріатом НАТО.

Для того щоб стратегічні комунікації у військовій сфері стали дієвим інструментом перемоги необхідно, провести низку заходів на державному рівні із залученням відповідного кваліфікованого персоналу та ресурсів. До кінця 2017 року запустити курси підготовки із комунікаційних дисциплін, які будуть в подальшому інтегровані до загальнодержавної системи підготовки у сфері комунікацій. Також в край необхідні обов'язкові курси з підготовки керівного та командного складу в сфері стратегічних комунікацій. До кінця 2018 року необхідно, виконати міжнародні правові норми щодо структури стратегічних комунікацій у військовій сфері згідно із стандартами НАТО. Створити до 2020 року комунікаційні спроможності на стратегічному, оперативному та тактичному рівнях.

Для реалізації перелічених заходів із розвитку стратегічних комунікацій у військовій сфері необхідно враховувати досвід та стандарти НАТО, а також внести зміни навчальних програм вузів. У країнах членів НАТО діяльність у сфері стратегічних комунікацій охоплює такі напрямки: як зв'язки з громадськістю; публічна дипломатія та військова підтримка публічної дипломатії; внутрішня комунікація; зв'язок зі ЗМІ; інформаційні та психологічні операції; інформування про ситуацію; залучення ключового лідера та інше. Але нажаль, найближчим часом проблемами розвитку стратегічних комунікацій у військовій сфері буде налагодження дієвої координації та взаємодії, створення повноцінного та дієвого механізму підготовки фахівців зі стратегічних комунікацій, залучення достатньої кількості ресурсів для задоволення потреб стратегічних комунікацій.

Література

1. Нова редакція Воєнної доктрини України: Указ Президента України від 24.09.2015 №555/2015 [Електронний ресурс]. – Режим доступу: www.president.gov.ua.

УДК 378

Пучков О.О.
кандидат філософських наук, професор
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ імені Ігоря Сікорського»
Конюшок С.М.
кандидат технічних наук, доцент
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ імені Ігоря Сікорського»

ПІДГОТОВКА ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ: ДОСВІД ІСЗЗІ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО

На даний час, в світі спостерігається тенденція суттєвого впливу розвитку інформаційних технологій на національну безпеку будь-якої держави, що змінює оперативне середовище функціонування спеціальних служб та розвідувальних органів. Наприклад, голова MI6 Алекс Янгер, виступаючи у Вашингтоні 20 вересня 2016 року зазначив: "Інформаційна революція повністю змінює умови, в яких працюють спецслужби. Зокрема, мова йде про наростання ролі інтернету в роботі спеціальних служб, які повинні активно вести моніторинг соціальних мереж, поштових серверів і інших інтернет-ресурсів" [1], а доля агентів та фахівців Служби загальної безпеки Ізраїлю (ШАБАК), зайнятих в сфері кібербезпеки, достягла вже 25% [2].

В Україні, Доктрина інформаційної безпеки України [3] ставить завдання щодо моніторингу спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері, а Стратегія національної безпеки України [4], в якості одного з пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів виділяє "створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони".

Ці та інші факти, що доступні у відкритих джерелах демонструють надзвичайну важливість проблеми підготовки національних кадрів у таких високоінтелектуальних сферах, як інформаційна та кібернетична безпека держави.

В доповіді викладений аналіз можливостей в цій сфері Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", який на даний час здійснює освітню діяльність з підготовки фахівців з вищою освітою з таких унікальних для

України спеціалізацій, як розробка та експлуатація систем урядового і конфіденційного зв'язку, криптографічний та технічний захист інформації, а також створення систем забезпечення кібербезпеки.

Протягом десятиріччя ІСЗЗІ КПІ ім. Ігоря Сікорського забезпечує підготовку офіцерських кадрів для потреб, насамперед, Держспецзв'язку, а також інших центральних органів виконавчої влади України, військових формувань і правоохоронних органів, що створені відповідно до законодавства (на даний час – Служби зовнішньої розвідки України, Служби безпеки України та Управління державної охорони України).

Метою доповіді є визначення основних актуальних питань підготовки фахівців у сфері інформаційної та кібернетичної безпеки, серед яких слід виділити наступні.

По-перше, нові вимоги до підготовки кадрів у сфері інформаційної та кібернетичної безпеки, а також підвищення стандартів військової освіти в цій сфері, що обумовлено специфічним статусом військової освіти у сучасному освітньому просторі.

По-друге, забезпечення підготовки фахівців у сфері інформаційної та кібернетичної безпеки найсучаснішим обладнанням, яке відповідає останнім розробкам науково-технічного прогресу, а також сучасному матеріально-технічному забезпеченню всіх складових навчально-виховного процесу.

По-третє, складність комунікаційної системи між викладачами і курсантами, якою є навчально-виховний процес професійної підготовки фахівців у сфері інформаційної та кібернетичної безпеки.

По-четверте, загальногуманітарна підготовка майбутнього фахівця у сфері інформаційної та кібернетичної безпеки, яка формує ціннісний і цивілізаційний рівень розвитку курсанта до соціокультурних викликів сучасного світу.

Для ефективного вирішення актуальних питань підготовки кадрів у сфері захисту інформації у колективу співробітників ІСЗЗІ КПІ ім. Ігоря Сікорського є багато можливостей. Системний підхід і колективна праця у напряму модернізації навчально-виховного процесу інституту підвищать рівень якості професійної підготовки кадрів у сфері захисту інформації і забезпечать інтелектуальний потенціал сектору безпеки і оборони держави.

Література

1. Британська служба розвідки МІ-6 збільшить чисельність персоналу на 40% [Електронний ресурс] : – Режим доступу: http://24info.in.ua/222-britanska-sluzhba-rozvdki-m-6-zblshit-chiselnst-personalu-na-40.html (дата звернення: 03.05.2017). – Назва з екрана.

2. Электронная служба Израиля [Електронний ресурс] : – Ре-

жим доступу: http://www.isrageo.com/2017/01/30/electridf/ (дата звернення: 03.05.2017). – Назва з екрана.

3. Доктрина інформаційної безпеки України / Указ Президента України від 25 лютого 2017 року № 47/2017. URL: http://zakon3.rada.gov.ua/laws/show/47/2017.

4. Стратегія національної безпеки України/ Указ Президента України від 26 травня 2015 року № 287. URL: http://zakon3.rada.gov.ua/laws/show/287/2015.

УДК 340. 13.(4)

Романов М.С.
доктор юридичних наук,
старший науковий співробітник, доцент,
Національна академія Служби безпеки України

УЧАСТЬ НАУКОВО-НАВЧАЛЬНИХ УСТАНОВ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЯХ

Інформаційні провокації і дезінформація з Росії зараз проводиться за участю недержавних структур або ЗМІ, науковими, навчально-науковими або академічними структурами [1].

Одним із напрямів задіяння наукових та науково-навчальних закладів Російської Федерації у інформаційній війні проти України є викривлення (фальсифікація) історії через перекручування історичних подій (історична міфотворчість). Вона є одним із способом управління свідомістю, впливу на світобачення як всередині Росії, так і впливу на українців. Визначено такі напрями цієї діяльності: показ історичної ідентичності російського і українського народів; історичні віхи походження Росії; фальсифікація історії у визначенні ролі і місця росіян у перемозі над німецько-фашистськими загарбниками у Другій світовій війні; причин сталінських репресій, тощо [2].

Основним координатором та регулятором участі наукових, навчально-наукових закладів РФ у інформаційній війні проти України є Російський Інститут стратегічних досліджень при Президентові РФ. Він визначає основні напрями наукової політики направленої проти України та інших держав. Так в березні 2014 року, в період активної фази „російської весни” в АР Крим, цим закладом було підготовлено ґрунтовну доповідь „Методи і технології діяльності зарубіжних та російських дослідницьких центрів а також дослідницьких структур та ВУЗів, що отримують фінансування із закордонних джерел: аналіз та узагальнення”. Цим документом визначено основ-

ні напрямки: зміни з політики лояльності державних структур, насамперед спецслужб РФ щодо діяльності низки наукових, громадсько-наукових структур, які існували і існують в цій державі, до рекомендацій, стосовно окремих з них про вжиття заходів до згортання їх діяльності на терирії РФ. Цим документом було визначено такі організації: 1) „Московский центр Карнеги", філія „Фонду Карнеги За міжнародний мир" (Carnegie Endowment for International Peace); 2) Російська асоціація політичної науки (РАПН) - загальноросійська громадська організація, яка об'єднує в своїх рядах політологів з різних регіонів РФ; 3) Центр політичних досліджень Росії (ПІР-Центр); 4) Інформаційне бюро НАТО в Москві; 5) Автономна некомерційна організація „Центр Юрія Левади" (АНО Левада-Центр); 6) Російська економічна школа (РЕШ, англ. – (New Economic School, NES) - вищий освітній заклад, що спеціалізується на розвитку „сучасної економічної освіти в Росії" і дослідженнях російського суспільства, бізнесу і держави; 7) Фонд „Нова Євразія" (ФНЄ), - російська некомерційна організація; 8) Російська асоціація міжнародних досліджень (РАМД) створена в 1999 році [3].

Сама Росія готує фахівців до участі в протиборстві в сучасній інформаційній війні. У багатьох вишах Росії для студентів ведуться курси з інформаційної, психологічної безпеки, кібербезпеки тощо. Окрім того, у де-яких школах Росії читають спецкурс для учнів 11 класу "Інформаційна війна з кіберзлочинами, кіберекстремізмом і кібертероризмом". І це ще не все там працюють численні "фабрики тролів", які забезпечують підривну діяльність у соцмережах, розхитуючи наше суспільство зсередини [4]. У школах України немає навіть натяку на таку роботу. Лише в Національному університеті імені Тараса Шевченка на факультеті журналістики запроваджено курс "Інформаційні війни".

Таким чином, з урахуванням вище викладеної практики організації інформаційного протиборства потребує кореляції її організації її в Україні. Доцільно, більш активне і цілеспрямоване задіяння наукових та навчально-наукових закладів України у інформаційному протиборстві, підготовці для цього кадрів. Одним із механізмів здійснення заначеного є впровадження в практику підготовки спеціалістів у цивільних вузах України фахівців за спеціальністю „Національна безпека" а також доведення до учнів випускних класів шкіл питань, що стосуються інформаційного протиборства та формування навиків протистояння інформаційно-психологіфчному впливу на особу.

Література.

1. Почепцов Г. Информационные войны» /Г. Почепцов// - Пропаганда и контрпропаганда – 2004 - [Электронный ресурс] - Режим доступа: http://psyfactor.org/autors/pocheptsov.htm

2. Тюняев А. Фальсификация истории это - оружие. URL: http://ru-an.info/новости/.

3. Российскитй институт стратегических исследований. Доклад „Методы и технологии деятельности зарубежных и российских исследовательских центров, а также исследовательских структур и ВУЗов, получающих финансирование из зарубежных источников: анализ и обобщение”. URL: https://riss.ru/analitycs/5043/

4. Колотій Н. Реалії інформаційної війни в Україні. URL: http://www.milnavigator.com/reali%D1%97-informacijno%D1%7-vijni-v-ukra%D1%97ni/

УДК 371. 134-057.875:81’ 243

Ромащенко І.В.,
кандидат педагогічних наук, доцент
Інститут спеціального зв’язку та захисту інформації
НТУУ «КПІ імені Ігоря Сікорського»

ІНОЗЕМНА МОВА ЯК КОМУНІКАТИВНА СКЛАДОВА ЗДІЙСНЕННЯ НАУКОВО-ДОСЛІДНОЇ ДІЯЛЬНОСТІ МАЙБУТНІМИ ФАХІВЦЯМИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Удосконалення змісту вищої освіти в цілому на сучасному етапі визначається не лише принципами інтеграції України в європейський та світовий освітній простір, переходом до ринкових відносин, що визначають вимоги до фахівців з вищою освітою, але і глобальною інформатизацією усіх сфер діяльності суспільства, конвергенцією інформаційно-комп’ютерних технологій тощо.

Відповідно значно зростає і потреба у фахівцях, здатних забезпечити безперешкодний доступ до інформації, якісно нею оперувати, обробляти отримані дані на науковій основі, компетентно захищати інформаційні системи та ресурси держави.

Стратегічна важливість підготовки фахівців, здатних ефективно протидіяти зовнішній інформаційній агресії, визначена системними законодавчими актами та нормативними документами серед яких «Доктрина інформаційної безпеки України», затверджена Указом Президента України від 25 лютого 2017 року № 47/2017, розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» та інші.

Зазначені вище документи визначають мету, базові принципи,

стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм реалізації цих завдань з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року. Ці документи надають не лише трактування понять «інформаційної інфраструктури» та інших, але і визначають умови розвитку інформаційного суспільства, підкреслюють важливість якості освітнього процесу у вищій школі, необхідність організації наукових досліджень та встановлюють пріоритетні завдання розвитку інформаційного суспільства у тому числі і створення відкритої мережі освітніх ресурсів; національного науково-освітнього простору, який має ґрунтуватися на об'єднанні різних національних багатоцільових інформаційно-комунікаційних систем; розроблення методологічного забезпечення у частині використання комп'ютерних мультимедійних технологій у процесі викладання навчальних дисциплін; удосконалення навчальних планів, відкриття нових спеціальностей з новітніх інформаційно-комунікаційних технологій. Нові завдання ставляться і перед вищою школою щодо організації науково-дослідної діяльності.

Науково-дослідна робота – це невід'ємна складова освітньої діяльності, що включає в себе сукупність мотиваційної сфери студента, забезпечення якої бере на себе педагог, методів і форм наукового пізнання, необхідних для повноцінного дослідницького процесу; формування усвідомлення студентами цінності та сенсу науково-дослідної діяльності; перетворення курсанта в суб'єкта дослідницької діяльності в процесі пошуку шляхів вирішення проблемних ситуацій; створення освітнього середовища, спрямованого на розвиток пізнавального інтересу і самостійність студентів; досягнення якісного кінцевого результату як сатисфакція виконаних досліджень. Водночас якісні наукові дослідження здобувачів вищої освіти освітньо-наукового та наукового ступенів вимагають значних комунікативних вмінь, які б могли забезпечити доступ до спеціальних наукових джерел, виданих іноземними мовами. Крім того, відповідно до Закону України «Про вищу освіту», значних обертів набирає процес мобільності: наукової, мовної, академічної, кредитної тощо. Нагальною є потреба здобувачів вищої освіти у володінні іноземною мовою на рівні, який дозволяє сприймати інформативний матеріал і виконувати завдання, які перед ними висуває процес здобуття вищої освіти в умовах загальноєвропейської та глобальної інтеграції, сучасних інформаційних і організаційно-діяльнісних технологій.

В умовах специфіки наукових цілей фахівців сфери захисту ін-

формації, поєднаних з їхньою професійною відповідальністю за забезпечення безпеки держави, іноземна мова є об'єктивною умовою здійснення комунікації під час наукових семінарів, конференцій тощо. Знання мови забезпечує ефективне позиціонування науковцями державних інтересів на міжнародному рівні, здатність не лише демонструвати свою компетентність, а і відстоювати свою позицію відповідними аргументами.

Наразі опанування іноземною мовою, яка є інтегративною складовою компетентнісної підготовки фахівців сфери захисту інформації, передбачає формування у здобувачів вищої освіти здатності до: проведення критичного аналізу, оцінки і синтезу нових ідей іноземною мовою; знаходження, обробки й аналізу необхідної інформації для рішення проблем й прийняття рішень у практичних умовах; використання сучасних методів і технологій наукової комунікації; лаконічно та аргументовано описувати проблеми, задачі та окреслювати стратегію їх розв`язання; до ефективного використання іноземної мови у професійних та академічних цілях; аналітичного опрацювання аутентичного англомовного матеріалу в сфері захисту інформації; аналізувати ситуацію, реагувати на запитувану інформацію та адекватно брати участь і представляти професійні інтереси у міжнародних наукових конференціях, симпозіумах; проводити наукові дослідження з використанням англомовних наукових джерел, ефективно підтримувати комунікацію за відповідною науковою тематикою у науковому та академічному середовищі;, брати участь у обговоренні актуальних наукових тем за своєю спеціальністю; письмово оформляти результати наукових досліджень у вигляді тез, статей, аналітичних доповідей, монографій тощо.

Таким чином, питання обсягів вивчення іноземної мови в науковій підготовці потребує практичного втілення у навчальних планах підготовки здобувачів вищої освіти спеціальностей галузі знань 12. Інформаційні технології.

Савич О.С.
кандидат юридичних наук, доцент
Національний університет «Одеська морська академія»

ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ У ТОРГІВЕЛЬНОМУ МОРЕПЛАВСТВІ

Глобальна комп'ютеризація сучасного суспільства, зачіпає практично всі сторони діяльності людей у тому числі і галузь торгівельного мореплавства.

Збільшені обсяги перевезень дають поштовх процесу оптимізації документальних процедур, які застосовуються у міжнародній морській практиці, шляхом впровадження системи електронного документообігу.

Під час торгівельного мореплавства відбувається безперервний процес обміну інформацією. Цей процес можна поділити на декілька груп. Перша група стосується обміну даними між вантажовідправником, вантажоотримувачем та адміністрацією судна з питань комерційної експлуатації судна. Друга група – між судновласником або фрахтівником та адміністрацією судна з питань безпеки судноплавства. Третя група стосується обміну даними між адміністрацією судна та портовими, митними службами з питань контролю та оформлення вантажів та судна в порту прибуття. Окрім вищеназваного, слід зазначити, що відбувається особистий обмін інформацією між моряком та його родиною.

Отже, загрози для судових інформаційних ресурсів можуть бути у вигляді: несанкціонований доступ до каналів супутникового обміну між судном та офісом його керування; викривлення навігаційних GPS-даних, які отримуються судном; несанкціонований доступ до супутникового каналу оперативного керування судном.

Усі, вище наведені групи відносин, містять життєво важливу (конфіденційну) інформацію для суб'єктів цих відносин. Втручання в таку інформацію може спричинити негативні наслідки у вигляді порушення роботи систем судна, що може привести до морської аварії; руху судна по хибній траєкторії; несанкціоноване розповсюдження комерційної або особистої інформації, що може привести до фінансових витрат; неповноту, невчасність та невірогідність інформації, щодо технічних характеристик судна, що може привести до додаткових затрат часу та фінансів та інш.

Наприклад, потрапляння вірусу до головного судового комп'ютера може привести до зупинки двигуна. Судно лягає у дрейф. Якщо це трапиться у зоні інтенсивного руху, відбудеться зіткнення суден.

Головною метою зловмисників при їх атаках на інформаційні ресурси суден є їхні навігаційно-інформаційні системи та системи оперативного морського зв'язку. Для їх захисту використовують апробовані на практиці стандартні заходи: криптографічне кодування, політику паролів, електронний цифровий підпис тощо.

Наприклад, для захисту офіційних векторних карт Міжнародною гідрографічною організацією (International Hydrographic Organization, IHO) розроблено спеціальний стандарт S63 «IHO Data Protection

Scheme», який визначає перелік заходів з метою: попередження несанкціонованого копіювання електронних навігаційних карт; обмеження доступу тільки до тих карт колекції, на які користувачем отримано доступ; забезпечення гарантії того, що електронні навігаційні карти надійшли з уповноваженого джерела.

На сьогоднішній день велика кількість судноплавних компаній та зовнішньоторговельних фірм відповідно до Конвенції з полегшення міжнародного морського судноплавства прагнуть використовувати під час перевезення вантажів морем електронних систем обміну інформацією. Це пов'язано з тим, що процес обробки паперових документів породжує велику кількість проблем (затримка у підготуванні, обробці, обміну документів; велика трудомісткість управління документообігом та інш.).

У зв'язку з цим, в практиці морських перевезень використовуються різні системи електронного обміну інформації: Electronic Date Exchange – EDI, Electronic Date Interchange for Administration, Commerce and Transport – EDIFACT, Bill of Lading for Europe – Bolero та інші).

В 1990 р. Міжнародної морський комітет (ММК) схвалив Єдині правила для електронних коносаментів (Rules for Electronic Bills of Lading), які застосовуються тільки за згодою сторін.

В основі цих правил ММК лежить концепція не центрального реєстру (у який може бути зданий на зберігання оригінал коносамента, а права на товари передаються шляхом обміну однозначно визнаними аутентфіцированним повідомленням між таким реєстром і подальшими сторонами, що мають права на вантаж, або безпосередньо, або на підставі застави), а ''конфіденційного ключа".

Система призначена для використання окремим перевізником, хоча за наявності центрального реєстру вона може використовуватися і групою перевізників.

У 1996 році був прийнятий Типовий закон ЮНСІТРАЛ про електронну торгівлю та у 2001 році був прийнятий Типовий закон ЮНСІТРАЛ про електроні підписи. Ці акти є основою не тільки міжнародних електронних проектів документообігу, а й профільного національного законодавства різних країн.

Першим нормативним актом з організації обміну інформаційними повідомленнями на морі стала Резолюція Асамблеї ІМО від 15 листопада 1979 р. про "Розвиток системи передачі повідомлень про лихо і безпеку на морі". Ця система визначається як координоване використання різних елементів, включаючи радіозв'язок, з метою охорони людського життя на морі.

Важливу роль у правовому забезпеченні інформаційної діяльності для безпеки мореплавства і охорони людського життя на морі відіграють ”Загальні принципи систем суднових повідомлень”, схвалені 13 сесією Асамблеї IMO 17 листопада 1983 р. Системи суднових повідомлень використовуються для збору інформації або обміну нею за допомогою радіоповідомлення.

Значну роль відіграє наявність на судні Автоматичної Ідентифікаційної Системи (AIC). Згідно з правилом V/19 Міжнародної конвенції з безпеки життя на морі SOLAS-74 з поправками усі судна тоннажністю понад 300 тонн, які здійснюють міжнародні рейси, і всі пасажирські судна незалежно від розміру мають бути оснащені AIC. Основні функціональні вимоги щодо суднової AIC зафіксовано в основоположній Резолюції IMO MSC.74(69), 1998. Технічні стандарти стосовно AIC розроблено в Рекомендації ITU-RM.1371,1998. Керівництво з використання суднової AIC дається в Резолюції IMO 917(22), 2001.

Очевидно, що на даний час у світі активізувались розробки програмно-технічних засобів, які спроможні перехоплювати потоки інформації з борту суден та активно впливати на процес їх експлуатації. Це створює загрозу торгівельному мореплавству і актуалізує задачу розробки дієвих механізмів міжнародно-правової протидії інформаційним загрозам.

Дослідження правової природи загроз інформаційній безпеці торгівельного мореплавства через їх зміст та класифікацію дає змогу покращити механізм державного забезпечення інформаційної безпеки мореплавства; на законодавчому рівні розмежувати різні види загроз інформаційної безпеці торгівельного мореплавства.

Транскордонний характер загроз інформаційній безпеці торгівельного мореплавства обумовлює потребу у виробленні і реалізації комплексних зусиль держав і міжнародних організацій для ефективної протидії їм.

Савінова Н.А.
доктор юридичних наук,
старший науковий співробітник
Національний університет «Одеська морська академія»,
НДІ інформатики і права НАПрН України
Осадчук Д.Д.
Національний університет «Одеська морська академія»

ТРЕНД «МОРСЬКА БЕЗПЕКА» ЯК СТРАТЕГІЧНА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Наміри України стати європейською країною, пов'язані, насамперед, з обійманням у глобальному ринку статусу безпечної економічно цікавої для світу країни з позитивним іміджем. Очевидно, що інформаційна безпека країни стосується, в цьому контексті, не лише внутрішньої безпеки, а і безпеки країни для світу, яка має відображуватися у об'єктивній позитивній оцінці учасників економічних відносин з Україною. Основним транспортним засобом товарообміну зі світом з України лишається морське судноплавство, і саме тому море сьогодні для нашої країни є не лише політичним та воєнним форпостом, а й найголовнішим каналом найвигідніших торговельних комунікацій зі світом. Інформація ж про морську безпеку в цьому сенсі стає критерієм прийняття рішень щодо торговельних та туристичних відносин, які здійснюються морем.

Радою національної безпеки і оборони України (далі – РНБО) 6 травня 2015 року було схвалене Рішення «Про Стратегію національної безпеки України»[1] (далі – Стратегія НБ), в якій зазначено: «Ця Стратегія національної безпеки України спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС[2], ратифікованою Законом України від 16 вересня 2014 року № 1678-VII[3], і Стратегією сталого розвитку "Україна - 2020", схваленою Указом Президента України від 12 січ-

[1] Рішення Ради національної безпеки і оборони від 6.05.2015 р., введене в дію Указом Президента України від 26 травня 2015 року № 287/2015 [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0008525-15 - Назва з екрану.

[2] Угода про асоціацією між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014 р. // Офіційний сайт Верховної Ради України [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/984_011/page - Назва з екрану.

[3] Закон України Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 16.09.2014 № 1678-VII [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/1678-18 - Назва з екрану.

ня 2015 року № 5[4]». Всі вказані у Стратегії НБ посилання, умовно можна об'єднати у групу актів, вектори яких спрямовані на досягнення стану безпеки, який сприяв би євроінтеграції країни.

Серед ***головних цілей Стратегії НБ*** визначені *утвердження прав і свобод людини і громадянина, забезпечення нової якості економічного, соціального і гуманітарного розвитку, забезпечення інтеграції України до Європейського Союзу та формування умов для вступу в НАТО.* ***Одним з пріоритетних напрямів утвердження стану безпеки країни у Стратегії НБ*** визначене «*формування ключових передумов, необхідних для набуття Україною членства в ЄС - важливої гарантії демократичного розвитку, економічного добробуту та зміцнення безпеки. Членство України в ЄС сприятиме покращенню клімату довіри і безпеки в регіонах Східної Європи та Чорного моря» (п. 4.6.) (курсив наш,* ***Н.С., Д.О.****).*

Безпосередня вказівка на потребу забезпечення морської безпеки в країні містяться в положенні ст. 135 Угода про асоціацією України з ЄС з посиланням на Договір про заснування Європейської Спільноти[5] - стосовно *реалізації основних правил міжнародних морських перевезень ЄС (курсив наш,* ***Н.С., Д.О.****).*

Стратегією сталого розвитку "Україна - 2020" визначено основні вектори руху України «вектори руху», до яких належать: вектор розвитку, вектор безпеки, вектор відповідальності і вектор гордості. Зокрема, вктор безпеки описаний як «… забезпечення гарантій безпеки держави, бізнесу та громадян, захищеності інвестицій і приватної власності. *Україна має стати державою, що здатна захистити свої кордони та забезпечити мир не тільки на своїй території, а й у європейському регіоні./…/»*[6] (*курсив наш,* ***Н.С., Д.О.***).

Очевидно, що всі вказані позиції, тією чи іншою мірою, але всі (!), стосуються Морської доктрини України на період о 2035 року (далі – Морська доктрина) [7]. У 2008 р., на обгрунтування тоді ще проекту цієї доктрини, Б. Буркинський, О. Котлубай, В. Степанов визначали: «… *стійкі тенденції витіснення нашої держави з міжнародного сектора морегосподарської діяльності - світового морського транспортного ринку*, а також рибопромислового, рекреа-

---

[4] Указ Президента України Про Стратегію сталого розвитку "Україна - 2020" [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/5/2015 - Назва з екрану.

[5] Договір про заснування Європейської Спільноти від 25.03.1957 [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_017 - Назва з екрану.

[6] Там же.

[7] Постанова Кабінету Міністрів України Про затвердження Морської доктрини України на період до 2035 року від 07.10.2009 № 1307 [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/1307-2009-%D0%BF - Назва з екрану.

ційно-туристичного та ін.; *значне погіршення геоекономічних і геостратегічних позицій України на просторах Чорного моря* й інших районів Світового океану»[8] (*курсив наш,* ***Н.С., Д.О.***). Отже, саме подолання таких вад була направлена у 2009 р. Морська доктрина. Утім, під впливом економічної складової гібридної війни, починаючи з 2013 р., Морська доктрина мала бути переглянута і удосконалена. Однак, хоча і з запізненням, але ж таки прийняте у 2015 р. таке рішення (пп. 5 п. 3 Рішенні РНБО 26 травня 2015 р. № 287/2015 КМУ доручалося «затвердити у тримісячний строк нову редакцію Морської доктрини України»[9]). Але до цього часу Морська доктрина України модернізована не була.

Утім, зміст цього документу, фахово сформованого і орієнтованого на визначення пріоритетні саме безпеки економічних відносин як основи міжнародного брендінгу України[10] - «… України як морської держави, створенню сприятливих умов для досягнення цілей та розв'язання завдань з розвитку морської діяльності»[11] та «Забезпечення захисту національних інтересів України як морської держави потребує визначення пріоритетів її державної морської політики до основних засад внутрішньої та зовнішньої політики держави»[12]. Очевидно, що *ці обидва компоненти мають гарантуватися, у тому числі, безпековою складовою у державній морській політиці (А), а також окремо предбачатися як необхідний для убезпечення стратегічний сегмент політики національної безпеки України (Б)*.

Отже, очевидно, що вказана доктрина, як документ фаховий, але - політичний, визнаний РНБО необхідним для модернізації, яка, до речі, доручена була у 2015 р. Національному інституту стратегічних досліджень при Президенті України, і про необхідність конкретних новацій якої ще у жовтня 2014 р. говорили експерти цього НДІ[13], безпосередньо пов’язуючи необхідність перегляду Морської доктрини у безпеко-

---

[8] Буркинський Б., Котлубай О., Степанов В. Формування Морської доктрини України // Вісник Національної академії наук України. - 2008. - № 9. – С. 6-11. – С. 6.

[9] Рішення Ради національної безпеки і оборони від 6.05.2015 р., введене в дію Указом Президента України від 26 травня 2015 року № 287/2015 [Текст] // Офіційний сайт Верховної ради України [Електронний ресурс]/ Режим доступу: http://zakon3.rada.gov.ua/laws/show/n0008525-15 - Назва з екрану

[10] Під «брендінгом України» ми розуміємо «цілеспрямований і вмотивований процес організації, планування, впровадження і моніторингу маркетингової, політико-дипломатичної, економічної та громадської діяльності зі стратегічного просування й належного позиціонування країни в глобальній економічній системі, формування нових та ефективне використання наявних конкурентних переваг країни та її суб’єктів господарювання на світових ринках, створення позитивного іміджу держави та підтримка її репутації для повнішої та результативнішої реалізації національних інтересів у глобальному середовищі» - за визначенням Г.Г.Полішко [Полішко Г.Г. Національний брендінг у глобальній екномічній системі: Автореферат дисс….канд екон. наук: 08.00.02. – Кив, 2016. – 19 с. - С. 4]

[11] Там же.

[12] Там же.

[13] Горовенко В., Тютюнник В. Виклик часу: перегляд морської політики України та відтворення її військових сил // Web-ресурс «Центр исследования армии, конверсии и разоружения» [Електронний ресурс]/ Режим доступу: http://cacds.org.ua/ru/comments/360 - Назва з екрану.

вій, насамперед, для економічних відносин, парадигмі.

Що ж відбувається в реаліях морської безпеки сьогодні? Які явища породжує відсутність належного комплексу забезпечення морської безпеки на політичному, законодавчому та правозастосовчому рівні в нашій раїні сьогодні? Іншими словами: які небезпечні явища утворюють негативний імідж України – морської держави, заваджуючи розвитку безпечних економічних відносин та інвестицій в сфері використання моря?

Сьогодні Україна, є одним зі світових лідерів, який володіє найпотужнішим портовим потенціалом серед всіх країн Чорного моря. На узбережжі Чорного і Азовського морів перебувають 18 морських торгових портів і 12 портових пунктів. Найбільш значимими є порти Одеса, Чорноморський і Південний. На їх частку припадає понад 60% усього вантажообігу.

У той же час, неприйнятні для безпечного мореплавства явища, що ескалують останній часу морській сфері, є лише шкідливими для економіки держави, а й утворюють негативну іміджеву - інформаційну складову, підриваючи довіру у відносинах України з країнами ЄС.

Торгівля людьми і зброєю, наркотрафік, незаконна міграція, шахраство з вантажами - це неповний перелік дектруктивних для безпеки мореплавства і морської безпеки в цілому явищ, що системно здійснюються в південно-західному морському секторі.

Українські порти Одеса, Чорноморське за оцінкою зарубіжних ЗМІ і представників страхових компаній, є портами підвищеної зоною ризику, пов'язаних зі страховими випадками розкрадань вантажів. Так, наприклад, товари, що перебувають у 20 фунтових морських контейнерах, після проходження оброки в портах України, товару зникають повністю або частково, що з’ясовується вже на території країн надходження товарів.[14]

Україна є одним лідерів експорту сипучих вантажів: зерно, кукурудза, рапс і т.д. Сипучий вантаж, що відправляється на балкер в країни одержувача (Європи, Азії і т.д.) може бути піддано так званому карантинному фітосанітарному знезараженню - фумігації. При фумігації даного виду вантажів в трюм закладаються фумігаційні патрони і пакети, які виділяють отруйний газ з метою ліквідація комах і дрібних гризунів задля недопущення їх потрапляння в інші країни.

При порушенні технологи фумігації, надмірне виділення фос-

[14] Так, зокрема, у березні 2017 р. правоохоронними органами було затримано групу злочинців, які вчинювали викрадення, займаючись контейнерними перевезеннями. По шляху проходження в порт, учасники даної злочинної схеми відхилялися від маршруту, і, заїжджаючи на заздалегідь підготовлені бази, товар з контейнерів частково, або повністю відвантажували. При цьому цілісність пломб не порушувалася і контейнера відправлялися одержувачу. При отриманні контейнерів країна-одержувач починала процедуру з виявлення причин відсутності товару і конпенсаціі заподіяної шкоди з України.

фінів може завдавати шкоди здоров1ю і, навіть, життю екіпажу. Екіпажу судів, на яких здійснюється фумігація, повинні видаватись захисні костюми, газоаналізатори парів отруйних речовин і медикаменти для надання першої допомоги в разі отруєння члена екіпажу. В силу зношеності судів і некомпетентності фірм, які здійснюють фумігацію, часто відбувається масове отруєння екіпажів суден. Компанії, які представляють Україну на міжнародному ринку в силу даних інцидентів караються багатотисячними штрафами через неякісно проведених фумігаційних операцій, залишки таблетованих пакетів, присутність комах у вантажі) пожежам через скупчення газів в трюмах і отруєння моряків. Такі небезпеки відверто «відштовхують» крани світу від роботи на морі в портах України.

Ще однією з нагальних проблем морського регіону України є незаконна міграція морем. Утім, така забезпечення такої міграції в регіоні півдня носить характер промислу. Через український сектор Чорного моря нелегали намагаються потрапити спочатку до Туреччини, а потім - в Італію та Грецію.[15]

Існує ще низка негативних фактів, що заважають добросусідським відносинам з країнами ЄС. Це торгівля зброєю і наркотрафік. В силу того, що Україна знаходиться в стані збройного конфлікту на Донбасі, маса зброї накопичується у злочинних угруповань, які чекають своєї реалізації в зонах конфліктів. Прикладом є затримання в Середземному морі німецького судна, яке було зафрахтоване українською компанією і нібито прямував до Сирії.

Стосовно наркотрафіку, то щорічно через порти Одеса, Чорноморське і Скадовськ водним шляхом в країни ЄС проходять з Афганістану, Туреччини і країн Кавказу потрапляють важкі наркотики: кокаїн, героїн. З Індії та Китаю - синтетичні наркотики. Правоохоронні органи ЄС постійно б'ють на сполох через те, що контрабанда наркотичних засобів з України зростає. Частина товару осідає в самій Україні. Про це йдеться в щорічному звіті Европола про ситуацію на наркоринку, і ця ситуація буде погіршуватися, оскільки, фактично знищена система управлінь по боротьбі з незаконним обігом наркотиків в країні, і, зокрема, на морі.

Тенденції негативного характеру, що з'являється в портово-господарчому комплексі України, можуть призвести до торгово-економічних втрат на світовому ринку, зруйнувавши статус України як сильного і надійного морського партнера. Внаслідок цього може

[15] Так, наприклад, у березні 2017 р. берегова охорона Туреччини затримала українську яхту з 4 членами екіпажу, на борту якої знаходилося 83 нелегальних мігранта з Сирії. Один із членів українського екіпажу раніше затримувався за підозрою в торгівлі людьми. Також у квітні 2017 р. біля берегів Сицилії було затримано 8 українських контрабандистів. На їх яхтах знаходилося по 30 осіб, які намагалися незаконно перетнути кордон Італії.

відбутися витіснення нашої держави з міжнародного сектора морегосподарської діяльності. Ця діяльність суперечить позиціям забезпечення захисту національних інтересів України як морської держави.

У той же час, серед напрямів національної безпеки і цілому напрям «морська безпека» не визначений: він не міститься ані в законах, ані на рівні напрямів політико-правових актів безпекового характеру. Зокрема у самій Морській доктрині він також не виділений, хоча самий термін «безпека» (без змістовного наповнення власне поняття, зустрічається у термінопоняттях «безпека держави», «безпека судноплавства», «екологічна безпека», «безпека морської та морегосподарчої діяльності [України]», - всієї групи безпекових компонентів, що мають включатися в обсяг комплексного векторного тренду.

Очевидно, що, розробка напряму «Морської безпеки» має виступати одним зі стратегічних напрямів НБ і комплексно охоплювати і передбачати всі напрями безпекових складових об'єктів Морської доктрини. Саме цей напрям НБ, у разі виділення його сфери і прямих та опосередкованих складових з Стратегії НБ, на рівні реалізації її в Морській доктрині України має приймати на себе тягар інкорпорації: сама суть Морської безпеки, її цілі і завдання, шляхи реалізації мають виступати первинними ключовими факторами змін Морської доктрини України до 2035 року.

УДК 341.338.47

Сервецький І.В.
доктор юридичних наук, доцент
Національна академія Служби безпеки України

ДЕЯКІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Одним із найважливіших напрямків національної безпеки є інформаційна безпека України. Проблема інформаційної безпеки стала особливо актуальною у наш час, коли використання інформаційних технологій поширилось практично на всі сфери суспільного життя, що знаходяться під захистом Конституції [1].

Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою забезпечення національної безпеки.

Національна безпека - захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах інформаційної безпеки [2]. Стратегія національної безпеки

полягає в тому, що як найефективніше використати інформаційний ресурс держави та забезпечити сталий розвиток суспільства [3].

Інформаційна безпека, в першу чергу, передбачає правове визначення інформації як стратегічно важливого для держави ресурсу, створення взаємопов'язаної системи інформаційних масивів держави різного рівня, їх призначення, а також контроль державних органів, що відповідають за формування, зберігання, використання і захист цих масивів, визначення прав, обов'язків, гарантій забезпечення прав і відповідальності суб'єктів інформаційних відносин, ліцензування і сертифікація найважливіших видів інформаційної діяльності, чітке законодавче визначення виду, типу обсягу інформації з обмеженим доступом, її використання, створення загальної системи забезпечення інформаційної безпеки [4].

Отже, важливими елементи інформаційної безпеки є: захист, контроль, конфіденційність.

Захист інформації - це комплекс правових, організаційних, інформаційно-телекомунікаційних засобів і заходів, спрямованих на запобігання неправомірним діянням щодо інформації [4].

Захищеність інформаційної сфери України це дотримання вимог чинного законодавства щодо неприпустимості розповсюдженню інформації, яка містить ознаки кримінального правопорушення, особливо щодо закликів до насильницької зміни конституційного ладу і захоплення влади, порушення територіальної цілісності держави, пропаганди війни, насилля, жорстокості, розпалювання расової, національної, релігійної ворожнечі, запобігання розміщенню відомостей, що становлять державну таємницю, чи відомостей з обмеженим доступом, а також захист інформації, щодо порушення конституційних прав і свобод особистості, державної таємниці, збереження важливої для суспільства , держави.

Контроль за національним інформаційним простором – заходи щодо мінімізації збитків від здійснення як іноземними державами, так і внутрішніми організаціями підривних операцій.

Що стосується компетенції державних органів у сфері охорони державної таємниці, так цей обов'язок покладений на Службу безпеки України [5].

Правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних [6].

Запобігання витоку конфіденційної інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації що є власністю держави, запровадження цензу-

ри, на окремі виді діяльності у політичних та економічних структур, окремих громадян в інформаційній сфері, протидія непередбачених ситуацій у системах, процесах, що ґрунтуються на використанні інформаційних технологій, внаслідок чого зростає ступінь ризику заподіяння збитків, а також їх розмірів, недосконалість чи відсутність технічних засобів забезпечення інформаційної безпеки.

Тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи розголошенню інформації, одержаної конфіденційно може бути встановлений інший порядок доступу до публічної інформації [7].

Крім того, забороняється оприлюднювати або надавати (розголошувати) зібрані відомості, а також інформацію щодо проведення або не проведення стосовно певної особи контррозвідувальної діяльності та заходів до прийняття рішення за результатами такої діяльності або заходів [8].

Отже, Інформаційна безпека України передбачає правове визначення інформації як стратегічно важливого ресурсу для держави, створення взаємопов'язаної системи інформаційних масивів держави, а також доступ до них СБУ, які повинні забезпечити безпеку інформаційних систем, але й контролювати доступ до них та запобігати незаконному проникненню, використанню іноземними спецслужбами.

Тому, пропонуємо внести зміни до законодавчих актів, які надають право спецслужбі (СБУ) мати доступ до усіх інформаційних ресурсів держави: правоохоронних органів, комерційних структур та приватних інформаційних ресурсів для ефективного забезпечення національної безпеки України.

Література

1.Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Про основи національної безпеки України. Закон України. //Відомості Верховної Ради України //, 2003, № 39, ст.351)

3. Указ Президента України "Про рішення Ради на" національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" від 26 травня 2015 року № 287/2015 // Офіційний вісник України. 2015. № 43. С. 14. Ст. 1353.

4. Про інформацію. Закон України. Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650.

5. Закон України "Про Службу безпеки України" // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

6. Про захист персональних даних.Закон України. // Відомості Верховної Ради України, 2010, № 34, ст. 481**)**

7. Про доступ до публічної інформації. Закон України. //Відомості Верховної Ради України, 2011, № 32, Ст. 314.

8. Закон України "Про контррозвідувальну діяльність" // Відомості Верховної Ради України. – 2003. – № 12. – Ст. 89.

УДК 81’371:81’42

Слухай Н.В.
доктор філологічних наук, професор
Інститут філології КНУ імені Тараса Шевченка

ЛІНГВІСТИЧНІ МАРКЕРИ ЗАМАСКОВАНОЇ СВІТОГЛЯДНОЇ ПОЗИЦІЇ СУБ’ЄКТА МАС-МЕДІЙНОЇ ІНТЕРАКЦІЇ

Світоглядні війни сучасності відзначаються надзвичайною роллю інформації та її провайдерів – мас-медіа – у формуванні ставлення до подій війни, реальних, сфальшованих або вимишлених, з боку колективного та індивідуального суб’єкта – сугеренда, тобто суб’єкта, на якого спрямований сугестивний (впливовий в обхід раціонального мислення) дискурс. За урахування налаштованості прокремлівських рупорів на хаотизацію світу та на активізацію ресурсів маскування позиції мас-медійного джерела ідентифікація напрямку формування суспільної думки учасником мас-медійної інтеракції становить неабиякі труднощі і потребує ідентифікації маркерів текстів «замаскованої ворожості».

Теоретичні засади дослідження мови як соціальної практики вивчені фахівцями у галузі дискурсології, особливо у межах критичного дискурс-аналізу, зокрема, П.Серіо, Ю.Степановим, Р.Водак, Н.Фейркло, Т.ван Дейком для ідентифікації вербалізаторів особливого ментального світу – мови радянського політичного дискурсу, мови влади Великобританії, мови соціального відторгнення іммігрантів у Австрії 1990-х років і таке інше. Віднайдені вербалізатори не склали системи; з-посеред них опинилися, зокрема: оцінні вирази, негативні епітети, негативний коментар, протиставлені ми- та вони-дискурси, когнітивні метафори, стереотипи, генералізація, номіналізація, пасивізація / активізація та подібні. Але, навіть не систематизовані, вербалізатори певного ментального світу виступали маркерами «міфології епохи» (Ю.Степанов). Так само, особливо за урахування повторюваних конструкцій, які використовують рупори прокремлівської риторики, можна визначити «формуючу плівку мови» сучасної світоглядної війни проти України. Дослідження, зокрема, змісту публікацій газети «Вести» засвідчило, що для ідентифікації

позиції мас-медіа достатньо тестувати заголовки. Решта основних сильних позицій – початок та кінцівка тексту – діє на свідомість реципієнта лише за умови прочитання публікації. Методом суцільної вибірки протягом березня-квітня 2017 року було вилучено 200 заголовків текстів, які стосувалися поточної політичної ситуації з метою визначення, якими мовними засобами в умовах світоглядної війни це мас-медійне джерело формує суспільну думку споживача інформації. З-посеред цих засобів центральне місце посіли негативні емоціогени різної референтної природи, введені в дискурс «мовними оболонками» кількох домінантних типів.

За типами відображення світу негативні емоціогени розподілилися на чотири групи: 1. **Негативні безреферентні емоціогени:** «У Украины **серьезные проблемы**, **Что творится** в Украине, **Что учудила** Украина». Особливе місце посідають прогнози страшного майбуття для світу, України, ключових фігур української політики: «Скоро начнется **война**; Над Украиной **нависла угроза**; Будущее Украины будет **страшным**; **Страшная** болезнь Порошенко». 2. **Слабореферентні сполучення з ключовим словом – негативним емоціогеном**: «**Издевательства** украинского правительства; Планы Киева **об атаке** на Россию; **Пагубность** европейского выбора Украины». Вони відрізняються від безреферентних наявністю уточнювача, який дозволяє зорієнтуватися в темі публікації, і посиленою емоційністю. 3. **Референтні сполучення – асоційовані провісники з ключовим словом – негативним емоціогеном**: «РФ стягивает войска; Мариуполь ментально готов; Украина распадется на четыре части». Специфіка цієї групи полягає у прихованій погрозі, яку читач подумки формулює за законами асоціативного мислення. До її складу входять **референтні сполучення із сакральними компонентами в негативному контексті**: «**Слово** на языке оккупантов; **Украины** больше нет и никогда не будет; **Геноцид украинской нации**; **Украина вымирает**». 4. **Засоби формування альтернативної референтності**: «**Кто же такой Бандера**?»

З-посеред мовних форм уведення негативного емоціогенну в дискурс зафіксовані: **сполучення з модальністю вірогідності** («Путин может забрать Донбасс; РФ готова нанести удар»); **висловлювання-псевдорезультати «розкриття» правди** («Новости взорвали соцсети; Всплыла запись»); **висловлювання, в яких бажане видається за дійсне** («Украина потеряла Мариуполь; Украины больше нет и никогда не будет»); **з модальністю безособової обумовленості** («Принято решении о присоединении Донбасса»); **лексичні і граматичні маркери меншовартості** (**на** Украине) **і зневаги** (москали, украинцы сами себя); **надактивні форми негації** («**Никто не**

хочет спасать Украину»); **метонімії** («**Газпром** оставил **Киев** с носом»); **новояз** («Оккупантоязычные»); **когнітивні метафори** («Загоните Киев в стойло, Пуля в сердце Украины»); **інвективи** («Гетто для дебилов; Неукраиноязычные дауны»); **усталені вирази із негативною семантикою** («Порошенко сдает позиции, Когда рванет курс»), **включно із залишками мови радянської епохи** («Разжигание межнациональной ненависти и вражды, Остановить агрессию»). Список лінгвістичних маркерів є відкритим, але інформативним щодо позиції джерела в мас-медійній інтеракції.

УДК 65.012.8+342.951

Столбовий В.М.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України
Черновський М.А.
Національна академія Служби безпеки України

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

Інформація, в наш час, є важливою складовою в усіх сферах суспільної діяльності. В українському законодавстві під інформацією розуміються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. З огляду на збільшення масивів електронної інформації і, зокрема, використання її в інформаційних (автоматизованих) системах постає питання комплексного та ефективного захисту такої інформації. Під захистом розуміється сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Важливими виступають основні поняття, що стосуються інформаційної сфери, зокрема, доступу до інформації, адже "право на інформацію визначається, передусім, доступом до неї" [1, с. 3].

Поняття доступу до інформації, на сьогодні, неоднозначно тлумачать, як науковці, так і законодавці. Загалом, доступ до інформації – це передбачений правовими нормами порядок її отримання, використання, поширення і зберігання [1, с. 3].

Деякі вчені розмежовують активне та пасивне право на доступ до інформації.

Активне право – це можливість безпосереднього ознайомлення з інформацією органів виконавчої влади, що реалізується шляхом

направлення громадянами запиту до органів виконавчої влади про надання інформації; відвідування відкритих робочих засідань органів влади; доступу до відкритих архівів офіційної інформації органів виконавчої влади [1, с. 3].

Пасивне право – це поширення інформації в засобах масової інформації, випуск спеціалізованих брошур і збірників, розміщення інформації в мережі Інтернет, на стендах офіційної інформації в приміщеннях, де розташовані органи виконавчої влади [1, с. 3].

У законодавстві низки європейських країн закріплене поняття "classified information", яке дехто з учених перекладає, як "класифікована інформація", посилаючись на те, що, окрім інформації, яка належить державі, такий вид охоплює ще й ті відомості, які держава на законних підставах зобов'язалася охороняти і, які можуть належати певним установам та відомствам (у тому числі комерційним), фізичним особам, навіть іноземним державам. Утім, термін "класифікована інформація" не притаманний національному законодавству України [1, с. 3].

Реалізація права на доступ до інформації з обмеженим доступом неможлива без процедури отримання допуску. Допуск – рішення, надане за результатами спеціальної перевірки, яким визначається, що фізична або юридична особа може проводити діяльність, пов'язану з інформацією з обмеженим доступом, згідно з національним законодавством [1, с. 3].

Адміністративно-правові заходи захисту інформації з обмеженим доступом – це сукупність методів, прийомів, засобів, які спрямовані на захист інформаційної безпеки громадян, суспільства і держави у всіх сферах їх життєво важливих інтересів. Сукупність цих заходів полягає у виявленні, вилученні та нейтралізації негативних джерел, причин і умов впливу на інформацію. Такі джерела становлять загрозу безпеці інформації, а методи адміністративно-правового захисту інформації з обмеженим доступом здійснюються з огляду на її зміст.

Тому зміст адміністративно-правового захисту інформації ототожнюється з процесом забезпечення інформаційної безпеки як необхідності нормального функціонування держави, суспільства, окремої людини.

Отже, на нашу думку, з метою захисту інформації в інформаційних (автоматизованих) системах необхідно забезпечити:

1. Створення відповідних умов для захисту приміщень, комп'ютерної техніки.

2. Облік та контроль за розповсюдженням, копіюванням інформації, діями персоналу.

3. Технічний захист доступу до баз даних (паролі, криптозахист).

4. Впровадження провідного досвіду зарубіжних країн щодо цих питань.

Література

1. Доступ до інформації з обмеженим доступом у країнах Європи (Литва, Болгарія, Румунія, Латвія, Словаччина): Оглядове видання. – К.: наук.-вид. відділ НА СБ України, 2008. – 52 с.

2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". URL: http://zakon.rada.gov.ua.

3. Шепета О.В. Адміністративно-правові засади технічного захисту інформації: дис. …канд.юрид.наук: спец. 12.00.07 // О.В. Шепета. – К.: 2011, НАСБУ. – 215 с.

Стрельбицька Л. М.
доктор юридичних наук, професор,
Заслужений працівник освіти України
Національна академія Служби безпеки України
Стрельбицький М.П.
доктор юридичних наук, професор,
Заслужений працівник освіти України.
Національна академія Служби безпеки України

АНТОЛОГІЯ ТА ІНСПІРУВАННЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

Інформаційний тероризм *(ІТ)* – в широкому розумінні – це система об’єднаних загальними мотивами та цілями злочинних дій як у фізичному, так і у електронному середовищі, пов’язаних з використанням методів автоматизованої обробки даних, заснованих на використані інформаційно-телекомунікаційних систем, що здійснюють маніпулювання суспільною свідомістю шляхом масованого поширення неправдивої і сфабрикованої інформації з метою створення напруженості у суспільстві, нестабільності, хаосу, спрямованих на реалізацію політичних чи економічних цілей в інтересах терористів. У вузькому розумінні – це кібератаки на інформаційні системи, що працюють в контурах управління державними і соціально важливими технологічними об’єктами і системами (атомними чи гідроелектростанціями, банками, хімічним виробництвом, авіацією та іншими видами транспорту тощо) з метою виведення їх із ладу, спричинення економічних, екологічних та інших катастроф. Тероризм узагалі, і духовний зокрема, являє собою діяльність, що виражається в залякуванні населення й органів влади з метою досягнення злочинних намірів.

***ІТ* полягає** також у спробах організації спеціальних медіа-

кампаній, покликаних зруйнувати знаково-символьну інфраструктуру суспільства, створити у ньому атмосферу громадянської непокори, недовіри до дій та намірів влади й особливо – її силових структур, що мають захищати суспільний порядок. Терористичні акти одноразові, мають знищуючу силу і пов'язані із національними або транснаціональними кримінальними структурами й спецслужбами іноземних держав. *ІТ* є особливим різновидом психологічного терору, який відносять до інфраструктурного, а саме – зловживання інформаційними системами, мережами та їх компонентами для здійснення терористичних дій та інших віднесених до них акцій. Здійснюється в області, що охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди й ідеї, тобто в духовній сфері, там, де ведеться боротьба ідей. В сучасних умовах став вагомим фактором «великої політики». Ця обставина реально означає істотний поворот в еволюції людства. Таким чином здійснюється нав'язування малою групою людей певної лінії поведінки владі і суспільству, що вже тепер починає відчутно проявлятися на політичному полі України. Суспільство виявилося не готовим до протидії цьому явищу – позначилися об'єктивні і суб'єктивні фактори.

На Заході *ІТ* часто ідентифікують із кібертероризмом, хоча, звичайно ж, вони дві частини одного явища. *ІТ* передбачає цілеспрямовані маніпуляції з інформацією, або її підтасування, а в деяких випадках і подача свідомо неправдивих фактів, у результаті якої відбувається залякування населення, поширюється паніка, настрої параноїдальних думок. На відміну від цього, кіберзлочини вчиняються з використанням нових технологій, наприклад пограбування банку через мережу або злом торговельних інтренет–площадок.

До факторів, що впливають на формування загроз інформаційній безпеці України відносяться: слабка інтегрованість у світове інформаційне поле; недостатня фаховість та активність її інформаційних служб, широке використання ЗМІ окремими політичними силами, які можуть залежати від організованої злочинності, мафіозних структур; формування неправдивого уявлення про Україну в світі засобами масової інформації інших, насамперед недружніх держав, які відстоюють свої власні інтереси; неможливість повноцінного протистояння інформаційно-пропагандистським та терористичним актам інших держав внаслідок слабкої матеріально-технічної бази і недостатнього фінансового забезпечення.

Відмінною рисою *ІТ* від кримінального є примус представників влади, посадових осіб до певної дії актом насильства або загрозою його здійснення, що має на меті, як правило, широкий соціальний резонанс, дестабілізацію ситуації або падіння існуючого режиму, під-

рив впливу органів державного управління та самоврядування на суспільство, дезорганізацію їхньої діяльності. Це – одна із форм ведення політичної боротьби, яка включає в себе дві складові: змістовну (ідеологія та культура) і технічну (інформаційна інфраструктура).

Характерною рисою сучасного інформаційного тероризму є, насамперед, публічність, забезпечення якої покладається на традиційні мас-медіа (пресу, радіо, телебачення) і Internet-медіа. Інформаційний тероризм нині не тільки відповідає ері інформаційних технологій, а й прагне підкорити її собі. Терористичні організації провадять широку інвестиційну політику. Крім традиційного підпорядкування активів легальних компаній і поліпшення інфраструктури наявного нелегального бізнесу сфери інформаційних технологій, терористичні організації активно втручаються в інформаційний простір. Створюють медіа-імперії з власних інформаційних ресурсів (друковані видання, радіостанції, телеканали, Internet-медіа), знаходять агентів впливу в авторитетних світових інформаційних носіях, провадять ефективні інформаційні операції, розробляють і застосовують методи маніпулювання масовою свідомістю.

Розглядаючи **теракт як вияв політичної активності й метод регуляції соціальних процесів**, теоретики інформаційного тероризму у своїй методології досягнення мети основне місце відводять засобам масової комунікації. Оперативність, масштабність, унікальна здатність впливати на суспільну свідомість властиві мас-медіа. Інформаційний потенціал терористичного акту величезний, і це прекрасно розуміють і суб'єкти терористичної діяльності, і ті, хто стоять за ними. Терористи апелюють до суспільства за допомогою мас-медіа, при цьому терористичний акт засобів масової комунікації творить свій власний віртуальний простір, визначальною характеристикою якого стає тривале існування, активне поширення й значне тиражування насильства. Ретрансляція насильства ЗМІ підсилює ефект самого насильства, тим самим викликаючи деструкцію суспільної свідомості.

Страх і невпевненість у завтрашньому дні людей і, як наслідок, психологічний ступор суспільної свідомості, найдієвіший із погляду дезорганізації, який проявляється слабістю й бездіяльністю влади або підвищеною тривожністю, і посиленням напруженості в суспільстві, негативними емоціями, які повинні знайти вихід, і врешті бути спрямованими проти влади, — до цього **прагнуть ідеологи тероризму**. Терористичний акт створює інформаційний привід і жорстко змінює порядок денний, а ЗМІ постають як засіб інформаційно-пропагандистського забезпечення терористичної діяльності. Таким чином не тільки задається інформаційний привід як ініціалі-

затор певних смислотворчих процесів в індивідуальній і масовій свідомості, а й реалізується можливість управління суспільною свідомістю, як формування суб'єктів дії – великих соціальних груп, сконсолідованих навколо лідерів думок і готових до масових виступів, зокрема і до антисоціальних дій. При цьому люди можуть висувати різні вимоги, а їх дії, найчастіше, далекі від логіки подій і способів вирішення існуючих, а тим більше уявних проблем, породжують беззаконня в діях учасників.

Аналіз соціально-політичних, політико-правових процесів свідчить, що в Україні присутні основні терогенні фактори, що створюють політичні, економічні, соціальні й етнорелігійні передумови для виникнення й розвитку інформаційного тероризму.

Інформаційним терористичним актам в залежності від часу і місця їх проведення властиві **цілий ряд характерних особливостей, які відрізняють їх від інших терористичних актів. Це, в першу чергу, мета, риси, суб'єкти, об'єкти, загрози, що визначають відповідні сили, засоби, методи його реалізації.** Ми виділяємо серед найбільш поширених із них такі.

Риси: відсутність географічних кордонів, труднощі у визначенні національної належності джерела та можливість анонімного доступу до інформаційних ресурсів; висока латентність і конспірація замовників, джерел фінансування та виконавців; швидка ескалація, що забезпечує миттєве досягнення запланованої мети; представляють реальну загрозу владі, органам управління, викликають нестабільність у суспільстві; легко контролюються, що дає змогу оперативно вносити корективи ззовні; дешеві за вартістю, масштабні за охопленням і відчутні за наслідками; безпосередньо впливають на прийняття політичних та управлінських рішень; групують населення навколо певних ідей та лідерів або проти них.

Суб'єкти (джерела) – зовнішні та внутрішні за місцем знаходження; держави, юридичні та фізичні особи, які проводять агресивну інформаційну політику стосовно України; іноземні спецслужби та недержавні організації; закордонні та окремі вітчизняні ЗМІ; релігійні фанатики, організації сектантів та церковників; різного роду місіонерські організації; окремі екстремістські організації та групи.

Об'єкти (цілі) – суспільні відносини, на які посягають терористи; акти інформаційного тероризму, що вчиняються проти безпеки та життєдіяльності держави, суспільства, прав і свобод окремих громадян; правоохоронні органи; система державного управління та її органи (Адміністрація Президента України, Кабінет Міністрів, міністерства і відомства, органи місцевого самоврядування); лідери держави, партій, громадських рухів; інформаційні ресурси, бази да-

них, статзвітність; молодь, студенти, соціально незахищені прошарки населення, безробітні, чорнобильці, афганці, дрібні підприємці.

Засоби: поширення повідомлень через видання засобів масової інформації (ЗМІ, Інтернет, телебачення), що викликають паніку серед населення; не зафіксовані на матеріальних носіях погрози; хибні повідомлення про очікуваний дефолт країни, вибухи, які готуються, вбивства, отруєння тощо.

Література:

1. Петров К. Е. Структура концепта «терроризм» // Полис. — 2003. — № 4.

2. Кримінальний кодекс України від 5 квітня 2001 р. - №2341-III // Відомості Верховної Ради. – 2001. - №№23-26.

3. Указ Президента України «Про виклики та загрози національній безпеці України у 2011 році».

4. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації. \\Навчальний посібник. Харків. «ФОЛІО».-2002., 284 с.

5. Див.: Національна безпека України 1994-1996рр.: Наукова доповідь інституту стратегічних досліджень. – К., 1997.

УДК 341.824:338.47 (043.2)

Тиква В.Л.

Національна академія Служби безпеки України

ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ВПЛИВУ НА СУСПІЛЬНУ СВІДОМІСТЬ

На даний час Інтернет все активніше і масштабніше використовується в інтересах здійснення прихованого інформаційного впливу. Він дає широкі можливості щодо формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси супротивника і поширення спеціально підготовленої інформації. У тому числі і дезінформації.

Таке активне використання мережі Інтернет для ведення інформаційного впливу обумовлено наявністю суттєвих переваг перед звичайними ЗМІ та іншими технологіями. Серед таких переваг слід відзначити наступні: 1. Оперативність, яка обумовлена тим, що розміщення та регулярне оновлення інформації не вимагають значного часу на підготовку матеріалів в електронному вигляді. При цьому користувачі отримують її в режимі реального часу на відміну, наприклад, від читачів друкованих ЗМІ та, навіть, телебачення. 2. Економічність, яка виникає у зв’язку з тим, що для підготовки інформаційних матеріалів,

їх розміщення та оновлення не потрібна значна кількість працівників та навіть офісного приміщення, комп'ютерної техніки, інщих матеріальних ресурсів. Співробітники можуть працювати віддалено у себе вдома або інших місцях, навіть не знаючи один одного, отримуючи винагороду за результатами виконаного завдання. 3. Прихованість джерела розміщення інформації, яка обумовлена тим, що вкидання значного обсягу інформації, або проведення хакерської атаки легко замаскувати, наприклад, під дії звичайних комп'ютерних хуліганів. Підготувати та провести кібератаку з використанням Інтернету може досить широке коло осіб – від військових і розвідувальних структур іноземних держав до партизанських формувань, окремих злочинців, промислових конкурентів, хакерів або просто невдоволених людей. Відстежити ж джерело надходження інформації або інших дій досить складно. 4. Масштабність можливих наслідків, яка пов'язана безпосередньо з вчиненими діями і які в свою чергу можуть мати значний вплив на формування громадської думки, на позиції офіційних осіб від яких залежить прийняття важливих рішень. Використання глобальної мережі для деструктивних впливів може призвести до порушення штатної роботи або тривалого виведення з ладу життєво важливих об'єктів і систем в окремих районах, країнах або регіонах. 5. Комплексність подачі інформації та її сприйняття пов'язана з можливістю подання будь-якої інформації у будь-якому вигляді розрахованої на різні аудиторії. На Інтернет-сторінках розміщується як текстова, так і графічна інформація в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Використання ж сучасних мультимедійних технологій, що дозволяють демонструвати документальні свідчення, фото- та відеоматеріали при спеціально підібраному супроводі (коментарі, музика) є додатковим емоційним впливом на користувачів мережі. 6. Доступність отримання інформації, яка обумовлена можливістю отримувати інформацію користувачами Інтернету, наявної на серверах різних країн, минаючі прикордонні, цензурні та інші бар'єри. При цьому будь-який користувач може розмістити власну інформацію (нерідко безкоштовно) на серверах, зареєстрованих в інших країнах.

На сьогодні ЗМІ все більше переходять в Інтернет, створюючи власні сайти та розміщуючи там інформацію. Окремі ЗМІ вже перестали виходити у друкованому вигляді, а лише в електронному. Також все більше поширюється сервіс соціальних мереж. Розвиток можливостей Інтернету та дедалі зростаюча роль його аудиторії дозволяє говорити про формування нового цифрового публічного простору який надає суспільству можливість контролювати владу, без-

посередньо висловлювати свою думку з найважливіших для нього питань за допомогою нових цифрових каналів комунікації, що також дозволяє в значній мірі впливати на соціальні та політичні процеси в державі. Так основними майданчиками для об'єднання протестуючих стають не юридично зареєстровані політичні, громадські та інші організації, а їх сайти в Інтернеті або соціальні мережі. Яскравим прикладом цього були події в країнах Північної Африки, Близького та Середнього сходу, що призвело до масових заворущень, відставкам урядів та зміни політичних режимів.

Інтернет дозволяє отримувати і зворотній зв'язок від користувачів інформації. Все це і обумовило той факт, що Інтернет виходить на передові позиції і його все більше обирають, якщо необхідно здійснити масовий інформаційний вплив. Водночас разом з перевагами використання Інтернету для інформаційно-психологічного впливу слід враховувати і його недоліки. Саме тут Україна має їх чимало, багато з яких відсутні в інших країнах. Це, зокрема, значно менший доступ до Інтернету та його використання у повсякденному житті. Є території, які не мають покриття мережею. Не всі соціальні та вікові групи населення мають можливість нт навички у користуванні Інтернетом. Все в підсумку і призводить до того, що в Україні ще значний вплив мають телебачення, інші ЗМІ. Однак з часом багато з цих недоліків будуть невільовані і Інтернет стане чи не єдиним найпотужнішим засобом отримання інформації.

Аналіз останніх конфліктів засвідчив зростання використання Інтернету в процесі ведення інформаційних війн. Відбувся перехід від традиційних засобів впливу листівки, радіо, телебачення до соціальних медіа та інструментів Інтернет простору з метою інформаційного впливу на учасників конфлікту та світової думки. Таким чином Інтернет-простір перетворився в новий майданчик для здійснення інформаційно-психологічного впливу, що має ряд суттєвих переваг над класичними методами впливу. Засоби інформаційно-психологічного впливу Інтернет простору дозволяють впливати на думку починаючи від особистості окремо до всесвітньої аудиторії.

Такий вплив мав місце мід час військових дій у Чечні, в колишній Югославії, в Іраку, Сирії. Тунісі, в інших країнах світу. Так, під час військових дій в Югославії в Інтернет-просторі для підтримки військової операції НАТО було розміщено близько 300 сайтів, які були присвячені косовській проблемі та військовій операції Альянсу. В Іраку було значне використання Інтернет ресурсів багатьох країн світу для інформаційно-психологічного впливу на світову громадську дкмку, населення та армію Іраку. Здійснювалось блокування інформаційних каналів, які по іншому висвітлювали ситуацію

в зоні конфлікту. Аналогічну ситуацію ми спостерігаємо в теперішній час і в Україні. Російська Федерація використовує всі наявні засоби - телебачення, друковані ЗМІ, а також Інтернет для подачі перекрученої, а й інколи неправдивої інформації про події, що відбуваються в Україні.

УДК 351.746.1

Тіщенко В.М.
Державна прикордонна служба України

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФІЛЬТРАЦІЙНО-ПЕРЕВІРОЧНОЇ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Агресія Російської Федерації, що призвела до окупації Криму і розгортання на сході України військових дій та ускладнення міграційної ситуації, коли нашу країну мігранти розглядають не тільки як країну-транзит, а й країну-кінцеву точку призначення, зумовлює потребу в нових способах боротьби із терористичною загрозою та міграційною кризою. Проведення фільтраційної роботи є ефективним засобом боротьби із зазначеними негативними прояви.

Метою проведення фільтраційних заходів є виявлення осіб з числа бойовиків незаконних збройних формувань так званих «ДНР» та «ЛНР», їх зв’язків та контактів, пособників терористів, незаконних мігрантів, осіб, що становлять оперативний інтерес для спецслужб.

Ефективність фільтраційної роботи в сучасних умовах інформаційних технологій багато в чому визначається рівнем її інформаційного забезпечення (якістю дій з добування, обробки та передачі значимої інформації в компетентні інстанції та відповідальним особам, які здійснюють обліково-реєстраційну, оперативно-розшукову, та інші види діяльності, тощо).

Процес інформаційного забезпечення можна розглядати не тільки як сукупність методів і засобів збору і обробки інформації, але і як організацію доступу до інтегрованих інформаційних банків і баз даних.

Використовуючи інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» для організації та проведення фільтраційних перевірок співробітники Державної прикордонної служби України (далі – ДПСУ) отримують достовірну та актуальну інформацію про осіб, які перетнули державний кордон Україні, осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або тимчасово обмежено право виїзду з України, осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних по-

карань, недійсних, викрадених і втрачених документів на право виїзду за кордон та інших баз даних, що створюються та використовуються відповідно до законодавства [1].

Методи отримання інформації різноманітні, вони можуть бути як гласними, так і негласними. Співробітники оперативних підрозділів ДПСУ отримують зазначену інформацію шляхом проведення оперативно-розшукових заходів, а також від осіб, які з ними співпрацюють.

Необхідно зазначити, що оперативними підрозділами ДПСУ практикується також використання оперативно-розшукової інформації шляхом цілеспрямованих інформаційно-психологічних впливів на свідомість особи (опитування, бесіда). При цьому використання зазначеного повинно відповідати принципам законності, об'єктивності та своєчасності.

Інформаційні масиви загального користування можуть використовуватися в довідковому режимі в формі «електронного досьє». До таких масивів відносяться: всі засоби масової інформації, офіційні звіти, повідомлення, відкриті статистичні дані, протоколи та дані з соціальних мереж, які не мають обмежень на розповсюдження та використання. Проте, незважаючи на значний обсяг відкритої інформації в мережах, її збирання, може класифікуватися як посягання на недоторканність приватного життя. Враховуючи викладене, оперативні працівники в праві накопичувати безособову відкриту інформацію, а відомості щодо окремих осіб мають право збирати лише в межах заведеної оперативно-розшукової справи або відкритого кримінального провадження [2, с.95].

У провідних країнах світу модель побудови інформаційного забезпечення зорієнтовано на отримання випереджувальних даних. Так Агентство розвідки Республіки Польща отримує дані з країн з високим рівнем терористичного ризику, з держав в яких відбуваються військові конфлікти, формує списки осіб, які не повинні перетинати межі Республіки Польща.

У процесі створення, перетворення і маніпуляція з інформацією, виникають наступні проблеми: забезпечення інформаційних прав і свобод громадян, держави і суспільства в галузі захисту від впливу неякісної інформації безпеки в інформаційній сфері, що забезпечує виявлення загроз і захист інформації від незаконного втручання; створення і застосування засобів і механізмів забезпечення інформаційної безпеки [3, с. 233].

З метою вдосконалення інформаційного забезпечення проведення фільтраційної роботи, доцільно посилити співробітництво з іншими правоохоронними органами на національному та міжнарод-

ному рівнях, забезпечити обмін інформацією, створити бази фільтраційно-перевірочних матеріалів для проведення аналізу та вдосконалення методики проведення перевірочної роботи, долучитися до використання бази даних EURODAC.

Література:

1. Про затвердження Положення про інформаційно-телекомунікаційну систему прикордонного контролю «Гарт-1» Державної прикордонної служби України [Електронний ресурс] : наказ Адміністрації Державної прикордонної служби України від 30.09.2008р. № 810 // Законодавство України : веб-сайт Верхов. Ради України. URL: http://zakon0.rada.gov.ua/laws/show/z1086-08, (дата звернення 02.05.2017).

2. Перепелиця М.М. Накопичення й аналіз оперативно-розшукової інформації з комп'ютерних мереж [Текст] / М. М. Перепелиця, В.В. Плукар // Науковий вісник Ужгородського національного університету : серія: Право. – Ужгород : Видавничий дім «Гельветика». – 2015. – Вип. 31. Т. 3. – С. 93-97.

3. Ильяшенко А. Н. Особенности использования оперативно-розыскной информации в криминалистической регистрации органов внутренних дел/ А. Н. Ильяшенко // Общество и право. – 2011. – №2 (34). – С.231-238.

УДК 378(477)(094)

Ткаченко В.В.
доктор історичних наук, професор
ДНУ «Інститут модернізації змісту освіти»

СТАНДАРТИ ВИЩОЇ ОСВІТИ У СФЕРІ КІБЕРБЕЗПЕКИ – ВАЖЛИВИЙ ІНСТРУМЕНТ МОДЕРНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ЗАПОРУКА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Наприкінці 1996 р. експерт Пентагону Роберт Банкер на одному із симпозіумів представив доповідь, присвячену новій військовій доктрині збройних сил США XXI ст. (концепція «Force XXI»). В її основу покладено поділ усього театру воєнних дій на дві складових − традиційний простір і кіберпростір, причому останній має навіть більш важливе значення. Р. Банкер запропонував доктрину «кібер-маневру», яка повинна з'явитися природним доповненням до традиційних військових концепцій, які переслідують цілі нейтралізації або придушення збройних сил противника. Фактично з середини 1990-х серед широкого загалу та у ЗМІ почали активно використо-

вуватися такі поняття як «кіберпростір», «кіберзлочин», «кібератака», «кіберзброя» тощо. На жаль для нашої держави та її безпеки ці поняття набувають конкретних проявів. Міжнародні нормативно-правові акти досить широко визначають поняття «кіберзлочин» та протизаконні дії пов'язані з ним [1]. Виходячи з приблизних підрахунків у світі близько 750 тисяч потенційних порушників-кіберзлочинців. Розмір збитків, що наносяться кіберзлочинами, становить більше 200 млрд. доларів [2]. Разом із цим більш небезпечним для національної безпеки є цілеспрямована кіберагресія однієї держави проти іншої. Нині ми не маємо достатньо доказів того, хто саме із стабільною регулярністю здійснює кібератаки на об'єкти української інфраструктури, але ми вже сьогодні маємо давати гідну на це відповідь. Складової останньої має бути достатня кількість висококваліфікованих фахівців у сфері кібербезпеки.

У порівняно короткий термін після введення в дію Закону України «Про вищу освіту» (01 вересня 2014 року) Урядом та Міністерством освіти і науки України були розроблені нормативні документи щодо концепції стандартів вищої освіти (далі СВО) та порядку їх створення [3].

Затверджено новий перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти. Замість колишніх 48 галузей знань, 144 напрямів та понад 500 спеціальностей введено 29 галузей знань і 122 спеціальності [4]. При цьому вищі навчальні заклади отримали право самостійно вводити спеціалізації, що дає можливість гнучко реагувати на потреби ринку праці.

Так, станом на кінець квітня цього року розроблені проекти стандартів освітнього ступеня «бакалавр» з 115 (із 122) спеціальностей з 28 (із 29) галузей знань. До кінця 2017 року планується повністю завершити розроблення та введення в дію СВО, після чого вищі навчальні заклади, реалізуючи право академічної автономії, отримають можливість розробляти освітні програми, які визначатимуть вимоги до рівня освіти осіб, що розпочинають навчання за цією програмою, перелік навчальних дисциплін і логічну послідовність їх вивчення.

У контексті обговорюваного питання слід відзначити успішне завершення розробки СВО зі спеціальності 125 Кібербезпека. Комісією у складі 9-ти провідних фахівців України у сфері інформаційної безпеки (голова − Олександр Юдін) у тісній співпраці з університетами, які здійснюють підготовку ІТ-фахівців, компаніями-роботодавцями, Держспецзв'язку, СБУ, МОН, ІМЗО створено проект стандарту, що пройшов усі етапи рецензування і експертизи та першим направлений міністерством на погодження до Національного агентства із забезпечення якості вищої освіти. Визначені в СВО

інтегральна, загальні і фахові компетентності, відповідний їм нормативний зміст освіти та прогнозовані результати навчання забезпечать оволодіння випускниками такими об'єктами професійної діяльності, як засоби інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.

Проблеми впровадження СВО та розроблення профільно-орієнтованої освітньої програми першого (бакалаврського) рівня зі спеціальності «Кібербезпека» обговорювались на нараді в МОН 20 березня поточного року за участю представників ВНЗ, ІТ-спільноти, Держспецзв'язку. За підсумками наради прийнято рішення про створення робочої групи, яка займатиметься розробкою типової освітньої програми для підготовки бакалаврів зі спеціальності «Кібербезпека» та координуватиме співпрацю всіх зацікавлених сторін. Спеціальність «Кібербезпека» є достатньо популярною серед абітурієнтів з високим рейтингом сертифікату УЦОЯО. У 2017 р. більше трьох десятків провідних вищих навчальних закладів України пропонує навчання за спеціальністю «Кібербезпека».

Отже, з боку МОН України та підпорядкованих йому структур проводиться масштабна і необхідна робота щодо творення нормативної, науково-методичної бази у сфері стандартизації вищої освіти за спеціальністю «Кібербезпека», що у свою чергу впливає на зміцнення національної безпеки та обороноздатності України.

Література

1. Конвенція про кіберзлочинність. [Електронний ресурс]. − Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575

2. Дані подано за матеріалами сайту: http://justicon.ua/ua/press-tsentr/expert/prezident-ukainy-vozlozhil-na-mvd-polnomochiya-po-borbe-s-kiberprestupnostyu.html#ixzz4g30z8Pnl

3. Закон України «Про вищу освіту», 1 липня 2014 р. №1556-VII. URL: http://zakon2.rada.gov.ua/laws/show/1556-18

4. Постанова КМУ від 29.04.2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти». [Електронний ресурс]. − Режим доступу: http://tntu.edu.ua/nv/files/266.pdf

УДК 659.4:327.88

Ткачук Л.М.
кандидат економічних наук, доцент
Вінницький національний технічний університет
Волчаста К.В.
Вінницький національний технічний університет

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

В нестабільних умовах проникливості кордонів і формування нової політичної географії виникли територіальні суперечності між державами та регіонами. У суперечках між державами широко використовуються засоби і можливості інформаційної війни. Для України ця проблема є особливо актуальною в умовах неоголошеної російсько-української війни на Сході й окупації Криму та частини Донецької та Луганської областей, коли прийоми інформаційної війни широко використовуються Росією для дестабілізації ситуації в Україні. Тому наразі першочерговим завданням стало забезпечення інформаційної безпеки держави.

У ст.17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [1]. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України [2], захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій, і програм в інформаційній сфері відповідно до чинного законодавства [3].

У Законі України «Про основи національної безпеки України» визначено основні напрямки державної політики з питань національної безпеки в інформаційній сфері [4]. До них належать: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем,

іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

25 лютого 2017 року Президент Петро Порошенко підписав Указ, яким увів в дію рішення Ради національної безпеки і оборони «Про Доктрину інформаційної безпеки України» [5]. Як зазначається у документі, необхідність прийняття Доктрини інформаційної безпеки України зумовлена виникненням актуальних загроз національній безпеці в інформаційній сфері, а також потребою визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації і вільного обігу інформації. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Незважаючи на низку заходів, впроваджених за період російсько-української війни в інформаційній сфері, в інформаційній безпеці України є прогалини, що загрожують національним інтересам. Подолати їх можна шляхом:

− розробки і впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, зокрема з вимогами Конвенції про кіберзлочинність;

− приведення законодавства з питань охорони державної таємниці до європейських стандартів;

− розробки та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці.

Отже, у сучасних умовах інформаційній безпеці слід приділяти особливу увагу як важливій частині боротьби у гібридній війні.

Література

1.Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. –1996. – № 30. – Ст. 141.

2.Боднар І. Р. Сучасні реалії інформаційного суспільства: про-

блеми становлення та перспективи розвитку: монографія [Текст] / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

3.Малик Я. Інформаційна безпека України: стан та перспективи розвитку / Я. Малик // Збірник наукових праць «Ефективність державного управління». – 2015. – № 44. – С. 13-20.

4.Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – 39. – Ст. 351.

5.Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року // Офіційний вісник України. – 2017. - №20. – Ст. 554.

УДК 343.3

Ткачук Н.А.
Служба безпеки України

ЗАГРОЗИ НАЦІОНАЛЬНІЙ СИСТЕМІ КІБЕРБЕЗПЕКИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Сьогодні в Україні здійснюється активна розбудова національної системи кібербезпеки (далі - НСК). Стратегією кібербезпеки України визначені основні засади та напрями кібербезпеки держави, сформульовані завдання основних державних суб’єктів її забезпечення; актами Кабінету Міністрів України, що затверджують плани реалізації Стратегії кібербезпеки на 2016 та 2017 роки, окреслені конкретні комплексні заходи, фактично спрямовані на розбудову ефективної кібербезпекової системи, а також визначені відповідальні за їх реалізацію державні суб’єкти; триває робота із удосконалення нормативно-правового підґрунтя НСК. Національний координаційний центр кібербезпеки, що функціонує при РНБО України, виконує важливу функцію із координації зазначених процесів.

Безперечно, національна система кібербезпеки держави є вагомою складовою національної безпеки. Тож її створення потребує комплексного та виваженого підходу, що передбачає скоординовані дії всіх суб’єктів сектору безпеки і оборони держави, налагодження взаємодії з приватним сектором та розбудову ґрунтовної законодавчої основи. Така система має забезпечувати безпечне функціонування кіберпростору, його використання в інтересах особи, суспільства і держави та своєчасну протидію кіберзагрозам сучасного безпекового середовища, основними з яких є кібервійна, кібертеро-

ризм, кіберзлочинність та кібершпигунство.

Водночас, з огляду на те, що кіберпростір перетворився на поле міждержавного протистояння, перевага в якому, наразі, є запорукою забезпечення власних політичних, економічних та інших стратегічних інтересів, національна система кібербезпеки держави сама по собі є потенційним об'єктом розвідувально-підривної діяльності спецслужб іноземних держав з метою послабити або взагалі знищити механізм протидії кіберзагрозам на національному рівні.

Протиправні спрямування до НСК можуть бути також реалізовані з боку терористичних організацій та міжнародних хакерських угруповань, які переслідуватимуть мету створення підґрунтя для подальшої організації та безкарного здійснення своєї злочинної діяльності, в т.ч. з території України, а також кіберпідрозділами збройних сил іноземних держав як підготовчий захід до військових кіберзаходів з метою унеможливити здійснення належної кібероборони держави.

Зазначеному сприяють особливості та комплексний характер кіберзагроз сучасного безпекового середовища. Адже сьогодні, в рамках складних кібероперацій можуть одночасно реалізовуватися декілька кіберзагроз національній безпеці держави, взаємопов'язаних між собою, а також до їх реалізації можуть бути залучені кардинально різні суб'єкти.

Зокрема, у ході міждержавного протистояння у кіберпросторі спецпідрозділами збройних сил та/або спецслужбами країни можуть бути залучені:

національні ІТ-корпорації – для здійснення акцій промислового кібершпигунства з метою підриву економічної безпеки іншої держави *(як це, наразі, відбувається з боку КНР щодо американських компаній)*, постачання програмного забезпечення із шпигунськими функціями до державних органів іноземної держави для отримання віддаленого доступу до інформації стратегічного характеру *(н-д, впровадження в органи влади України антивірусного програмного забезпечення підконтрольних ФСБ компаній «Доктор Веб» та «Лабораторія Касперського»)*, збору персональних даних стосовно об'єктів зацікавленості *(н-д, використання російськими спецслужбами соціальних мереж «ВКонтакте» та «Одноклассники» для збору розвідданих)*;

злочинні хакерські угруповання – для розробки та впровадження комплексного шкідливого програмного забезпечення в ІТС противника, а також безпосереднього здійснення кібератак *(н-д, залучення російськими спецслужбами хакерського угруповання Fancy Bear для проведення складних кібератак на інформаційну інфраструктури інших держав)*;

терористичні організації, спонсоровані урядами держав, які не

тільки можуть бути причетними до здійснення кібернетичного впливу, а й здатні взяти відповідальність за гучну кібератаку, організовану спецслужбами, на себе *(це ілюструю кібератаки, здійснені з території РФ, на урядові веб-сайти України із розміщенням інформації, що пропагує терористичну діяльність «ДНР»)*.

Особливості сучасних викликів кіберпростору зумовили поступове зростання у національних кібербезпекових системах провідних країн світу ролі спецслужб та контррозвідувальних органів, які за допомогою спеціального інструментарію оперативно-розшукової, розвідувальної та контррозвідувальної діяльності, наявних сил та засобів можуть найбільш ефективно протидіяти актуальним кіберзагрозам. Також, набула особливої актуальності міжвідомча взаємодія суб'єктів забезпечення кібербезпеки держави.

Отже, національна система кібербезпеки України, як можливий об'єкт спрямувань спецслужб іноземних держав, військових структур, терористичних організацій та злочинних хакерських угруповань, потребує окремого механізму захисту, здатного гарантувати її стале функціонування та розвиток в інтересах забезпечення кібербезпеки держави.

Вважаємо, що такий механізм, у першу чергу, потребує спеціального інструментарію, сил та засобів вітчизняних органів безпеки, які повинні стати не лише ключовим елементом НСК, а й виконувати координаційну функцію на національному рівні щодо протидії спеціальним кібероперацiям проти нашої держави.

УДК:340+35.078.3

Ткачук Т.Ю.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

КІБЕРБЕЗПЕКА: ПІДХОДИ ДО ВИЗНАЧЕННЯ В ОКРЕМИХ КРАЇНАХ

Останні два роки довели, що у сучасномувисокотехнологічному світі не існує жодноїгалузі, компанії або навіть уряду, які б незазнали впливу змін. Так, діловий світ зазнає негативноговпливу кібератак на системи безпеки, і цевже має серйозні наслідки для міжнародноїбезпеки та дипломатії.

Атака хакерів на Всесвітнє антидопінгове агентство (WADA) – далеко не перший кіберзлочин, в якому багато хто бачить російський слід[1]. Влітку 2016 р. масштабної атаки зазнав сайт Національного комітету Демократичної партії США. Хакери розмістили на порталі

Wikileaks майже 20 тис. електронних листів, пов'язаних з кандидатом у президенти від демократів Гілларі Клінтон. З них випливає, що керівництво партії надавало перевагу Клінтон, при цьому щосили намагаючись завадити виборчій кампанії її внутрішньопартійного конкурента у передвиборчій боротьбі Берні Сандерса[2].Подібних прикладів безліч. Відповідно міжнародне законодавство останнім часом почало приділяти значну увагу кіберзагрозам та протидії їм.

Серед основних загроз національним кіберпросторам стратегії більшості країнвизначають:

– *кібершпигунство та військові дії, які здійснюються за підтримки або з відома держави*. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією[3]. Так, однією з найрезонансніших кібератак за останній час стали дії КНДР проти компанії "SonyPicturesEntertainment", внаслідок яких зловмисники заволоділи конфіденційними даними, в тому числі інформацією про комерційні операції компанії [4].

– *Використання Інтернету у терористичних цілях*. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників.

– *Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом*. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе ПЗ.

– Відповідно, національні законодавства країн, як правило, регулюють питання:

– Захисту персональних даних (Канада, Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);

– Захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (США, Канада, Польща, Естонія, Італія);

– Захисту дітей (США);

– Захисту важливих об'єктів інфраструктури та інформаційних систем (Франція).

По-різному й трактують поняття «кібербезпека» в зарубжних країнах:

– сукупність організаційних, правових,технічних та освітніх заходів,спрямованих на забезпеченнябезперервного функціонуваннякіберпростору (*Політика захисту кіберпростору Республіки Польща*).

– бажаний стан безпеки інформаційнихтехнологій, за якого ризики длякіберпростору скорочені до прийнятногомінімуму (*Стра-*

тегія кібербезпекиНіменччини).

– заходи з попередження шкоди від збоївв роботі ІКТ та в її усуненні (*Національнастратегія кібербезпеки КоролівстваНідерланди*).

– бажаний стан інформаційної системи, заякого вона може протидіяти викликамкіберпростору, які можуть негативновплинути на достовірність, цілісність таконфіденційність даних, що зберігаютьсяабо обробляються даною системою(*Стратегія безпеки та обороніинформаційних систем Франції*).

Ми живемо в еру революційнихперетворень у сфері цифровихтехнологій – перетворень, якітрансформують відносини міжспоживачами та виробниками,стирають кордони між галузямиекономіки і, зрештою, спонукаютьдалекоглядних топ менеджерів адаптувати методизабезпечення інформаційної безпеки до сучасних реалій.

Література

1. Топ-5 найгучніших кібератак, в яких звинувачують російських хакерів. URL: http://ua.112.ua/mnenie/top-5-naihuchnishykh-kiberatak-v-iakykh-zvynuvachuiut-rosiiskykh-khakeriv-338871.html
2. Російські хакери злили нову порцію вкрадених у WADA документів // УКРІНФОРМ. URL: https://www.ukrinform.ua/rubric-abroad/2085046-rosijski-hakeri-zlili-novu-porciu-vkradenih-u-wada-dokumentiv.html
3. Canada’s Cyber Security Strategy: For a Strongerand More Prosperous Canada. URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
4. TheDepartmentOfDefenseCyberStrategy . URL: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
5. 18-е Щорічне опитування керівників найбільших компаній світу. URL: www.pwc.com/ceosurvey

УДК 316.6-027

Тронц В.М.

Національна академія Служби безпеки України

Колонюк В.В.

Національна академія Служби безпеки України

ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАСІБ ВЕДЕННЯ КОНФЛІКТУ

Очевидно, що інформаційна війна - складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує безпечне ставлення до них.

Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням можуть перевищувати наслідки збройних конфліктів.

Інформаційний обмін регулюється відповідно до основних принципів міжнародного права: суверенної рівності; невтручання у внутрішні справи держав, заборони застосування сили або загрози силою; дотримання міжнародних зобов'язань, мирного врегулювання міжнародних спорів; непорушності кордонів; загальної поваги до прав людини; співробітництва; виконання міжнародних зобов'язань. Дана сфера регламентується також низкою спеціальних галузевих принципів. Тому порушення з боку суб'єкта-агресора основоположних принципів тягне за собою застосування відповідних заходів.

Офіційного визначення, закріпленого у міжнародно-правових конвенціях, немає, однак науковці схиляються до декількох точок зору. У широкому значенні під інформаційною війною можна розуміти будь-який негативний інформаційний вплив на ворога. Суб'єктом такого впливу може бути будь-як приватне або публічне утворення. У вузькому значенні - це новий, що не укладається у міжнародно-правову кваліфікацію, вид або спосіб ведення збройних конфліктів.

Метою інформаційних війн загалом є маніпулювання масами. Якщо детальніше розглянути цю мету, то можна виділити кілька напрямів: внесення у суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів; дезорієнтація та дезінформація мас; послаблення певних переконань; залякування населення образом ворога; залякування противника своєю могутністю. Не обов'язково, щоб метою такої війни була сукупність всіх факторів, може бути достатньо лише одного окремого напрямку.

Таким чином, виділяється декілька рівнів впливу інформації в ході ведення ІВ, завдяки якому досягається мета, а саме вплив на населення, на системи управління та озброєння, а також комплексний вплив.

Однак інформаційний вплив може стосуватися не тільки заборонених міжнародним правом ідей і поглядів, але й породжувати негативні соціальні та економічні наслідки. Такий інформаційний вплив на населення іноземної держави за допомогою різних засобів впливу є порушенням принципу невтручання в справи держав. Особливе значення мають засоби такого впливу. Вони можуть знаходитися як на території держави, так і поза нею.

Інший аспект проблеми, коли такий вплив здійснюється не щодо населення іноземної держави, а на треті держави і міжнародне співтовариство в цілому з метою дискредитувати іноземні держави та політику, що ними проводиться. Пряма заборона на такі дії відсу-

тня в міжнародному праві, хоча вони в повній мірі можуть вважатися інформаційною війною.

Науковці та дослідники даної проблеми вводять поняття інформаційної війни першого та другого покоління. Так, для інформаційної боротьби першого покоління характерні: вогневе придушення (у воєнний час) елементів інфраструктури державного та військового управління; одержання розвідувальної інформації шляхом перехоплення й розшифровки інформаційних потоків; здійснення несанкціонованого доступу до інформаційних ресурсів з наступною їх фальсифікацією чи викраденням; масове подання в інформаційних каналах супротивника чи глобальних мережах дезінформації для впливу на особи, які приймають рішення. Інформаційна боротьба другого покоління передбачає: створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини противника; маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу; дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни; дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління; підрив міжнародного авторитету держави, його співробітництва з іншими країнами. Розвиток і ведення стратегічної інформаційної війни другого покоління, її скоординовані інформаційні операції у перспективі можуть привести до повної відмови від використання військової сили.

Отже, виходячи з вищевикладеного, можна виділити два види інформаційних війн: поза збройними конфліктами, так звані «холодні інформаційні війни» та в умовах збройних конфліктів, або напередодні збройного конфлікту. За ступенем інтенсивності інформаційна війна може включати: ідеологічний вплив; вплив на системи управління та озброєння**;** комплексний вплив. Збройні конфлікти із застосуванням інформаційної складової вже відбувалися. Норми міжнародного права до них застосовувалися і мають застосовуватися надалі.

Література

1. Джерела та принципи міжнародного права. [Електронний ресурс].- Режим доступу: http://helpiks.org.

2. Поняття інформаційної війни в міжнародному праві. [Електронний ресурс].- Режим доступу: http://nbuv.gov.ua.

УДК 342.95

Тугарова О.К.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

ДО ПРОБЛЕМИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ВИКРИВАЧІВ ІНФОРМАЦІЇ

Процес становлення інформаційного суспільства в Україні зумовив створення нових правових інститутів, які б відповідали сучасним європейським стереотипам у сфері доступу до інформації. Протягом останнього часу особливу увагу української спільноти прикуто до розкриття суспільно необхідної інформації, яка є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Закон України «Про доступ до публічної інформації», прийнятий у 2011 році, запровадив важливий принцип свободи інформації – захист особи, яка розкриває відомості, що становить суспільно необхідний інтерес. Такі особи в міжнародному праві отримали назву «викривачів («whistleblowing») інформації», а спеціальні механізми їх захисту вже не один рік успішно працюють у більшій кількості розвинених країн світу. Прикладами сильного, працюючого законодавства у цій сфері є, приміром, законодавство США, Південної Кореї, Словенії, Румунії, Естонії, Литви. Викривачам інформації у цих країнах гарантовано анонімність при повідомленні про правопорушення, створено надійні канали розкриття суспільно важливої інформації, забезпечено захист від репресій на робочому місці, закріплено право повідомляти таку інформацію у ЗМІ, парламентські комітети чи комісії та ін.

Чи актуальним і важливим є це питання для України? Вбачається, що так, адже за останні роки в нашій державі потенційних викривачів суспільно важливої інформації стало майже втричі більше. За даними соціологічних опитувань, проведених в Україні міжнародною організацією Transparency International, сьогодні в Україні вже 45% громадян декларують готовність відкрито говорити про випадки порушень прав і свобод людини з боку представників влади, шкідливі негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо. Щоправда, інформаторів, які дійсно звертаються до правоохоронних органів про відомі їм факти протиправних діянь, залишається дуже мало – лише 2%. [1]. Однією з причин такої ситуації є відсутність чіткого законодавчого врегулювання механізму звільнення викривачів інформації від юридичної відповіда-

льності за розкриття суспільно необхідної інформації, змістом якої є інформація з обмеженим доступом.

Нормативні приписи ст.29 Закону України «Про інформацію» та ст. 11 Закону України «Про доступ до публічної інформації» закріплюють положення щодо недопущення притягнення до юридичної відповідальності осіб, які всупереч своїм посадовим або службовим обов'язкам розголосили інформацію (у тому числі з обмеженим доступом) про правопорушення або відомості, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю [2, 3]. Отже законодавець окреслюючи межі правомірності дій викривачів інформації, зосередив увагу на трьох основних підставах: 1) добрі наміри; 2) обґрунтоване переконання у достовірності інформації; 3) докази правопорушення. Якщо перші дві підстави мають загальнотеоретичне розуміння, поняття «доказ» є суто процесуальною категорією і потребують чіткого уявлення щодо його змісту і форми.

Інструкція для викривачів інформації, підготовлена в рамках проекту «Боротьба з корупцією: залучення журналістів та викривачів до платформи Хабардокс», підготовлену за підтримки Фонду сприяння демократії Посольства США в Україні [4], рекомендує будь-які докази зберігати та передавати в електронному вигляді. Наголошується у зазначеному документі і на тому, що в електронному вигляді простіше перевірити достовірність наданих доказів, аніж у випадку з паперовими копіями. Тому навіть якщо інформатор має документи або фотографії у паперовому вигляді чи аудіо- або відеозаписи в аналоговому форматі на фізичному носії (наприклад, на касеті чи компакт-диску), варто перевести їх в електронний вигляд – відсканувати або оцифрувати – і передавати вже в такому форматі. Також викривачам інформації рекомендовано обирати для роботи безпечний браузер – Tor Tor (The Onion Router) – це інтернет-браузер, який забезпечує анонімність і захист користувачів від стороннього моніторингу.

Звичайно, запропоновані зарубіжними колегами заходи забезпечення безпеки викривачів інформації, є цікавими і потребують подальшого вивчення. Проте, слід враховувати, що вітчизняна наука кримінального процесу базується на іншому розумінні поняття доказу, особливо в частині його правових ознак – належності і допустимості. Допустимість доказу, насамперед, передбачає законність отримання і можливість його перевірки у судовому процесі. Аноні-

мність викривача інформації, а також негласний спосіб отримання та передачі інформації може поставити під сумнів допустимість доказу, а межа між суспільно корисними і протиправними діями інформатора перестане існувати.

Вбачається, що означена проблема потребує подальшої наукової розробки, а її вирішення сприятиме подальшому вдосконаленню механізму захисту викривачів інформації у цивілізованій і європейській Україні.

Література

1. Викривачі або whistleblowers: чому вони потребують захисту. URL: http://ti-ukraine.org/news/vykryvachi-abo-whistleblowers-chomu-vony-potrebuyut-zahystu/

2. Про інформацію: Закон України від 02.10.1992 № 2657 –XII. URL: http://zakon.rada.gov.ua

3. Про доступ до публічної інформації: Закон України від 13.11.2011 № 2939 –VI. URL: http://zakon.rada.gov.ua

4. Інструкція для викривачів: як себе убезпечити. URL: http://uipp.org.ua/uploads/news_message/at_file_uk/0073/55.pdf

УДК 004.621

Хорошко В.О.
доктор технічних наук, професор
Національний авіаційний університет
Блавацька Н.М.
кандидат технічних наук, доцент
Національна академія Служби безпеки України
Хохлачова Ю.Є.
кандидат технічних наук, доцент
Національний авіаційний університет
Тимченко М.П.
Національний авіаційний університет

КЛАСИФІКАЦІЯ ВХІДНОЇ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ЗАХИСТУ

Однією з цілей автоматизованої обробки вхідних оперативних повідомлень в системах захисту є підвищення достовірності результуючої інформації при сполученні часу обробки.

Оперативні повідомлення класифікуються в залежності від їх функціонального призначення, необхідного ступеня оперативності, частоти надходження, особливостей обробки що міститься в цій інформації. За функціональною ознакою повідомлення можна розді-

лити на звітні, подієві, запити, відповідні.

Звітні повідомлення містять зазвичай узагальнену інформацію про параметри стану, охорону звіту або дохід процесу захисту інформації. Звітні повідомлення надходять один раз на добу з інформацією про виконання захисних заходів, про результати протидії атакуючим діям зловмисників, про розподіл функцій між підсистемами, про виконання графіку проведення рекламних робіт.

Подієві повідомлення складаються та передаються безпосередньо після завершення подій і містять інформацію типу «до відома» або інформацію, за якою потрібна відповідна реакція системи захисту. У підсистемах захисту і в комплексах задач, як правило, містять інформацію про порушення системи захисту та про атаки на інформацію. Такі повідомлення передбачають прийняття рішень на запобігання втрати інформації та посилення найбільш важливих напрямків захисту.

Повідомлення-запити можуть надходити протягом доби як в певні періоди часу так і в нерегламентному режимі. Це вид повідомлень вимагає в інформаційному плані складання і посилки на підсистему повідомлення-відповідь. Такий вид повідомлень в системах захисту найчастіше використовується в підсистемах, що базуються на засобах обчислювальної техніки, причому повідомлення-запити можуть надходити як від віддалених, так і безпосередньо пульта оператора. Здійснення повідомлень-відповідей обумовлюється характером надходження повідомлень-запитів, а обсяг повідомлень-відповідей залежить від організації та повноти інформації. За характером використання вмістимої інформації повідомлення можна розділити на два: що містять автономну інформацію, прийняття рішень по якій не залежить від інформації в інших повідомлення, і містять інформацію, використання якої можливе при надходженні всієї безлічі повідомлень.

Найбільш високим ступенем оперативності мають подієві та повідомлення-запити, час обробки яких не повинно перевищувати декількох хвилин.

Література

1. Хохлачева Ю.Е. Обработка информационных потоков и составление для них расписаний в системах защиты информации / Хохлачева Ю.Е., Хорошко В.А., Иванченко Е.В. / Інформатика та математичні методи в моделюванні, т.4., №3, 2014. – С. 256-263.

2. Хорошко В.А. Особенности защиты информации в сетях связи / Хорошко В.А., Хохлачева Ю.Е. // Вісник СНУ ім. В.Даля, №15(204), ч.1, 2013. – С. 219-222.

УДК 351:007

Чередниченко А.О.
кандидат економічних наук
Харківський національний університет міського господарства імені О.М.Бекетова
Чередниченко О.Ю.
кандидат економічних наук, доцент
Інститут підготовки юридичних кадрів для СБУ Національного юридичного університету імені Ярослава Мудрого

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ БУДІВЕЛЬНОЇ ГАЛУЗІ

Ефективність роботи вітчизняних будівельних підприємств, як підприємств базових галузей економіки країни, багато в чому обумовлена середовищем його функціонування, як внутрішнього, так і зовнішнього. Це знаходить своє вираження в широкому спектрі постійно і динамічно змінюваних небезпек і загроз, здатних чинити негативний вплив на результати діяльності, рівень безпеки і конкурентоспроможність підприємств.

Систему економічної безпеки будівельних підприємств можна охарактеризувати як цілісний, структурно позначений, складний, централізований комплекс методів, дій і засобів захисту підприємства від небезпек і загроз внутрішнього та зовнішнього середовища і забезпечення активного розвитку підприємства.

Головною метою управління економічною безпекою вказаної категорії підприємств є забезпечення ефективного функціонування, продуктивної роботи операційної системи та економічного використання ресурсів, забезпечення певного рівня персоналу та якості господарських процесів підприємства, його стабільного розвитку.

До основних функціональних цілей управління економічною безпекою підприємств будівельної галузі належать:

- забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності підприємства;
- забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу;
- досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;
- досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу;
- мінімізація руйнівного впливу результатів виробничо-

господарської діяльності на стан навколишнього середовища;

- якісна правова захищеність усіх аспектів діяльності підприємства;

- забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації;

- ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Загальна схема процесу управління економічною безпекою включає такі дії (заходи), що здійснюються послідовно або одночасно:

- формування необхідних корпоративних ресурсів (капіталу, персоналу, прав інформації, технології та устаткування);

- загально стратегічне та тактичне прогнозування та планування економічної безпеки за функціональними складовими;

- стратегічне та тактичне планування фінансово-господарської діяльності підприємства;

- оперативне управління фінансово-господарською діяльністю підприємства;

- здійснення функціонального аналізу рівня економічної безпеки;

- загальна оцінка досягнутого рівня економічної безпеки.

Динамічність зовнішнього і внутрішнього середовища будівельних підприємств обумовлює необхідність врахування постійних змін, і як наслідок, інформаційної складової, що призводить до збільшення обсягу прийнятих управлінських рішень і, зростання обсягів інформації. Процеси управління в системі економічної безпеки будівельних підприємств повинні бути нерозривно пов’язані з пошуком і аналізом інформації, діагностикою небезпек і можливостей, пошуком оптимальних шляхів реагування та захисту об'єктів. В таких умовах нагальною для цілей управління виступає потреба в достовірній обліково-аналітичній інформації, що дозволяє діагностувати поточну діяльність підприємства, враховуючи всі ризики, ідентифіковані й оцінені системою бухгалтерського обліку, та передбачити майбутній розвиток, виходячи з прогнозних розрахунків. Зважаючи на те, що процес формування та функціонування системи економічної безпеки пов'язаний з постійними значними інформаційними потоками, на перший план в управлінні економічною безпекою цих підприємств виступає необхідність наявності цілісної інформаційної системи.

Система аналітичної інформації для прийняття управлінських рішень відрізняється складністю, бо відбувається систематичне зростання обсягів інформації, її надмірності при інформаційній недостатності для прийняття оптимальних управлінських рішень. Інтегрована

обліково-аналітична система будівельного підприємства має розглядатися, як система бухгалтерського, фінансового і управлінського обліку, система податкового і екологічного обліку, соціального обліку, а також система внутрішнього контролю. Синтез перерахованих вище елементів, об'єднання методологічного та організаційного аспекту, дозволяє змінити методологію управління економічною безпекою будівельних підприємств, в основі якої буде закладена концепція формування інтегрованої обліково-аналітичної системи підприємства, спрямована на підвищення його ефективності та результативності.

УДК 004.91

Чередниченко О.Ю.
кандидат економічних наук, доцент
Інститут підготовки юридичних кадрів для СБУ Національного юридичного університету імені Ярослава Мудрого

АКТУАЛЬНІСТЬ ТА ПРОБЛЕМНІ ПИТАННЯ ПРАКТИЧНОГО ВТІЛЕННЯ ПОНЯТТЯ «ПЕРСОНАЛЬНОГО ОНЛАЙН-КАБІНЕТУ» В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

Розвиток науково-технічного прогресу, зміни в громадянському та соціально-економічному середовищі країни, нові загрози в сфері боротьби з кримінальними злочинами та необхідність впровадження найкращих світових стандартів підштовхують вітчизняного законодавця до внесення змін кримінально-процесуального законодавства. З цього приводу в середовищі як законодавців так і практичних фахівців розгорнута серйозна дискусія.

В теперішній час до відповідних комітетів Верховної Ради України подано декілька нових законопроектів щодо змін чи прийняття нових кримінально-процесуальних кодексів, в одному з яких пропонується введення такого поняття як «персональний онлайн-кабінет» для доступу судів, адвокатів та самих звинувачених до матеріалів кримінального провадження в електронному вигляді. Це стосується відеозаписів засідань, фото- відео доказів, сканування документів, процесуальних записів тощо. Причому, роботу, щодо введення їх в спеціальний банк даних, пропонується покласти на технічних співробітників судів.

В результаті, виникає декілька проблемних питань, що може призвести не тільки до негативних наслідків чи збоїв у роботі судів, а й до порушень вимог діючого законодавства, насамперед про захист інформації з обмеженим доступом (закони України «Про дер-

жавну таємницю», «Про захист персональних даних», «Про інформацію» та ін.).

Дискусійним є і питання щодо механізму надання доступу до «онлайн-кабінету» для затриманих, які утримуються в закладах пенітенціарної системи за санкцією судів. Ця можливість також міститься в одному із законопроектів. Для цього треба обладнати технічними засобами всі заклади пенітенціарної системи одночасно, з метою уникнення порушень прав затриманих. Але основною проблемою є неможливість надійної протидії несанкціонованим втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, або, так званим, «хакерським атакам» (злочини передбачені ст. 361, ст.361-2, ст. 362, ст.363,ст.363-1 КК України). Причому їх наслідки можуть призвести не тільки до витоку інформації, а й скомпрометувати як посадових осіб учасників судочинства так і осіб які ще не є засудженими, інших суб'єктів кримінального судочинства, правоохоронців тощо. Також, незрозуміло яким чином будуть долатися чисельні вимоги, що стосуються технічного захисту обладнання (насамперед комп'ютерів, комп'ютерних мереж, систем), приміщень, інформаційних ресурсів (баз даних), допуску технічного персоналу до роботи з документами з грифами обмеженого доступу і т.ін. Яскравим прикладом не зовсім вдалого вирішення проблеми технічного захисту інформаційних ресурсів є введення в дію восени 2016 року Національним агентством запобігання корупції (НАЗК) системи, так званого «е-декларування» та послідуючі проблеми її експлуатації.

Також, виникає і ще одна проблема – різке зростання кількості секретоносіїв не тільки з числа штатних посадовців в судах, насамперед з числа технічного персоналу (це не тільки спеціалісти, які повинні вводити інформацію в систему та фахівці з захисту, ремонту, експлуатації), а й особи зі сторони захисту. В свою чергу, це призведе не тільки до додаткових обов'язкових заходів з персональної перевірки на предмет можливого допуску до роботи з інформацією з обмеженим доступом, а й до додаткового фінансового навантаження (наприклад, доплат за секретність тощо).

Окремі правники вбачають в цієї ідеї ще й спробу збільшити судовий сбір, інші сплати до бюджету (бо пропонується брати такого роду платежі із нерозглянутих справ, кількість яких дуже велика).

Таким чином, не ставлячи під сумнів необхідність «осучаснення кримінального процесу», поспішне, ретельно неопрацьоване прийняття рішення щодо впровадження системи «персональний онлайн-кабінет» може призвести не до покращення, а навпаки до погіршення ситуації та виникнення передумов до низки порушень норм діючого

законодавства, прав і свобод громадян.

Тому, для вирішення вказаних проблемних питань як на етапі підготовки законопроекту та і в процесі його апробації й впровадження, необхідний комплексний підхід із залученням не тільки фахівців-праників, а і спеціалістів в галузі технічного захисту інформації, ІТ-технологій, спеціалістів щодо захисту інформації з обмеженим доступом, пенітенціарної системи, співробітників-практиків правоохоронних органів, співробітників судів та інших фахівців.

УДК 004.056.5

Шевченко А.С.
кандидат технічних наук
Військовий інститут телекомунікацій та інформатизації

КОНЦЕПЦІЯ ПОБУДОВИ ТЕХНІЧНОЇ СКЛАДОВОЇ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

В період з 2014 та по сьогоднішній час, під час анексії Автономної республіки Крим та в ході бойових дій на сході України з боку Російської Федерації (РФ) здійснюються масовані кібернетичні атаки на елементи критичної інформаційної інфраструктури держави та Збройних Сил (ЗС) України вчасності. Межі протистояння у кіберпросторі не обмежуються територією збройного конфлікту, що загострює питання захисту власних ресурсів.

Реалізація атак в кібернетичному просторі ЗС України призводить до витоку інформації, несанкціонованого доступу та порушення керованості елементами ІТС, відмови в доступі до ресурсів та систем, дезінформації особового складу ЗС. Наявність вразливостей ІТС, систем захисту інформації та низька підготовленість особового складу ЗС призводить до суттєвих ризиків інформаційної безпеки, а успішна реалізація кібернетичних атак призводить до значних збитків.

На сьогоднішній час в Україні лише формується система кібернетичної безпеки (СКБ). Розвиток СКБ ґрунтується на формуванні нормативно-правової бази з кібернетичної безпеки, формуванні та впровадження у діяльність організаційних заходів, побудови технічної складової та підготовці кадрів з кібернетичної безпеки [1].

Одним о основних та найбільш критичним на сьогодні є питання побудови технічної складової СКБ. При вирішенні даного завдання виникає велика кількість протирічь. Деякі з напрямків розвитку технічної складової СКБ ведуть до значного перевитрачання державних фінансових ресурсів, при чому зовсім не виправдовуючи

незначне підвищення ефективності захисту.

З огляду на це, актуальним та невідкладним завданням є формування концепції побудови технічної складової СКБ для захист кіберпростору ЗС України.

З урахуванням особливостей побудови ІТС, сучасних систем захисту інформації та кібернетичної безпеки можна виділити наступні функціональні рівні кіберпростору [2]:

рівень інформаційних систем (програмного забезпечення);

рівень кінцевого телекомунікаційного обладнання;

рівень мережного телекомунікаційного обладнання;

рівень транспортної телекомунікаційної мережі.

Під час управління військами вказані функціональні рівні кіберпростору взаємодіють з рівнями які об'єднують особовий склад та фізичне середовище стаціонарних та польових об'єктів.

Для забезпечення безпеки кіберпростору ЗС України необхідне впровадження комплексу систем та механізмів захисту ІТС на різних функціональних рівнях кіберпростору. До таких систем та механізмів відносяться [3]:

системи розмежування доступу користувачі до елементів ІТС;

системи міжмережного екранування на основі фаерволів (*Firewall*);

системи та механізми криптографічного захисту інформації;

віртуальні приватні мережі *VPN*;

системи антивірусного захисту елементів ІТС;

системи виявлення та запобігання вторгненням (*IDS/IPS*);

механізми автентифікації, авторизації та аудиту (*AAA*);

системи попередження втрати даних (*DLP – data loss prevention*).

системи управління інформацією та подіями безпеки (*SIEM*).

системи аналізу захищеності (САЗ) та інші.

Як відомо, найбільш ефективним підходом для побудови систем захисту інформації є ешелонований захист. Відповідно, при побудові технічної складової СКБ необхідно враховувати, що не один з програмних або апаратно-програмних засобів захисту інформації та забезпечення кібербезпеки відомих вендорів не дозволяють забезпечити 100 % захисту. Відповідно до цього багато рубіжна система захисту дозволить підвищити ефективність захисту та знизити ризик від реалізації кібернетичних загроз. Одним з основних питань при цьому залишається оптимізація фінансових витрат.

Важливою частиною технічної складової СКБ є реалізація підсистеми збору та аналізу інцидентів кібернетичної безпеки. На сьогоднішній день здійснення розслідування кібернетичних інцидентів

є процесом досить складним. Для автоматизації та забезпечення взаємодії різних державних структур (ЗСУ, СБУ, ДССЗЗІ, МВС тощо) доцільно впровадити єдину уніфіковану підсистему збору та обробки даних кібернетичної безпеки. Дана підсистема повинна забезпечувати можливість аналізу стану кібернетичної безпеки, відслідковувати та розслідувати інциденти кібернетичної безпеки з забезпеченням візуалізації та зручного представлення даних. Прикладами даних систем є централізовані систему моніторингу стану інформаційної безпеки та кібернетичних атак Cisco Cyber Threat Defense та WatchGuard Dimension.

Забезпечення кібербезпеки Збройних Сил України – завдання яке потребує значних фінансових затрат, тому для вибору рішень щодо його вирішення потрібно підійти комплексно, враховуючи досвід країн НАТО та США. Впровадження систем та механізмів захисту інформації дозволять забезпечити комплексний захист кіберпростору ЗС України з урахуванням стаціонарної та польової компоненти.

Література

1. Стратегія кібербезпеки України. URL: http://zakon5.rada.gov.ua/laws/show/96/2016 – Назва з екрану.

2. Cyberspace operations : Air Force Doctrine Document 3-12. – DOD US. – Government Printing Office, 2010. – 60 p.

3. Шевченко А.С. Забезпечення захисту кіберпростору ЗСУ / А.С. Шевченко. // Телеком. Телекоммуникации и сети. Военная связь. Технологии, решения, проекты. – 2016. – Специальный выпуск. – С. 68-71.

УДК 342.9

Шевченко М.О.

Національна академія Служби безпеки України

ПРАВОВИЙ СТАТУС БІЖЕНЦІВ У КОНТЕКСТІ БОРОТЬБИ З ТЕРОРИЗМОМ

Відповідно до визначення правового статусу біженця та підстав набуття такого статусу існує науково обґрунтована позиція дослідника І. Г. Ковалишина в цій сфері, який зазначає, що проблема правового статусу біженців, з одного боку, це частина загальної проблеми правового статусу особи в сучасному світі прав людини і громадянина; з іншого – цю проблему необхідно розглядати як складову проблеми правового статусу іноземців у країні їх тимчасового перебування. Проблема біженців в Україні існує й дедалі загострюється як правова, гуманітарна, політична [1].

Показово, що зміни векторності терористичної діяльності наклали відбиток і на проблему правового статусу біженців та захисту прав людини.

Набуття статусу біженця в України не завжди супроводжується справжньою метою особи набути його за законодавством України та продовжити проживання на її території як законослухняного мігранта.

Через анексію Криму та у зв'язку із проведення антитерористичної операції на території Донецької та Луганської областей, менш контрольованим стало питання перетину кордону України та притоку осіб, задіяних в терористичній діяльності. При цьому, порядок набуття статусу біженця за законодавством України має «слабкі» місця, які можуть бути використані мігрантом як законна підстава перебування на території України, під час якого особа може займатися терористичною діяльністю.

Актуальність зазначеної темактики обумовлено тим, що існуючий правовий механізм набуття статусу біженця є недостатньо відпрацьованим та регламентовним.

Метою дослідження є з'ясування та розкриття поняття правового статусу біженця, з'ясування стадій набуття такого статусу та виявлення проблемних питань, що виникають у зв'язку з цим та можуть бути використані для здійснення терористичної діяльності.

Завдання дослідження:

- дослідити поняття правового статусу біженців та його законодавче регулювання;
- розкрити зміст стадій набуття правового статусу біженців в Україні та виявити можливості використання недоліків таких стадій для здійснення терористичної діяльності;
- встановити детермінанти вчинення біженцями злочинів терористичного спрямування;
- виявити шляхи подолання тероризму в контексті удосконалення міграційного законодавства.

Об'єктом дослідження є суспільні та правові відносини, пов'язані з набуттям та припиненням статусу біженця крізь призму виникнення та ескалації тероризму, а також здійснення міжнародно-правової протидії цьому злочину.

Предметом дослідження є правовий статус біженців у контексті боротьби з тероризмом.

З огляду на розглянуту проблематику можемо дійти висновку про необхідність внесення змін до чинного законодавства України, яке регламентує процес набуття правового статусу біженця. Для забезпечення запобігання терористичним актам на території України, авторами пропонується удосконалити нормативно-правову базу, що

регулює боротьбу з тероризмом, а саме:

1) передбачити навчання окремих працівників територіальних міграційних органів, спрямоване на підготовку спеціалістів у справах біженців;

2) забезпечити оперативність взаємозв'язку Держаної прикордонної служби України з Державною міграційною службою України та Службою безпеки України з питання збирання та передачі інформації щодо мігрантів, які виявили бажання отримати статус біженця в Україні;

3) встановити квоти на кількість мігрантів, які протягом року можуть отримати статус біженця в Україні, з метою забезпечення повноцінного контролю за їх працевлаштуванням та отриманням соціальних гарантій, періодичного моніторингу способу їхнього життя в контексті боротьби зі злочинністю, в тому числі з тероризмом та встановлення яких даватиме можливість ретельної перевірки таких осіб, тобто вжиття заходів щодо «відсіювання» серед біженців осіб з потенційними терористичними ризиками;

4) призначення особам, які звернулися із заявою про надання статусу біженця, соціальних виплат, які гарантували б особам можливість проживання в країні протягом періоду до отримання статусу біженця та можливості офіційного працевлаштування;

5) встановити абсолютну заборону на придбання та зберігання зброї особами, які отримали статус біженців;

6) створити Єдиний центр узагальнення інформації з координації антитерористичної діяльності та моніторингу її стану на базі Служби безпеки України, законодавчо регламентувати його діяльність в Україні;

7) розробити та запровадити програми із заохочення інформаторів, які повідомлятимуть Службу безпеки України про підготовку терористичних актів;

8) врегулювати порядок реєстраціі біженців, роботу з шукачами статусу біженців, які прибули в Україну без документів, яким відмовлено у наданні статусу біженця через перебування до прибуття в Україну в третій безпечній країні;

9) врегулювати питання видворення осіб, які втратили або позбавлені статусу біженця і не мають інших правових підстав перебування на території України;

10) використовувати ЗМІ, у т. ч. Інтернет, для надання громадянам країни ширшого доступу до інформації стосовно вчинених проти їх держави терористичних актів для пропаганди антитерористичної спрямованості та для вжиття заходів соціальної профілактики тероризму.

Вивчення зарубіжного досвіду у контексті міграційних процесів та усунення прогалин у правовому регулюванні статусу біженця з метою запобігання та протидії тероризму є найголовнішим завданням у боротьбі з тероризмом на державному рівні.

Діяльність органів із запобігання та протидії тероризму передбачає виконання завдань організаційного, правового, інформаційного та оперативно-розшукового характеру при взаємодії всіх суб'єктів боротьби з тероризмом, а саме: профілактику терористичної злочинності; виявлення та усунення причин та умов, що сприяють виникненню терористичної злочинності; виявлення ознак терористичної діяльності; встановлення контролю за діяльністю структур, які мають зв'язки з терористами.

Література

1. Деякі аспекти правового статусу біженців та осіб, які потребують додаткового захисту в Україні. [Електронний ресурс] / Ю. М. Мартинюк // Митна справа. – 2013. – № Спец. вип. – С. 87–91. – Режим доступу: http://nbuv.gov.ua/UJRN/Ms_2013_Spets.

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗОВНІШНІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

УДК 519.816

Андрійчук О.В.
кандидат технічних наук
Інститут проблем реєстрації інформації НАН України
Ланде Д.В.
доктор технічних наук, старший науковий співробітник
Інститут проблем реєстрації інформації НАН України

ЗАСТОСУВАННЯ ІНСТРУМЕНТАРІЮ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ВИЯВЛЕННІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Інформаційна операція (ІО) [1] - це комплекс інформаційних заходів (новини в Інтернеті та медіа, коментарі в соціальних мережах, форумах і т.п.), націлений на зміну громадської думки про певний об'єкт (особистість, організація, інститут, країна і т.п.). При виявленні ІО слід враховувати вплив різних тематик публікацій на формування інформаційного простору.

В роботах [2-3] показано, що ІО відноситься до слабо структурованих предметних областей, для роботи з якими застосовують системи підтримки прийняття рішень (СППР) [4]. Застосування описаного в наступному пункті методики [2-3] вимагає наявності групи експертів. Робота експертів коштує досить дорого та потребує значного часу. Отже актуальною проблемою постає зменшення використання експертної інформації при побудові бази знань (БЗ) СППР при виявленні ІО.

1. Прогнозування зміни значень цільових показників об'єкта на поточний період

Сутність прогнозування зміни значень цільових показників об'єкта на поточний період полягає в наступному:

1. Проводиться попереднє дослідження об'єкта ІО, вибираються його цільові параметри (показники). Припускається, що раніше в ретроспективі вже мали місце ІО проти об'єкта і його стан (відповідні цільові показники) від них погіршувався.

2. Проводиться групова експертиза щодо визначення та декомпозиції цілей ІО, а також оцінці ступеня впливу. Таким чином, об'єкт ІО декомпозується як складна слабко структурована система.

Для цього використовуються засоби системи розподіленого збору і обробки експертної інформації (СРСОЕІ).

3. Будується відповідна база знань (БЗ) засобами СППР на підставі результатів проведеної засобами СРСОЕІ груповий експертизи, а також наявної об'єктивної інформації.

4. Проводиться аналіз динаміки тематичного інформаційного потоку засобами системи контент-моніторингу (СКМ). Доповнюється БЗ СППР.

5. Розраховуються рекомендації засобами СППР на підставі побудованої БЗ у вигляді прогнозу зміни значень цільових показників об'єкта на поточний період.

2. Визначення рейтингу інформаційного впливу тематик публікацій, які пов'язані з деякою подією за поточний період

Сутність методики визначення рейтингу інформаційного впливу тематик публікацій, які пов'язані з деякою подією за поточний період полягає в наступному:

1) Проводиться групова експертиза щодо визначення та декомпозиції цілей ІО, як складної слабо структурованої системи. Для цього використовуються засоби СРЗОЕІ.

2) Засобами СППР будується відповідна БЗ на підставі результатів проведеної засобами СРЗОЕІ груповий експертизи, а також наявної об'єктивної інформації.

3) Проводиться аналіз динаміки тематичного інформаційного потоку засобами СКМ. Доповнюється БЗ СППР частковими коефіцієнтами впливу.

4) Розраховуються рекомендації засобами СППР на підставі побудованої БЗ у вигляді рейтингу інформаційного впливу тематик публікацій.

Висновки

1) Запропоновано методику застосування інструментарію експертної підтримки прийняття рішень при виявленні інформаційних операцій, що дозволяє на підставі аналізу ретроспективи прогнозувати зміну значень цільових показників об'єкта на поточний період.

2) Запропоновано методику побудови БЗ СППР в процесі виявлення ІО, що дозволяє визначати рейтинг інформаційного впливу тематик публікацій, які пов'язані з деякою подією, за поточний період на основі аналізу ретроспективних даних.

Дослідження проведено в рамках проекту Ф73 / 23558 "Розробка методів і засобів підтримки прийняття рішень при виявленні інформаційних операцій". Проект є переможцем конкурсу Ф73 на грантову підтримку науково-дослідних проектів Державного фонду фундаментальних досліджень України і Білоруського республікан-

ського фонду фундаментальних досліджень.

Література

1. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія – К., Інтертехнологія, 2009 – 164 с.

2. Andriichuk O.V., Kachanov P.T. Usage of expert decision-making support systems in information operations detection / Proceedings of the International Symposium for the Open Semantic Technologies for Intelligent Systems (OSTIS 2017), Minsk, Republic of Belarus, 16-18 Ferbruary, 2017, pp. 359-364.

3. Андрейчук О.В., Качанов П.Т. Методика применения инструментария экспертной поддержки принятия решений при идентификации информационных операций / Информационные технологии и безопасность: Материалы международной научно-технической конференции 1 декабря 2016 года / – К: ИПРИ НАН Украины, 2016. – С. 141-155.

4. Тоценко В. Г. Методы и системы поддержки принятия решений. Алгоритмический аспект. К.: Наукова думка, 2002. 382 с.

УДК 343.1

Браіловський М.М.
кандидат технічних наук, доцент,
Київський національний університет
ім. Тараса Шевченка

ВИКОРИСТАННЯ ВІРТУАЛІЗАЦІЇ ДЛЯ СТВОРЕННЯ МЕРЕЖ МАЙБУТНЬОГО ПІД ЧАС НАДЗВИЧАЙНОГО СТАНУ

В період до 2020 року міжнародний союз електрозв’язку (МСЕ) прогнозує впровадження принципів створення мережі майбутнього – FN (Future Networks), визначення та основні положення якої наведені в рекомендації МСЕ Y.3001 [1]. Вищезазначені напрямки розвитку телекомунікацій стосуються будь якої країни і є достатньо суттєвими.

В України цей розвиток необхідно починати з вирішення уже існуючих проблем [2]: низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами; використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій; недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики

щодо регуляторного впливу на ринок телекомунікацій тощо.

Крім того, необхідно відзначити, що для України, зважаючи на її економічне та геополітичне становище, проблема створення майбутніх мереж набуває рівня – створення сучасної інфокомунікаційної мережі наступного покоління у стані надзвичайної ситуації (НС). Це обумовлене присутністю більшості факторів, характеризуючих НС, зокрема: часті відключення електроживлення, тероризм, складні технології, недостатня кваліфікація обслуговуючого персоналу, фізичний та моральний знос обладнання та механізмів тощо.

Таким чином, для створення систем майбутнього необхідно визначити вимоги не тільки до самих мереж, а й до мереж майбутнього при надзвичайних обставинах [Y.2205] [3] та наявності зовнішніх та внутрішніх загроз та атак.

Вдалим рішенням цієї проблеми може бути використання віртуалізації ресурсів мережі. Вона дозволяє створювати логічно ізольовані ділянки мережі в рамках спільно використовуваної фізичної мережевої інфраструктури таким чином, що в цій інфраструктурі можуть одночасно працювати багато різнорідні віртуальні мережі, що в свою чергу підвищує безпеку. Ця технологія дозволяє також об'єднувати багато ресурсів і створювати об'єднані ресурси, які вважаються єдиним ресурсом. Забезпечується підтримка динамічного переміщення логічних елементів мережі, послуг і можливостей між логічно ізольованими ділянками мережі. При цьому кінцеві користувачі або інші постачальники можуть знаходити такі дистанційні послуги та елементи і здійснювати до них доступ. Це означає, що користувач віртуальної мережі не обов'язково повинен мати власні фізичні мережеві ресурси. Це дозволяє динамічно додавати й видаляти необхідні ресурси у віртуальній мережі з пулу загальних віртуальних ресурсів у відповідь на що з'являються в ній зміни (збільшення або зменшення обсягу трафіку, поява відмов або збоїв в роботі мережевого обладнання та ін.). Оскільки додавання віртуальних ресурсів здійснюється набагато швидше і економніше, ніж розгортання додаткового фізичного ресурсу, функціонування та управління в цих мережах буде більш ефективне і гнучке.

Література:

1. Global information infrastructure, internet protocol aspects and next generation networks ─ future networks. Future networks: Objectives and design goals // Recommendation ITU-T Y.3001, 2011.

2. Кривуца, В. Г. Інфокомунікаційні мережі нового покоління: монографія / В. Г. Кривуца, Л. Н. Беркман, С. В. Толюпа; за ред. В. Г. Кривуци.— К.: ДУІКТ, 2012.— 288 с.

3. [Y.2205] http://handle.itu.int/11.1002/1000/11093

Горовий В.М.
доктор історичних наук, професор
Національна академія Служби безпеки України

ЕВОЛЮЦІЙНІ ПРИЧИНИ ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ

Активізація глобалізаційних процесів на основі розвитку електронних інформаційних технологій стала фактором нерівномірного, але одночасного входження в інформаційне суспільство країн світу, що до того знаходились на індустріальному і навіть доіндустріальному етапі розвитку. Дана нерівномірність стимулює розвиток суперечностей, викликаних неспівпадінням інтересів еволюції, на міждержавному рівні. Ці суперечності відтінюються однаковими вимогами нового суспільства до всіх членів світової спільноти держав незалежно від можливостей засвоєння його організаційно-технологічних особливостей. Ця характерна риса суттєво позначилась і на проблемах інформаційної безпеки в міждержавних відносинах, що в системі виникаючих протистоянь держав в сучасних умовах набуває першорядного значення. Використання інформаційного ресурсу Росії в якості інструмента негативних впливів на національний інформаційний простір нашої країни в «Доктрині інформаційної безпеки України» визначається як технологія гібридної війни проти України, технологія першорядного значення, що перетворює інформаційну сферу на ключову арену міждержавного протиборства.

У зв'язку з цим для нас нині є дуже важливим постійно враховувати спонукальні мотиви Російської Федерації в протистоянні з Україною. Причину цих мотивів, виводити, як це робиться в багатьох ЗМІ, лише з «імперських замашок», з «природної агресивності» нашого північного сусіди є справою малопереконливою, побудованою на чисто емоційних рефлексіях. У той же час вони, ці спонукальні мотиви, пов'язані з більш глибокими процесами, із відмінностями прояву в обох державах утвердження елементів нового, інформаційного суспільства в суспільстві індустріальному, що поступово відходить в минуле.

Інформаційне суспільство – це перше суспільство в людській історії, що не лише свідомо перетворює навколишню дійсність згідно із власними інтересами, але при цьому свідомо перетворює себе, самовдосконалюється як складна система, оптимізуючи свою ефективність. В порівнянні із індустріальним суспільством, де лише в дуже загальному вигляді міг пропонувати варіант руху в майбутнє «привид, що бродив по Європі», воно прагматично підходить до викори-

стання ідей, ідеологій, відображених у багатоваріантності політичних рішень, розроблюваних і уточнюваних на практиці при активній участі членів суспільства, яке називають сьогодні громадянським.

Очевидно, що майбутні дослідження інформаційного суспільства зможуть підтвердити невідворотність процесу розвитку громадянської активності як обов'язкового механізму даного етапу розвитку, що найбільше сприяє вивільненню творчого потенціалу людини. І якраз на нинішньому російському прикладі можемо наочно спостерігати той спротив, який елементи нового, інформаційного суспільства зустрічають, проникаючи в суспільство індустріальне, що вже втратило не лише перспективи свого розвитку, а й ідеологічну основу існування. Відсутність, в той же час, чіткої перспективи російського розвитку, орієнтирів у майбутньому без обов'язкової надії на зростання світових цін на нафту, фактичне обмеження розвитку національної економіки інтересами російських олігархічних монополій, зацікавлених насамперед експлуатацією багатих сировинних ресурсів, обумовлює застій еволюції російської держави і суспільства в сучасних умовах. Домінування олігархічних інтересів в міжнародних відносинах в принципі підмінило на практиці зміст декларованих раніше моральних принципів братського добросусідства Росії з країнами-сусідами, солідарності з росіянами за рубежем, на прагматизм прибутку і відштовхнуло сусідів.

Неможливість існування здорової творчої атмосфери в суспільстві все більше починає турбувати російську інтелігенцію, проявляється в російських ЗМІ. В той же час внесення цієї турботи до масової аудиторії в сучасному російському суспільстві стає все більш проблемним. Зростаюче цензурування владою вертикальних інформаційних обмінів, блокування горизонтальних, насамперед соцмереж, боротьба зі спробами суспільного оновлення з посиланнями на «інтереси народу» стала характерною особливістю інформаційних процесів у сучасній Росії. Ця особливість продовжує базуватись на спадкоємності традицій контролю за інформаційним простором, характерних ще для союзної держави.

У той же час в усьому розмаї соціальних трансформацій в Україні починають проявлятися паростки нових закономірностей, зрушення в напрямі до становлення громадянського суспільства. В основі цього процесу – середній клас: гуманітарна і інженерно-технічна інтелігенція, організатори дрібного і середнього бізнесу – всі освічені і невдоволені нинішніми можливостями своєї реалізації в сучасній Україні люди. Середній клас підтримав Майдан, впливав на розвиток його фактично деолігархічної ідеології. В результуючому процесі вона сприяє поступовому, з великими труднощами

перемелюванню олігархічної складової української економіки і пов'язаних з нею факторів впливу на суспільне життя, на економіку, доведену до перебування в десятці найбідніших країн світу.

Суттєві зміни геополітичної орієнтації українців в напрямі європейських цінностей, становлення громадянського процесу в Україні, фактичне свідоме протистояння традиційній інформаційній залежності від Москви через переформатування інформаційних вертикалей в національному інформаційному просторі – все це негативно сприйняте російським керівництвом і ввійшло в мотиваційну частину наступних трагічних подій.

Неприємною для нинішнього російського керівництва несподіванкою стало також і те, що, не зважаючи на всі проблеми становлення українського суспільства, український середній клас опанував інноваційний інструмент демократизації – електронні інформаційні технології. І з його допомогою поступово формує елементи нової ідеології, орієнтири інформаційного суспільства. Практика показує, що ці особливості розвитку стають все більш небезпечними для українських олігархів. Однак, вони небезпечні своїми всепроникаючими властивостями і самим прикладом функціонування також і для російської влади, що насьогодні успішно охороняє інтереси власних олігархів від незручностей, які вже завдає їм думаюча Росія. І дану небезпеку російська влада пробує нейтралізувати «на далеких рубежах», за межами своїх кордонів, традиційним для індустріального суспільства способом – силовими діями в Криму і на Донбасі.

У зв'язку з цим видається важливим широке роз'яснення в глобальному інформаційному просторі дійсних цілей російської пропаганди, всієї системи мотивацій нинішнього російського керівництва в інформаційній сфері. В той же час зростає актуальність введення в глобальний інформаційний простір матеріалів теоретичних досліджень з обґрунтуванням реальних причин російсько-українського протистояння, того, що в даному випадку керівництво РФ має справу не стільки з Україною, скільки з закономірностями суспільного розвитку. І спроби впливати на них застосуванням якихось технологій, навіть гібридних, в реаліях історичного процесу є справою малоперспективною.

Гринь А.К.
кандидат технічних наук, доцент
Національна академія Служби безпеки України
Гамаліна К.А.
Національна академія Служби безпеки України

ОСОБЛИВОСТІ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ В УМОВАХ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Досвід проведення антитерористичної операції на Сході країни показує, що Україна на період загострення соціального і збройного конфлікту та безрамкового інформаційно-психологічного впливу на суспільство була не готова до оперативного створення «інформаційної броні». Це зумовлено тим, що крім низької обізнаності суспільства у питаннях особистої інформаційної безпеки (це дає підстави для виникнення повної довіри до контенту засобів отримання інформації та легкого маніпулювання думкою), відсутня низка нормативно-правових актів у сфері інформаційної безпеки як складової національної безпеки України.

Як в мирний, так і військовий час досягнення інформаційної переваги над вірогідним, потенційним або реальним противником стає однією з основних цілей провідних країн світу, і в першу чергу така мета повинна бути в України. Основним інструментом для досягнення відповідної переваги над противником є спеціальні інформаційні операції.

Не дивлячись на ініціювання з боку науковців та державних установ нормативно-правових актів щодо інноваційних підходів у протидії інформаційно-психологічному впливу на населення під час проведення антитерористичної операції, в Україні за три роки збройного та інформаційного протистояння не сформований чіткий концепт із зазначених питань. Слід зазначити, що у Доктрині інформаційної безпеки України затвердженої Указом Президента України №47/2017 від 25.02.2017 р. тричі зустрічається формулювання «спеціальні інформаційні операції», проте жоден нормативно-правовий акт України не дає визначення відповідного поняття [1].

Крім того, проведення спеціальних інформаційних операцій та протидія їм відповідно до зазначеної Доктрини покладається на Службу безпеки України та Міністерство оборони України. Проте нормативно-правові акти, які регулюють діяльність згаданих суб’єктів включають в себе різну термінологію: «інформаційні операції», «психологічні операції», «інформаційно-психологічні опера-

ції», «спеціальні інформаційні операції», «пропаганда».

Закон України №638-15 від 07.05.2017 р. «Про боротьбу з тероризмом» визначає, що один із принципів боротьби з тероризмом – це комплексне використання правових, політичних, соціально-економічних, інформаційно-пропагандистських можливостей. Проте функції проведення спеціальних інформаційних операцій визначеними суб'єктами боротьби з тероризмом Закон не визначає [2].

З огляду на викладене, враховуючи проведення антитерористичної операції на Сході країни та активний руйнівний інформаційно-психологічний вплив з боку країни-агресора на населення України, жителів анексованого Криму та окупованих територій Донецької та Луганської областей вважаємо за необхідним:

- виключити правову колізію термінів «спеціальні інформаційні операції», «інформаційні операції», «психологічні операції», «інформаційно-психологічні операції», «пропаганда» у законодавстві України;
- шляхом змін до Законів України, які регламентують діяльність суб'єктів боротьби з тероризмом (в межах своїх повноважень) у розділ «функції» внести наступне: «проведення спеціальних інформаційних операцій та протидія їм»;
- з метою взаємодії та координації дій під час виконання оперативно-службової (бойової) діяльності із боротьби з тероризмом, створити робочий нормативно-правовий акт з грифом обмеження доступу «Концепцію проведення спеціальних інформаційних операцій в умовах антитерористичної операції», яка визначає стратегічні та тактичні плани проведення СІО, суб'єктів та їх функціонал, методологію та інструментарій.

Вважаємо, що зазначені положення будуть сприяти ефективному проведенню антитерористичної операції в контексті інформаційного протистояння та захисту інтересів особи, суспільства і держави в цілому.

Література

1. Про Доктрину інформаційної безпеки : Указ Президента України №47/2017. URL: http://www.president.gov.ua/documents/472017-21374

2. «Про боротьбу з теротизмом» : Закон України № 638-IV від 20.03.2003 (ред. від 07.05.2017). URL: http://zakon3.rada.gov.ua/laws/show/638-15

УДК 32.019.51

Дубов Д.В.
доктор політичних наук,
старший науковий співробітник
Національний інститут стратегічних досліджень
Дубова С.В.
кандидат історичних наук
Київський національний університет культури і мистецтв

ПУБЛІЧНА ДИПЛОМАТІЯ В УМОВАХ ВОЄННО-ПОЛІТИЧНИХ КРИЗ: КАМПАНІЯ США ПРОТИ ГРЕНАДИ

Публічна дипломатія є важливим чинником інформаційного позиціонування держави на міжнародній арені і сприяє досягненню її стратегічних цілей всією сукупністю доступних їй методів. До таких методів традиційно відносять [1]: програми освітніх обмінів (для вчених, студентів та школярів); програми відвідання країни; популяризація мови держави у світі та сприяння вивченню цієї мови іноземними аудиторіями; поширення знань про державу, її культуру, а також проведення культурних заходів та обмінів; забезпечення широкого спектру мовлення (радіо, телебачення, мережа інтернет) для закордонних аудиторій.

Водночас, в умовах воєнно-політичних криз різного рівня складності ці завдання частко змінюються. Як і для всієї системи стратегічних комунікацій держави, одним з основних завдань стає вироблення єдиного наративу для висвітлення ситуації, надання спікерам всіх рівнів належних месиджів для впровадження такого наративу у всіх публічних виступах.

В цьому сенсі показовим є те, як США інформаційно реагувало на ситуацію в Гренаді. 25 жовтня 1983 року ВС США розпочали військову операцію проти острівної держави Гренада, яка закінчилась вже 27-го жовтня перемогою американських військових сил. Сама операція була підготовлена поспіхом, мала багато неточностей та проблем із підтримкою. Вже 31 жовтня Держдепартамент США підготував документ [2] для ключових державних відомств (РНБ США, Міністерства оборони США, USIA та керівництву ЦРУ) щодо ситуації в Гренаді - «Теми публічної дипломатії щодо Гренади» [3]. Цей невеликий (2 сторінки) документ фіксує ключові тези, від яких мають відштовхуватись всі основні відомства у публічних дискусіях щодо подій в Гренаді. Він описує 6 основних напрямків, які можуть мати значення при вибудовуванні подальшої політики:

1. **Базова ситуація**. США, взаємодіяли з 6-ма карибськими

державами заради захисту життів та відновлення порядку у Гренаді. Ці колективні зусилля мали політичний та військовий вимір. США були невідворотною складовою військового аспекту, в той час як карибські держави є ключовими саме у політичному аспекті. Якщо б ці дії не були вжиті, це б створило загрозу іншим державам та миру в регіоні. ЗС США залишать Гренаду так швидко, як тільки це може бути. Але ми не знаємо, коли це станеться.

2. **Політичні аспекти**. Вбивство прем'єр міністра Бішопа та його колег вело до розпаду ефективного уряду Гренади. Лідері карибських держав вірили, що Бішоп був вбитий бо міг виграти вибори та очолити демократичні зміни, які б зменшили зростаючу мілітаризацію острова під контролем Куби. Оцінюючи ситуацію як безпосередню загрозу їх миру та стабільності, вони [карибські держави] визначили 21 жовтня як час діяти та шукали нашої допомоги. Вони дали нам ясно зрозуміти, що вони переконані, що подальша боротьба за владу буде пов'язана із внутрішнім насильством і що в результаті постане диктаторський режим.

3. **Гуманітарні питання**. Жорстока поведінка та записи членів Революційного народного уряду чітко показували, що вони готуються діяти як новий уряд, що змушує відчувати стурбованість щодо безпеки близько 1000 американців та інших іноземців у Гренаді. Наше занепокоєння безпекою американських громадян додатково посилились, коли під час комендантської години відбулась перестрілка та грабежі, а сама комендантська година була відмінена у п'ятницю 21 жовтня, що мало наслідком спроби місцевих жителів зафрахтувати човни та тікати.

4. **Стратегічні аспекти**. Гренада була єдиною державою Східних Карибів з військовими силами (замість поліцейських сил). Військові сили Гренади були 5 разів більші ніж у Барбадоса та на 50% більше ніж у Ямайки. На додачу, кубинські збройні сили таємно будували фортифікації, схованки зброї та військові комунікаційні споруди. Наша спроможність співпрацювати з урядами для дотримання миру та стабільності в регіоні має стратегічну важливість для США.

5. **Юридичні повноваження**. В цьому пункті йдуть численні посилання на пункти угоди OECS, окремі положення Статуту ООН та OAS.

6. **Поточна військова та політична ситуація**. Генерал-губернатор Гренади живий та неушкоджений та використовуючи свої повноваження надані йому Конституцією працює разом з OECS для відновлення порядку та функціонування інституцій. Організовані Кубою повстанці є основним фактором, що затримує завершення військової фази та початку політичної фази. Евакуація інозе-

мних громадян продовжується.

Цей документ є важливим прикладом того, як саме має швидко та професійно вибудовуватись загальний наратив навколо події, даючи чіткі відповіді на ключові питання, які можуть бути задані як посадовцям, так і недержавним учасникам системи публічної дипломатії. Заявлені ж теми дозволяли досить цілісно утримувати загальну рамку розуміння подій, мінімізуючи негативні наслідки для іміджу США.

Слід визнати, що цими директивами послуговувались більшість урядовців. Навіть виступ Р.Рейгана 4 листопада 1983 року який був присвячений низці питань (серед яких була і Гренада) містив ті самі формулювання, які були запропоновані в наведеному вище документі (наприклад, про дії у відповідь на запит держав Карибського басейну, а також про занепокоєння щодо безпеки американських та інших іноземних громадян тощо).

Література:

1. Defining Public Diplomacy. URL: http://uscpublicdiplomacy.org/page/what-pd

2. Briefing Papers on Grenada (CIA-RDP85M00364R001502590068-9). URL: https://www.cia.gov/library/ readingroom/

3. Greanda Public Diplomacy Themes (CIA-RDP85M00364R001502590073-3). URL: https://www.cia.gov/library/ readingroom/

УДК 35.078.3:025.4.03+65.012.8

Князєв С.О.
кандидат юридичних наук,
старший науковий співробітник
Національна академія Служби безпеки України

ІНФОРМАЦІЙНА ВІЙНА: ПРИЧИНИ ВИНИКНЕННЯ ТА СУЧАСНІ ТЕНДЕНЦІЇ

Сучасний розвиток світового суспільства супроводжується масовим впровадженням інформаційних технологій у різні сфери життя. Інформаційно-комунікативні технології суттєво спростили можливість різноманітного спілкування між людьми. Саме завдяки цьому чиннику кордони між країнами стали майже прозорими для різноманітних видів зв’язку, а відстань для спілкування взагалі перестала відігравати роль перепони. Значна кількість соціальних мереж об’єднали мільйони користувачів у всьому світі відповідно до їх уподобань, інтересів, поглядів, ділових стосунків, знайомств тощо.

Швидка та доступна можливість отримати майже будь-яку інформацію у «світовій павутині» з використанням різних пошукових систем, баз даних, електронних видань дозволяє припустити, що паперові видання, найближчим часом можуть стати раритетними спогадами.

Разом з тим, поряд з вагомими перевагами, які отримує від інформаційних технологій людство, з'явились, активно розвиваються і поширюються новітні загрози як для життєдіяльності самої людини, так і для безпечного існування цілих держав.

Особливість сучасного суспільства полягає в тому, що в руках значної кількості людей опинилися інструменти впливу на громадську думку, які раніше були доступні лише небагатьом – політикам, журналістам, дипломатам, відомим особистостям, тим, хто мав доступ до ЗМІ. Сьогодні при бажанні й ентузіазмі можна без особливих зусиль акумулювати серйозні людські ресурси. Це й дозволяє влаштовувати масові акції, демонстрації, протести швидкого реагування, а також забезпечувати миттєве поширення інформації.

Крім того, дослідження психологів підтвердили вельми небезпечну тенденцію: молоді люди, які з дитинства перебувають у світі телекомунікації, звикають до глибокого занурення у віртуальний простір, що змушує їх сприймати об'єкти звичайної культури як незначні й навіть нереальні [1; 3]. Така людина інформаційного суспільства може втратити вміння прогнозувати навіть найближче майбутнє, оскільки в неї надмірно розвивається шаблонність мислення, що робить її слухняним об'єктом інформаційних технологій.

Сучасна швидкість розповсюдження та подання інформації завдяки інформаційним технологіям, ефективність її сприйняття дозволяють у мільйони разів помножити наслідки від «розкидання з літаків пропагандистських листівок», що активно використовувалось під час Другої світової війни.

Тепер перекручування, підміна змісту інформації, трактування подій і фактів на певну користь стає основою страшної, руйнівної зброї, спрямованої на маніпулювання свідомістю як населення окремої країни, так і взагалі світової спільноти. Широкомасштабне, цілеспрямоване проведення таких дій на державному рівні сприяло появі поняття «інформаційна війна».

Досить часто під цим терміном розуміють всеохоплюючу, цілісну стратегію реалізації інформаційно-психологічного впливу на противника, зумовлена зростаючою значущістю і цінністю інформації у питаннях політики й управління [1; 2].

Як зазначають аналітики, з масовим упровадженням інформаційних технологій і застосуванням інформаційної зброї метою війни стало не знищення супротивника, а цілеспрямоване керування ним [3; 4].

Іншими словами, інформаційні технології в наш час зробили, як видавалось, неможливе – «дистанційне управління противником» за мінімального насильства і кровопролиття. Тепер завдання знешкодження противника полягає не у знищенні живої сили, а у зміні світоглядних орієнтирів населення, руйнуванні інфраструктури держави, зокрема збройних сил, у підриві авторитету керівництва держави тощо.

Причини проведення інформаційної війни можуть бути різні. Зокрема, територіальні зазіхання. Масована, цілеспрямована пропагандистко-підривна інформація, врешті-решт має спровокувати місцеві референдуми, відокремити частину території від решти країни, а далі – поглинання цієї території країною – інформаційним агресором.

Крім того, досить часто інформаційна війна може бути пов'язана із забезпеченням ринку збуту для своєї економіки. У цьому випадку вона стає складовою частиною конкурентної боротьби. Переваги отримує той, хто контролює більше інформаційного простору та застосовує ефективніші інформаційні технології.

На закінчення варто навести думку німецького філософа і психолога Еріха Фромма (1900-1980), який у фундаментальній праці «Анатомія людської деструктивності» (1973) звернув увагу на те, що людині, як істоті, важливо спиратися на певну систему моральних координат – розділяти добро і зло, щоб протистояти зовнішнім загрозам.

Якщо особа чітко ідентифікує себе з певним суспільством, бачить себе частиною групи, колективу, єдиної держави, вона здобуває «моральне коріння», оскільки суспільство пропонує їй певну систему координат, яка допомагає всім колективно вижити в найскладніших ситуаціях. Адже недарма найменше піддаються маніпулюванню люди з чітко вираженою соціальною позицією, оскільки маніпулятивні дії пропорційно співвідносяться із соціокультурною ідентичністю, освіченістю, груповою солідарністю тощо [2; 4]. Саме тому у виробленні колективного, загальнодержавного спротиву в умовах інформаційної війни особливе значення має система виховання й освіти, яка розвиває громадянські якості, патріотизм, любов до Батьківщини.

Література

1. Богуш В. М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К.: «МК-Прес», 2005. – 431 с.

2. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення // Information technology. Вісник НАДУ, 2015. - № 1. – с. 136 - 141

3. Кухаренко Р. Інформаційні війни в українському контексті. URL: http:// http://www.global-analityk.com/

4. Юринець Ю. «Інформаційні війни» України та Росії в контексті ст.10 ЄКПЛ // Юридична Газета. - Режим доступу : http://yur-gazeta.com/publications/practice/inshe/informaciyni-viyni-ukrayini-ta-rosiyi-v-konteksti-st10-ekpl.html

УДК 004.491.2

Козюра В.Д.
кандидат технічних наук, доцент
Національна академія Служби безпеки України
Степаненко В.І.
Державний університет телекомунікацій
Хорошко В.О.
доктор технічних наук, професор
Національний авіаційний університет України

ТАРГЕТОВАНІ КІБЕРАТАКИ – РЕАЛЬНА ЗАГРОЗА ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Кібератаки, здійснювані проти об'єктів критичної інфраструктури України носять цілеспрямований характер. Про це свідчать инцинденты, пов'язані з енергосистемами західних областей України, спроби вторгнення в інформаційно-телекомунікаційні системи повітряного транспорту, атаки на сайти державних органів і т.п.

Таргетована атака (від англ. target - цільова) є безперервним тривалим процесом несанкціонованої активності в умовах конкретного об'єкту критичної інфраструктури, покликаний здолати конкретні механізми забезпечення безпеки і завдати конкретного збитку (фізичного, інформаційного, морального і т.д.). Цей процес видалено керований в реальному часі організованою професійною групою хакерів, озброєних витонченим технічним інструментарієм.

Інструментарієм таргетованих кібератак є засоби APT (Advanced Persistent Threat – атакуюча безперервна загроза) – комбінація спеціальних утиліт видаленого доступу, шкідливого програмного забезпечення, механізмів використання уразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки.

Цільова кибератака включає наступні фази:

1. Підготовка – виявлення об'єкту атаки, збір детальної інформації про об'єкт, спираючись на яку виявляються слабкі місця в інфраструктурі, розробка стратегію атаки, моделювання атаки, підбір і розробка інструментів атаки, їх тестування на стендах.

2. Проникнення – активна фаза атаки, що використовує комбіновану техніку соціальної інженерії й уразливостей «нульового дня» для первинного інфікування цілі та проведення внутрішньої розвідки. Після закінчення розвідки і визначення приналежності інфікованого хоста по команді порушника через центр управління може завантажуватися додатковий шкідливий код.

3. Поширення – фаза закріплення усередині об'єкту критичної інфраструктури переважно на ключових комп'ютерах. При необхідності через центри управління вносяться необхідні корективи в шкідливий код на основі зібраної ключової інформації.

4. Досягнення мети – ключова фаза цільової атаки, залежно від вибраної стратегії в ній може застосовуватися внесення змін до технологічних процесів, що призводять до аварій і катастроф, розкрадання закритої інформації, умисне внесення змін до закритої інформації, маніпуляцій з бізнес-процесами, розкрадання фінансових ресурсів та ін.

Обов'язкова умова цільової кибератаки – приховання слідів активності на усіх її етапах.

Інструментарієм проникнення на об'єкти критичної інфраструктури є:

- експлойти – шкідливі коди, що використовує уразливості в програмному забезпеченні;
- валідатори – шкідливі коди, вживані в первинному інфікуванні об'єктів атаки з метою збору інформації про хости і передачі її в командний центр для подальшого прийняття рішення про розвиток атаки;
- завантажувачі модуля доставки Dropper (використовуються в атаках, побудованих на методах соціальної інженерії);
- модуль доставки Dropper – троянська програма, завданням якої є доставка основного вірусу Payload на заражену комп'ютер;
- вірус Payload – основний шкідливий модуль в цільовій атаці, що завантажується на інфікований хост. Складається з декількох модулів, кожен з яких виконує свою функцію (клавіатурного шпигуна, видаленого доступу, поширення усередині інфраструктури, взаємодії з командним центром, шифрування, управління технологічними процесами, очищення слідів активності, самознищення і т.д.).

Що можна протиставити таргетованим кибератакам?

1. Запобігання цільовим атакам – не допустити запуск неконтрольованих процесів в корпоративній мережі. Основні заходи: а) технічні рішення (захист кінцевих точок, міжмережеві екрани і системи запобігання вторгненням); б) навчання персоналу (ознайомлення з кіберзагрозами, тренування з кібербезпеці і т.п.).

2. Виявлення слідів атаки, розпізнавання ознак зараження. Для цього використовуються мережеві/поштові сенсори, що дозволяють здійснювати збір інформації з різних контрольних точок, сенсори робочих станцій, що дозволяють збільшити охоплення і деталізацію аналізованої інформації, компоненти динамічного аналізу об'єктів, центри аналізу аномалій, хмарні сервіси – оновлювані в реальному

часі бази знань про загрози.

3. Реагування – реакція на інцидент інформаційної безпеки – застосування набору прийнятих процедур, спрямованих на мінімізацію збитку і усунення наслідків атаки. Етапи реагування включають ідентифікацію, заборону, лікування, відновлення, профілактику.

4. Прогнозування – реалізація проактивних заходів, що дозволяють істотно утруднити порушникам підготовку і проведення атаки. Етап прогнозування включає наступний набір послуг: тест на проникнення, оцінка рівня захищеності, своєчасна оцінка уразливостей, аналітичний звіт про загрози інформаційної безпеки.

УДК 32.01:[316.772.4–021.131:316.621]

Кудирко В.М.
ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»
Горшков Г.М.
ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського»

ЩОДО ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ АСТРОТЕРФІНГУ В ІНФОРМАЦІЙНІЙ АГРЕСІЇ РФ НА ШКОДУ ІНТЕРЕСАМ УКРАЇНИ

Методи та засоби інформаційного протиборства постійно вдосконалюються. За таких умов технологія впливу тролінгу на індивідуальну та масову свідомість, була взята на озброєння інформаційної війни, як активний елемент пропаганди і контрпропаганди. Нове явища отримало назву «астротерфінг».

Астротерфінг - використання сучасного програмного забезпечення або спеціально найнятих оплачуваних користувачів для штучного управління громадською думкою, з метою заглушити думки реальних користувачів на Інтернет-форумах і підмінити їх думку на іншу, так би мовити, потрібну.

Термін був придуманий інтернет-користувачами. Походить від назви популярного бренду AstroTurf - синтетичного килимового покриття, яке виглядає як справжня трава.

Даний вид інформаційно-психологічного протиборства активно використовується Російською Федерацією в інформаційній війні проти України. Паралельно з боями, вибухами, захопленням полонених ведуться дії, для завоювання інформаційної переваги над Україною з боку російського агресора.

Над створенням викривленої картинки світу у віртуальному просторі «трудяться» цілі «фабрики тролів», і потреба в таких «бійцях» постійно зростає. Найбільш відомими з них давно стали так

звані «ольгінські тролі», за назвою одного з передмість Санкт-Петербурга, де спочатку знаходився їх офіс. За деякими оцінками, на утримання лише одного цього офісу під нейтральною назвою ТОВ «Агентство Інтернет-досліджень» зі штатом понад 400 тролів витрачається не менше 20 млн. рублів на місяць. А таких «фабрик брехні» розплодилося сьогодні в Росії десятки.

До їх основних завдань належить створення видимості масовості, донесення оплаченої позиції, зіпсування неугодної дискусії, під пропагандистськими матеріалами для схвалення або засудження, стимулювання дискусії, спотворення інформаційного фону брехнею, дезорієнтація читачів, паралізування громадянської активності.

Основна небезпека тролів полягає в тому, що вони в більшості випадків намагаються маскуватися під представників певного соціального прошарку громадян України. В українському кіберпросторі сьогодні працюють чотири основних типи проросійських тролів:

Ультрарадикали. Як правило, їх пости рясніють закликами до повалення існуючої влади революційним шляхом. Акаунт і аватарки - мілітаризовані та малюють образ їх автора як воїна АТО, козака чи члена добробату. Зображення облич здебільшого у балаклавах, «арафатках» або тактичних окулярах.

Політкоментатори. Цей тип троля полюбляє прикрашати свої сторінки в соцмережах цитатами видатних політиків, здебільшого про боротьбу чи зраду. Постять некоректні чи образливі фото діючих політиків та держпосадовців. Здійснюють різноманітний тролінг та викривлення резонансних політичних та суспільних подій.

Показові українці. Особливістю даного типу є аватарки з дівчатами-україночками у вінках зі стрічками національних кольорів, або парубки з прапорами чи у вишиванках на фоні українських пейзажів (пшениця, небо, Дніпро тощо). Пости вирізняються постійним негативом щодо дій влади, зокрема, зради інтересів народу, несправедливості, геноциду і т.п.

Хижаки. Це малочисельний, але не менш небезпечний тип тролів. Як правило, мають численні зв’язки у різних соцмережах, створюють та адмініструють групи, але самі рідко постять.

На нашу думку спецслужби Російської Федерації обрали методи тролінгу для ведення інформаційної війни проти України саме тому, що у тролів більше шансів бути прочитаними, бо коли користувач читає їхні дописи чи коментарі, він не бачить за ними прихованого активіста-пропагандиста чи солдата інформаційної війни. Для нього це грубий, моментами брутальний користувач, який висловлюється з елементами абсурдності й чорного гумору. Він має громадянську позицію і подає її в незвичний спосіб, що лише привертає увагу одно-

думців чи людей, які сумніваються. У своїх дописах тролі не використовують жодних аргументів чи правдивих фактів. Вони більше апелюють до емоційного стану людину, інколи це робиться для того, щоб вивести користувача з рівноваги, а інколи просто систематично повторюються ключові слова для тих, хто сумнівається.

Безумовно, далеко не всі антиукраїнські коментарі в інтернеті - проплачені. Серед 70 млн користувачів рунету є мільйони, хто, наприклад, радий війні на Україні. Від їх постів і коментарів пахне реальним хворобою, збитковістю, озлобленістю.

УДК 004.056.53:656.078

Лахно В.А.
доктор технічних наук, доцент
ПВНЗ «Європейський університет»

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТРАНСПОРТУ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Транспорт є найважливішою та найпотужнішою галуззю будь-якої країни світу. Інформаційно-комунікаційне середовище транспортної галузі (ІКСТГ), орієнтоване на взаємодію з іншими секторами економіки для скорочення затримок при транспортуванні вантажів, обробці морських та річкових суден, контейнерів, залізничних вагонів і вантажів на прикордонних переходах на основі використання даних електронних накладних, систем клієнт-банк, e-business, систем GSM-R, VSAT, взаємодії із клієнтурою й партнерами тощо.

Активне розширення ІКСТГ, особливо в сегменті мобільних, розподілених і бездротових технологій, супроводжується виникненням нових загроз для інформаційної безпеки (ІБ), про що свідчить зростання кількості інцидентів, пов’язаних із ІБ та захистом інформації, а також виявлених уразливостей у інформаційниї системах (ІС) транспортної галузі (ТГ).

Враховуючи вище зазначене, варто зупинитися на наступних існуючих передумовах захисту інформаційно-комунікаційного середовища транспортної галузі України.

1. Досі не розроблена єдина методологія створення захищеного ІКСТГ, адаптованого до умов функціонування ІС ТГ, у тому числі на етапах експлуатації та реконструкції.

2. Недостатньо повно формалізовані підходи до забезпечення схоронності інформації, способи і методи структурно-технологічного, віртуально-відновного і відновного резервування

критичних даних ІКСТГ.

3. Не в повній мірі досліджені дії порушника при реалізації складних атак у ІС ТГ для створення і оцінки якості функціонування систем захисту інформації (СЗІ).

4. Недостатньо повно формалізовані задачі та методи визначення складу комплексів СЗІ і урахування впливу засобів і методів захисту інформації на функціональні характеристики ІС ТГ.

5. Не в повній мірі в існуючих СЗІ враховується поява нових класів атак, що не дозволяє проводити їх дослідження, здійснювати вибір раціональних способів протидії і нейтралізації наслідків, аналізувати більш складні і раніше невідомі види нападів на інформацію.

Отже, актуальність досліджень, спрямованих на подальший розвиток методів захисту ІКСТГ та забезпечення ІБ галузі в умовах створення державної єдиної інтегрованої інформаційної системи (ДЄІІС) [1-3], є однією з ключових проблем захисту інформації об’єктів критичної інфраструктури держави.

Важливість зазначеної проблеми обумовлена такими обставинами.

По-перше, важливість транспортної галузі в національній безпеці та економіці України.

По-друге, необхідність гарантувати безпеку транспортного процесу та його інформаційної складової, роль якої постійно зростає.

По-третє, з інтеграцією України до євразійських транзитних коридорів, інформаційні ресурси набувають для галузі такого ж значення, як матеріальні й виробничі.

По-четверте, значна уразливість ІС ТГ, що пов’язано з появою нових методів нападів на інформацію, зокрема комп’ютерних (КНІ), значним поширенням бездротових комунікацій, систем навігації із використанням GPS, ГЛОНАСС, GALILEO, систем відеоспостереження (SC), технологій зв’язку GSM-R, VSAT, систем диспетчерського управління (SCADA, HMI), PLC на різних видах транспорту та ін.

По-п'яте, необхідністю розроблення принципів побудови захищеного ІКСТГ і методики управління інформаційно-обчислювальним процесом, на підставі комплексного застосування існуючих засобів і методів захисту та зберігання інформації в інтересах підтримки стійкої працездатності ІС ТГ.

З розвитком інформаційних технологій набула актуальності проблема ІБ ТГ, як складової державної безпеки, що пов'язано із забезпеченням схоронності й конфіденційності збереженої й опрацьованої інформації. Враховуючи різноманітність потенційних загроз, складність їх структури й функцій, а також участь людини в технологічному процесі опрацювання інформації, її цілісність, доступність і конфі-

денційність досягається шляхом створення комплексних систем захисту (КСЗІ) для транспортного сектору України.

Інформаційна безпека ТГ ніколи не виділялася в якості самостійного виду національної безпеки. Більше того, ІБ транспортної галузі (ІБ ТГ) не може існувати поза рамками національної безпеки. Як частина єдиного цілого, вона несе в собі спадковість концептуальних підходів щодо забезпечення безпеки країни на мікро- і макрорівнях, нерозривність взаємозв'язків, спільність принципів і методів. Причому ІБ на транспорті об'єктивно має свої особливості і специфіку, що відображає галузеву спрямованість і визначальне її місце, роль і значення в структурі національної безпеки [2, 3].

Література

1. Лахно В.А. Інформаційна безпека інтелектуальних транспортних систем / В.А. Лахно // Захист інформації. – 2015. – Том 17, № 4. – С. 298-305.

2. Лахно В.А. Кібербезпека комп'ютерних систем транспорту / В.А. Лахно // Електротехнічні та комп'ютерні системи. – 2016. – № 21 (97). – С. 76-80.

3. Лахно В.А. Підвищення кібербезпеки інформаційно-комунікаційних систем транспорту / В.А. Лахно // Безпека інформації. – 2016. – Том 22, № 1. –С. 44-50.

Марущак А.І.
доктор юридичних наук, професор
Національна академія Служби безпеки України

СУСПІЛЬНО НЕОБХІДНА ІНФОРМАЦІЯ І ПРИВАТНІСТЬ ОСОБИ

На сьогодні практичного значення набуває поняття суспільно необхідної інформації. Норми чинної редакції Закону України «Про інформацію» містять положення: «Інформація з обмеженим доступом (ІзОД) може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Предметом суспільного інтересу є інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо» [1, ст. 29]. До ІзОД зокрема відносимо конфіденційну інформацію про особу і та-

ємницю приватного життя особи, що загалом охоплюється поняттям приватність особи.

У мирний час норма про можливість поширення ІзОД, зважаючи на те, що вона є предметом суспільного інтересу, стосувалася переважно відомостей, які перебували у володінні органів державної влади. Посилалися на таку норму громадські організації, які бажали отримати докладну інформацію, захищену грифом обмеження доступу.

В умовах військової й інформаційної агресії проти України зазначена норма може і фактично використовується органами державної влади, насамперед правоохоронними, для поширення інформації про осіб, які мають протиправні наміри терористичного характеру. Прикладами реалізації норми щодо переважання суспільного інтересу над правом особи на приватність є транслювання перехоплених розмов осіб, які здійснюють або мають намір здійснити протиправні діяння терористичного спрямування.

Таким чином, інститут суспільно необхідної інформації набуває нових форм реалізації у сучасних умовах збройного протистояння на Сході України.

Література

1. Закон України від 13.01.2011 р. «Про внесення змін до Закону України «Про інформацію» (нова редакція) //Відомості Верховної Ради України. — 2011. — № 32. — Ст. 313.

УДК 341.824:338.47 (043.2)

Мошко М.С.
Служба безпеки України
Прозоров А.Ю.
Національна академія Служби безпеки України

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗОВНІШНІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

На сьогоднішній день, у зв’язку з нестабільною суспільно-політичною обстановкою, яка склалася в нашій країні та за її межами, з метою мінімізації загроз національної державності, особливо важливо детально аналізувати і вивчати одну з найбільш ефективних її різновидів – інформаційні агресії, а також інструменти їх протидії, зокрема стратегічні комунікації.

За результатами аналізу відкритих джерел інформації, а також державних стратегій провідних країн світу та їх політично-економічних об’єднань, у частині, що стосуються забезпечення формування зовнішньої та внутрішньої інформаційної політики, можна зробити висновок,

що протистояння в інформаційній сфері набуло геополітичних масштабів. В Україні також прийнято ряд законодавчих нормативно-правових актів, які регулюють зовнішні та внутрішні аспекти інформаційної діяльності нашої держави, в тому числі з широким використанням стратегічних комунікацій. Розглядаючи кожну концепцію з різних точок зору, в тому числі стратегічних комунікацій, можна зробити багато позитивних і негативних оцінок цих програм та зробити висновки щодо міри ефективності їх використання.

Якщо розглядати стратегічні комунікації України як внутрішній фактор стримування зовнішньої та інспірованої нею внутрішньої інформаційної агресії, то наша держава, не в повній мірі, але частково діє ефективно, в переважній більшості через підтримку міжнародних партнерів.

Якщо ж стратегічні комунікації України розглядати як зовнішній фактор впливу на інформаційні агресії, то до ефективного їх результату можна віднести значно меншу кількість показників, одним з найбільш вагомих з яких є привернення уваги світової спільноти до зовнішньої агресії (в тому числі інформаційної) в сторону України.

З метою підвищення ефективності дії стратегічних комунікацій як інструменту протидії зовнішній інформаційній агресії на українському прикладі, доцільно було б змістити деякі акценти, які застосовуються в стратегічних комунікаціях нашої держави (особливо це стосується внутрішньодержавного, а не тільки міжнародного напрямку), беручи за основу розробки видатного американського вченого в області психології Абрагама Маслоу, зокрема загальновідому «діаграму (піраміду) потреб».

На думку автора статті Мошко М.С., основним недоліком стратегічних комунікацій України по напряму протидії інформаційній агресії, який не вирішений українськими суб’єктами стратегічних комунікацій є не в повній мірі розуміння основного принципу «діаграми потреб» та як наслідок – його не врахування в зовнішніх та внутрішніх стратегічних комунікаційних процесах, а саме: практична неможливість людини у задоволенні своїх потреб вищих рівнів (матеріальні та нематеріальні цінності, без яких людина здатна прожити, проте прагне їх досягнення), не задовольнивши до цього потреб базового рівня (фізіологічні потреби, безпека, засоби для підтримки існування та мінімального накопичення матеріальних резервів). Таке нерозуміння частково призвело до реальних загроз національній державності України.

Наслідком такого неврахування також є те, що суб’єктами комунікацій провідних країн світу, які здійснюють реальний вплив на світову геополітику, Україна частіше розглядається як об’єкт, а не

суб'єкт комунікацій, і на жаль в ситуації, що склалася, суб'єкти стратегічних комунікацій України мало що можуть зробити, крім апеляції до міжнародного співтовариства щодо права на суверенітет та територіальну цілісність держави, міжнародні меморандуми та договори, які не виконуються [1], або виконуються частково [2-5] і не завжди на користь України.

Проте, варто відзначити і деякі успіхи українських суб'єктів стратегічних комунікацій, зокрема що відображає діяльність вищого керівництва нашої держави у залученні міжнародної спільноти до проблем порушення територіальної цілісності та суверенітету України. Так, українські суб'єкти стратегічних комунікацій сформували та формують і реалізовують стратегічні комунікації на міждержавному рівні, приносить хоч інколи і тимчасові та сумнівні, але і позитивні результати у вигляді фінансових допомог (у тому числі безповоротних), організації міжнародної місії ОБСЄ в зонах нестабільності, постійна підтримка на повістці дня проблем України на засіданнях міжнародних організацій (ООН, ЄС, НАТО), вищих політичних діячів провідних країн світу.

Врахування в стратегічних комунікаціях України основного принципу «діаграми потреб» покращить зазначені результати не лише тимчасовими успіхами на міжнародній арені, а й сприятиме консолідації українського суспільства на всій її території, в тому числі в зонах нестабільності, що в свою чергу в багато разів знизить ефективність інформаційних агресій проти нашої країни та зміцнить її державність.

Література

1. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї від 05.12.1994 № 998_158 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/998_158

2. Протокол за результатами консультацій тристоронньої контактної групи щодо спільних кроків, спрямованих на імплементацію мирного плану президента України Петра Порошенка та ініціатив президента Росії Володимира Путіна від 05.09.2014. URL: http://www.osce.org/ru/home/123258?download=true

3. Меморандум про виконання положень протоколу за результатами консультацій Тристоронньої контактної групи щодо спільних кроків, спрямованих на імплементацію мирного плану президента України Петра Порошенка та ініціатив президента Росії Володимира Путіна від 19.09.2014 [Електронний ресурс]. – Режим доступу : http://www.osce.org/ru/home/123807?download=true

4. Комплекс заходів по виконанню Мінських домовленостей від 12.02.2015. URL: http://www.osce.org/ru/cio/140221?download=true

5. Рамкове рішення тристоронньої контактної групи про розведення сил і засобів від 20.09.2016 [Електронний ресурс]. – Режим доступу : https://www.osce.org/ru/cio/266271?download=true.

УДК 004.056

Наконечний В.С.
доктор технічних наук,
старший науковій співробітник
Державний університет телекомунікацій
Курченко О.А.
кандидат технічних наук, доцент
Державний університет телекомунікацій
Рабчун Д.І.
Державний університет телекомунікацій

МЕТОД РЕСУРСНОЇ ОПТИМІЗАЦІЇ КОМПЛЕКСУ ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ ДИНАМІЧНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ

На сьогоднішній день широкого поширення набули Unified threat management-системи (комплекси програмних засобів захисту інформації, далі КПЗЗІ). Ефективне функціонування такого класу систем в процесі динамічного інформаційного протистояння потребує вирішення проблем адаптаційних змін у їх структурі з метою оптимізації наявних ресурсів.

Адаптаційні зміни можливостей комплексів ПЗЗІ інформаційно-телекомунікаційних мереж (ІТМ) організацій в умовах динамічного інформаційного протистояння можуть відбуватися на основі активізації та використання наявних чи затребуваних програмних ресурсів. Зважаючи на це сучасні КПЗЗІ з механізмами адаптації можна віднести до класу дискретних динамічних або логіко-динамічних систем [1].

Метою даного дослідження є постановка задачі та формалізація ресурсної оптимізації комплексу програмних засобів захисту інформації з використанням теорії адаптивного управління та логіко-динамічних систем.

Виклад основного матеріалу дослідження. Для простоти спочатку будемо вважати всі чинники параметрів що впливають і забезпечують роботу складної технічної системи (КПЗЗІ) детермінованими.

Введемо такі позначення.

$\overline{X}_1(t) = \{\overline{x}_{11}(t), \overline{x}_{12}(t), ..., \overline{x}_{2i}(t), \overline{x}_{1m1}(t)\}$ – вектор впливаючих на функціонування КПЗЗІ факторів, що визначаються параметрами об'єктів та умов зовнішнього середовища (тип атак, вид загроз та інше).

$\overline{X}2(t) = \{\overline{x}_{21}(t), \overline{x}_{22}(t), ..., \overline{x}_{2k}(t), \overline{x}_{2m2}(t)\}$ – вектор ресурсів адаптаційного

розвитку комплексу ПЗЗІ в момент часу t.

$Y(t)$ – показник якості (ефективності цільового застосування КПЗЗІ в момент часу t.

$\Phi(X_2, y)$ – оператор адаптації;

Задамо механізм адаптації КПЗЗІ в умовах динамічного інформаційного протистояння за допомогою функціонально-динамічної моделі (рис.1) [2].

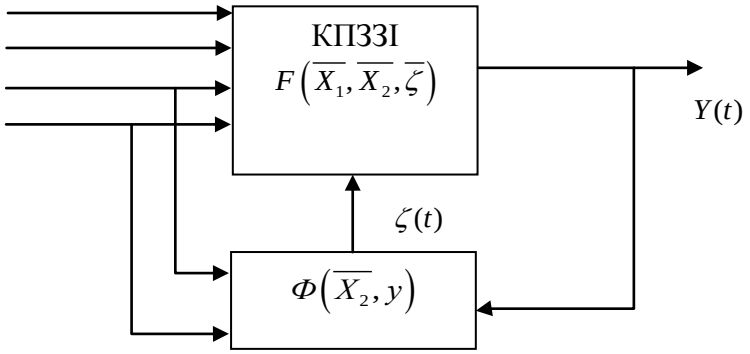

Рис.1. Функціонально-динамічна модель адаптації КПЗЗІ

Приймемо допущення, що вплив адаптаційного процесу на функціонування системи здійснюється за допомогою узагальненого показника $\zeta(t)$, зв'язаного з відносними темпами зміни традиційних показників якості та ефективності його цільового застосування (оперативність, стійкість, захищеність):

$$\zeta(t) = \sum_{k=1}^{m_2} b_{2k} \overline{\mu_k'}(t) / \overline{\mu}_k(t), \qquad (1)$$

де b_{2k} – вагові коефіцієнти, котрі визначають значимість використання k-го ресурсу в адаптаційному процесі КПЗЗІ $\sum b_{2k} = 1$ $(b_{2k} \geq 0, \forall k)$;

$$\overline{\mu}_k = Y(t)/X_{2k}(t), \qquad \overline{\mu_k'} = d\overline{\mu}_k(t)/dt.$$

Функціонально-динамічна модель, що відображає вплив адаптації на ефективність цільового застосування (функціонування) КПЗЗІ з урахуванням прямих і зворотних зв'язків, може бути аналітично представлена системою таких рівнянь:

$$Y(t) = F\left(\overline{X}_1(t), \overline{X}_2(t), \zeta(t)\right), \qquad (2)$$

$$\zeta(t) = \Phi\left(\overline{X}_2(t), Y(t)\right), \qquad (3)$$

$$F\left(\overline{X}_1(t), \overline{X}_2(t), \zeta(t)\right)\Big|^{F\left(\overline{X}_1(t), \overline{X}_2(t)\right)}_{\zeta(t)=0}, \qquad (4)$$

Гранична умова (4) дає можливість розімкнути ланцюг зворотного зв'язку по адаптації системи. Розкладаючи оператор F – функцію ефективності системи, в ряд Тейлора в околі вектора $x_1(t)\big|_{t=t_1}$ і точки $\xi_1(t) = 0$ та обмежившись лише лінійним числом ряду Тейлора (зберігши високу для практичних цілей точність) отримаємо

диференціальне рівняння адаптаційного процесу системи [3]:

$$Y'(t) = \alpha_1(t)y(t) + \beta_1(t)y^2(t), \quad (5)$$

$$\alpha_1(t) = \sum_{k=1}^{m_2} b_{2k}\, x'_{2k}(t)/b_{2k}(t) - F\big(\overline{x}_1(t_1), \overline{x}_2(t_1)\big)/C_{11}(t),$$

$$\beta_1(t) = 1/C_{11}(t).$$

Рівняння (5) описує процес ресурсної оптимізації КПЗЗІ. Якщо вважати, що у відсутності резервів і механізмів адаптаційних змін в КПЗЗІ ефективність роботи системи дорівнює $F\big(X_1(t_0), X_2(t_0)\big)$, де t_0 – час початку експлуатації системи ($t > t_0$), то розбіжність між ефективністю роботи системи на момент початку її експлуатації і станом експлуатаційних характеристик КПЗЗІ, які визначаються рівнянням (5) на поточний момент часу t, є кількісною мірою тієї ресурсної оптимізації КПЗЗІ, яка виникла в системі.

Висновки. У роботі представлено постановку та формалізацію задачі оптимізації ресурсів КПЗЗІ. Наведений математичний опис дозволяє в повній мірі використовувати апарат теорії логіко-динамічних систем для побудови системи управління ресурсами комплексів програмних засобів захисту інформації.

Література

1. Рабчун Д.І. Оцінка ефективності інформаційної безпеки з урахуванням економічних показників // Сучасний захист інформації: наук.-практ. журнал, 2015. – №4. – С.91 – 96
2. Жук К.Д. Исследование структур и моделирование логико-динамических систем / К. Д. Жук, А. А. Тимченко, Т. И. Доленко; АН УССР, Ин-т кибернетики. – Киев: Наук. думка, 1975. – 199 с.
3. Ansoff H. I. Strategic Management / H. I. Ansoff; Springer, 2007, 251 p.

УДК 343.3

Панченко В.М.

кандидат технічних наук,

старший науковий співробітник

Національна академія Служби безпеки України

ПОНЯТТЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ У НАУКОВОМУ ДИСКУРСІ

Зростання ролі засобів інформаційного впливу у сучасних міждержавних та внутрішньополітичних відносинах викликало інтерес науковців до низки понять, які характеризують даний феномен. Поняття інформаційна агресія, інформаційна експансія, інформаційний тероризм, інформаційні атаки та багато інших широко вживаються сьогодні засобами масової комунікації та використовуються у нау-

ковому дискурсі. Зокрема, поняття інформаційного тероризму стало предметом багаточисельних наукових праць (М. Стрельбицький, Т. Тропіна, М. Девост, Б. Хьютон, Н. Поллард, М. Поллітт, Д. Деннінг та ін.). Зауважимо, що увага вітчизняних учених до вивчення цього явища зростала у період активізації інформаційних акцій РФ проти України (у 2006 та 2014 роках).

Разом з тим, на сьогодні продовжують точитися наукові дискусії щодо сутності поняття інформаційного тероризму та взагалі доцільності його вживання у науковому дискурсі.

Так, інформаційний тероризм як загрозу національній безпеці України досліджували Г.В. Форос, А.В. Форос [1], як один із способів інформаційної війни - Т.П. Яцик [2], як провідний інструмент сучасної політичної практики - В.Г. Пугач [3]. Низка авторів, на нашу думку помилково, ототожнює інформаційний тероризм із кібертероризмом [4], вважає кібертероризм складовою або різновидом інформаційного терроризму [5, 6]. Запропоновані окремими авторами визначення цього поняття є недостатньо обґрунтованими та повними [3, 7, 8].

Метою даного дослідження є уточнення сутності поняття інформаційного тероризму у науковому дискурсі з урахуванням сучасного стану інформатизації суспільної діяльності та технологічних процесів.

З цією метою, зважаючи на відсутність переконливих аргументів на користь будь-якого підходу щодо визначення поняття інформаційного тероризму, нами було проведено опитування серед осіб, які мають вищу освіту та постійно використовують засоби масової комунікації у своїй повсякденній діяльності, у тому числі науковці, підприємці, працівники державних органів та комерційних організацій. Під час опитування пропонувалося відповісти на одне питання: «Що таке інформаційний тероризм, з чим у Вас асоціюється це поняття?».

Узагальнення відповідей опитаних надає можливість виокремити такі основні підходи до розуміння сутності інформаційного тероризму (наведені у порядку пріоритетності залежно від кількості опитаних, які так вважають):

1. Маніпулювання суспільною свідомістю через засоби масової комунікації (ЗМІ, соціальні мережі, Інтернет-ЗМІ, листи електронною поштою) – 31 %.

Сутність такого феномену полягає у поширенні «фейкових» новин, створенні «фейкових» акаунтів з метою прийняття об’єктом впливу рішень в інтересах суб’єкта впливу. Як приклад, вплив на думку виборців США через Фейсбук, внаслідок чого Х. Клінтон програла вибори Президента [9]. Або отримання одним із провідних американських новинних видань US Today «фейкових» підписників та «лайків», внаслідок чого редакцією приймались хибні рішення [10].

2. Розповсюдження інформації з метою залякування, негативний вплив на свідомість, що призводить до насильницького спонукання до певних дій – 23 %.

Такий варіант відповіді був характерним для осіб, які мають юридичну освіту. На нашу думку, це пояснюється тим, що при формуванні поняття інформаційного тероризму вони послуговуються своїми знаннями про тероризм як про кримінально карне явище. Прикладом акцій такого типу може бути залякування через надсилання погрозливих електронних листів, трансляція убивств через соціальні мережі з метою підвищення тривожності певної особи або групи осіб з метою спонукання її/їх до певних дій.

3. Хакерські атаки на об'єкти критичної інфраструктури як терористичні акти – 23 %.

Класичним прикладом теракту такого типу є каскадне відключення електричного струму на північному сході США та в Канаді у серпні 2003 року. Причиною відключення стало порушення функціонування основних та резервних комп'ютерних систем FirstEnergy (компанії з надання комунальних послуг штату Огайо, звідки розпочалось відключення). Відповідальність за інцидент взяло на себе терористичне угруповання „Бригади Абу-Нафса", яке входить до складу мережі „Аль-Каїда". Крім цього, до цієї категорії можна віднести DDoS-атаки на сайти урядів (вихід з ладу офіційних сайтів Верховної ради України, МВС України внаслідок припинення діяльності файлообмінника «Ex.ua» у лютому 2012 року).

4. Використання інформаційних технологій терористами для зв'язку, вербування прихильників, поширення інформації про здійснені теракти тощо – 15 %.

5. Зомбування, гіпноз – 8 %.

Отже, перший підхід передбачає ототожнення поняття інформаційного тероризму із різними формами інформаційного впливу або складовими інформаційної агресії. Другий підхід, на нашу думку, характеризує явище „класичного" тероризму із застосуванням інформаційних технологій. Адже, як зазначав С. Кара-Мурза головним об'єктом тероризму є «не ті, хто став жертвою, а ті, хто залишилися живими. Його мета – не вбивство, а залякування та деморалізація живих. Жертви – інструмент, вбивство – метод» [11, с.83]. Тобто, будь-який терористичний акт спрямований на те, щоб створити подію (в інформаційному чи фізичному просторі), яка має викликати суспільний резонанс та вплинути інформацією про цю подію на свідомість, почуття і волю людей для досягнення політичних цілей. Третій підхід ототожнює інформаційний тероризм із кібертероризмом, що було доцільним на початку 21 ст., коли незначний рі-

вень інформатизації технологічних процесів на об'єктах критичної інфраструктури не дозволяв говорити про кібертероризм як про окрему визначальну форму тероризму. Четвертий підхід характеризує інформаційну діяльність терористичних організацій. П'ятий підхід описує методи нейролінгвістичного програмування. Таким чином, найбільш поширені підходи до розуміння сутності досліджуваного поняття не містять характеризуючих елементів, притаманних виключно такому явищу, як інформаційний тероризм. На сьогодні це поняття є штучним симбіозом різних феноменів – інформаційної агресії, застосування інформаційних технологій терористами, кібертероризму, інформаційної діяльності терористичних організацій, методів нейролінгвістичного програмування.

З огляду на викладене, з урахуванням сучасного стану інформатизації суспільної діяльності та технологічних процесів, на сьогодні ще зарано говорити у науковому дискурсі про інформаційний тероризм як про окремий феномен зі своїми характеризуючими ознаками. Разом з тим, зростання впливу популістських течій на суспільно-політичні процеси у демократичних країнах безумовно сприятиме поширенню використання цього поняття у публіцистичному дискурсі.

Література

1. Форос Г.В., Форос А.В. Інформаційний тероризм як загроза національній безпеці України // Правова держава. 2010. № 12. С. 256-261.

2. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т.П. Яцик // Науковий вісник Національного університету ДПС України. 2014. № 2(65). С. 55-60.

3. Пугач В.Г. Інформаційний тероризм і політика / В. Г. Пугач // Політологія. – 2015. - № 11/1 (127). – С. 6-11.

4. Грицун О.О. Питання міжнародно-правового регулювання інформаційного тероризму [Електронний ресурс] // Електронна бібліотека WEB ІРБІС. - Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Chkup_2014_4_76.pdf.

5. Протидія інформаційному тероризму та його фінансуванню в сучасних умовах : монографія / В. В. Крутов, М. П. Стрельбицький, О. А. Шевченко (за заг. ред. В. В. Крутова). - К. : Вид-во НАПрНУ; Ужгород : ТОВ «ІВА», 2014. 309 с.

6. Стрельбицький М.П. Соціальні передумови (юридичні факти) інформаційного тероризму та кіберзлочинів / М. П. Стрельбицький, С. Л. Саржан // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. - 2014. - Вип. 2. - С. 217-226.

7. Бабенко Ю. Інформаційний тероризм [Електронний ресурс] /

Юлія Бабенко // Сайт „Аррата”. - Режим доступу: http://www.aratta-ukraine.com/text_ua.php?id=149.

8. Бондар Ю. Громадська думка; Журналіст; Засоби масової інформації; Інформатика; Інформаційна безпека; Інформаційна війна; Інформаційна діяльність; Інформаційна зброя; Інформаційна мережа; Інформаційний суверенітет; Інформаційний тероризм; Інформація; Комунікація; Національний інформаційний простір; Право на інформацію; Преса; Свобода слова та ін. (24 статті) / Ю.В. Бондар // Політологічний словник [за ред. М.Ф. Головатого, О.В.Антонюка] - К.: МАУП, 2005. - 792 с.

9. "Текст года": Как Трамп стал президентом США благодаря BigData [Електронний ресурс] // Інтернет-видання „Гордон”. – Режим доступу: http://gordonua.com/publications/tekst-goda-kak-tramp-stal-prezidentom-ssha-blagodarya-big-data-162924.html.

10. Шмырова В. Силовиков привлекут к расследованию поддельных аккаунтов в Facebook [Електронний ресурс] / Валерия Шмырова // CNews безопасность. URL: http://safe.cnews.ru/news/top/2017-05-08_silovikov_privlekut_k_rassledovaniyu_poddelnyh.

11. Кара-Мурза С.Г. Манипуляция сознанием. – М.: Алгоритм, 2000. – 464 с.

УДК 316.774:351.862.4

Петров В. В.
кандидат політичних наук
Апарат РНБО України

ДО АСПЕКТІВ РОЗБУДОВИ СИСТЕМИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Ключовою складовою «гібридної війни» Російської Федерації проти України стала інформаційна агресія, яку РФ активно реалізує як на території України, так і за її межами.

Саме тому побудова ефективної системи координації дій влади з ключовими каналами комунікації, розробка і впровадження єдиної системи взаємодії усіх органів влади в інформаційній сфері, узгоджене донесення до всіх категорій населення інформації про ситуацію в Україні є актуальним завданням для нашої держави в умовах інформаційної агресії РФ. Дієвим комплексом заходів для реалізації зазначених завдань є стратегічні комунікації.

22 вересня 2015 року з метою розвитку спроможностей органів влади України у сфері стратегічних комунікацій Секретарем РНБО України О. Турчиновим та Генеральним Секретарем НАТО Є. Сто-

лтенбергом було підписано Дорожню карту Партнерства у сфері стратегічних комунікацій (далі – Партнерство).

За результатами підписання Апаратом РНБО України був підготовлений та затверджений План заходів із реалізації Дорожньої карти Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО (далі – План).

В рамках виконання зазначеного Плану протягом 2015 року було **проведено аудит** структурних підрозділів державних органів, які відповідають за публічні комунікації. Робота здійснювалася на базі 22 центральних органів виконавчої влади, зокрема щодо вивчення наявних комунікаційних можливостей органів влади, законодавства у цій сфері.

За результатами дослідження практично **всі державні органи,** залучені до реалізації заходів Партнерства, провели відповідні організаційно-штатні зміни, затвердили внутрішні плани, **переглянули внутрівідомчу нормативну** базу щодо стратегічних комунікацій.

Окрім цього результати аудиту були враховані у механізмі реалізації Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № 47/2017.

На виконання Плану **Міністерством інформаційної політики України** надано організаційне та методичне сприяння у розробці проекту Центру стратегічних комунікацій при Національному університет оборони України ім. І. Черняховського, зокрема проведено аналіз поточних навчальних програм, сформовано концепцію Центру стратегічних комунікацій, підготовлено проект навчальної програми для пілотного проекту.

За сприяння МІП запущено проект для журналістів і блогерів із пошуку й обробки інформації з використанням новітніх технологій, методик медіа-розвідки журналістських розслідувань — OSINT. Протягом 2016 року було проведено 25 тренінгів у 19 містах України, у яких взяли участь понад 1000 осіб, 30% з яких склали представники ЗМІ.

Також планом МІП на 2017 рік передбачено розробку Стратегії інформаційної присутності України на окупованих територіях. Протягом 2016 року МІП проаналізовано процес формування політики України стосовно Криму, дії Росії після анексії, становлення інституцій окупаційної влади, реалізацію інформаційної політики після окупації Кримського півострова.

В рамках розбудови сфери публічної дипломатії у грудні 2015 року **Міністерством закордонних справ України** створено новий інструмент механізму популяризації України у світі та взаємодії з

громадськістю – Управління публічної дипломатії.

МЗС України проведено низку заходів, спрямованих на популяризацію соціально важливих тем та активізацію взаємодії з міжнародними партнерами, а також поширення інформації щодо результатів розслідування катастрофи літака Малайзійських авіаліній MH17, інфографіки щодо подібності сценаріїв реалізації агресії РФ в Україні та Сирії та закликів до їх припинення.

До третьої річниці Революції гідності МЗС України спільно з міжнародними партнерами з ЄС, США, Великої Британією та Нідерландів було організовано іміджевий захід, присвячений пріоритетним завданням зовнішньої політики України, зокрема посиленню санкції проти РФ, реалізації процесу деокупації Донбасу та Криму, прискоренню реформ, підвищенню інвестиційної привабливості України та ін.

Міністерством оборони України в рамках реалізації Партнерства започатковано **нову програму Ціль партнерства С0021 «Стратегічні комунікації»**, що передбачає комплекс заходів у цій сфері до кінця 2018 року.

У Національному університет оборони України ім. І. Черняховського 0створюється відповідна навчальна база, запроваджена комплексна модель стратегічних комунікацій в МО та ЗСУ із залученням відповідних підрозділів.

Службою безпеки України на базі Національної Академії СБУ організовано проведення на постійній основі навчальних курсів з питань стратегічних комунікацій для оперативних працівників та керівників усіх ланок.

Національним інститутом стратегічних досліджень проведено ряд досліджень у сфері стратегічних комунікацій, зокрема щодо функціонального аналізу сфери стратегічних комунікацій; потенціалу прямих комунікацій влади з громадськістю; концепції стратегічних комунікацій як документу державної політики та ін.

Наразі ми перебуваємо на етапі становлення системи стратегічних комунікацій. Першочергові заходи на цьому шляху вже зроблено. Завданнями стратегічного рівня у просуванні цього процесу залишається запровадження практичного механізму ефективного використання стратегічних комунікацій у кризовий період, системи аналізу і моніторингу громадської думки, вирішення проблем інформаційної присутності України на окупованих та звільнених територіях, впровадження тематичних навчальних програм, а також створення ефективної міжвідомчої системи стратегічних комунікацій, яка передбачатиме налагодження тісної взаємодії між її учасниками.

УДК 342.951

Пучков О.О.
кандидат філософських наук, професор
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ імені Ігоря Сікорського»
Уваркіна О.В.
доктор філософських наук, професор
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ імені Ігоря Сікорського»

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Пріоритетними напрямами сучасної політики держави у сфері інформаційної безпеки є розвиток стратегічних комунікацій, які визначені у Доктрині інформаційної безпеки України як «скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави» [1].

Актуальність питання захисту національних інформаційних інтересів в умовах стрімких трансформацій світового комунікативного простору підтверджується наявністю державних нормативно-правових актів, які регулюють процеси зовнішньої і внутрішньої політики у сфері новітніх тенденцій інформаційної глобалізації. Зокрема указами Президента України затверджені: Стратегія національної безпеки України [2], Воєнна доктрина України [3], Стратегія кібербезпеки України [4], Доктрина інформаційної безпеки України [1].

Сучасне законодавство визначає основні принципи реалізації державної, воєнної та інформаційної політики, а також інноваційні підходи до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Феномен стратегічних комунікацій обґрунтували науковці В. Ліпкан і Т. Попова, які у словнику «Стратегічні комунікації» вперше у вітчизняній науці визначили понятійно-категоріальний апарат дефініції «стратегічні комунікацій» і розширили діапазон сучасних інформаційних та комунікативних стратегій [5].

На думку О.Кушнір, яка також вивчає сутність стратегічних комунікацій у сучасному українському державотворенні, категорія стратегічні комунікації – це стратегічна взаємодія й взаємовплив в інформаційному середовищі між окремими суб'єктами, що полягає у всебічному залученні можливостей кожного окремого компонента страте-

гічної комунікації у комплексі або відокремлено, та спрямовані на досягнення визначеної мети [6].

Аналіз наукових та нормативно-правових джерел показав, що стратегічні комунікації є предметом реалізації і комунікативним засобом інформаційної безпеки держави.

Основні положення пріоритетів державної політики в інформаційній сфері, які зазначені у Доктрині інформаційної безпеки, передбачають по-перше, у сфері забезпечення інформаційної безпеки: створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них, створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, недопущення використання інформаційного простору держави в деструктивних цілях; по-друге, у сфері забезпечення захисту і розвитку інформаційного простору України: удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці, стимулювання розвитку національного виробництва текстового і аудіовізуального контенту; по-третє, у сфері відкритості та прозорості держави перед громадянами: розвиток механізмів електронного урядування; сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних, проведення реформи урядових комунікацій; по-четверте, у сфері формування позитивного міжнародного іміджу України: реформування системи представлення інформації про Україну на міжнародній арені, розвиток публічної дипломатії, участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності [1].

Таким чином, головний та ключовий чинник стратегічних комунікацій – це гарантування реалізації національних інтересів у сфері інформаційної безпеки держави. Інформаційний простір сучасності постійно оновлює теорію і практику стратегічних комунікації у зв'язку зі стрімким розвитком інформаційних технологій і появою нових форм і засобів комунікаційної взаємодії між різними суб'єктами та об'єктами суспільства, а також актуалізує розробку стратегічних комунікацій у різних сферах діяльності суспільства і, особливо, у безпеко-інформаційному вимірі.

Література

1. Доктрина інформаційної безпеки України / Указ Президента України від 25 лютого 2017 року № 47/2017 [електронний ресурс] / – Режим доступу: http://zakon3.rada.gov.ua/laws/show/47/2017

2. Стратегія національної безпеки України/ Указ Президента України від 26 травня 2015 року № 287 [електронний ресурс] / – Режим доступу: http: // zakon3.rada.gov.ua/laws/show/287/2015

3. Воєнна доктрина України / Указ Президента України від 24 ве-

ресня 2015 року № 555/2015 [електронний ресурс] / – Режим доступу: http://www.president.gov.ua/documents/5552015-19443

4. Стратегія кібербезпеки України / Указ Президента України від 15 березня 2016 року № 96/2016 [електронний ресурс] / – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016

5. Попова Т.В., Ліпкан В.А. Стратегічні комунікації: [словник] / Т.В. Попова, В.А. Ліпкан / за заг. ред. В.А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2016. – 400 с.

6. Кушнір О.В. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. URL: http://goal-int.org / ponyattya-ta-sutnist-strategichnix-komunikacii-u-uchasnomu ukrainskomu derzhavotvorenni/

УДК 55.244.1:356.255.2

Рогов П.Д.
кандидат технічних наук,
Національний університет оборони України
імені Івана Черняховського

ДО ПИТАНЬ УПРАВЛІННЯ СИСТЕМОЮ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ ДЕРЖАВИ У ВОЄННІЙ СФЕРІ

В сучасних умовах розвитку світового суспільства поряд з економічними і політичними важелями впливу не менш важливими постають інформаційні. У XXI столітті традиційні конфлікти перемістилися в принципово новий простір – інформаційний, де маніпулятивні технології за допомогою так званої інформаційної зброї набувають широкого використання. Завдяки їм ведуться інформаційні війни, здійснюється вплив на цільову аудиторію і багато інших дій, що спрямовані на завдання шкоди протиборчій стороні (противнику). Тому, останнім часом великої актуальності набув інформаційний тероризм та протидії ньому [1 – 3].

Інформаційний тероризм – це особлива форма насильства, що представляє собою свідомий та цілеспрямований інформаційний вплив або загрозу застосування такого впливу на особистість, суспільство і державу всіма існуючими видами інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об’єктивної інформації, що спричиняє виникнення кризових ситуацій в державі, нагнітання страху і напруги в суспільстві.. Він ведеться різноманітними силами та засобами - від окремих інформаційних терористів до агентури іноземних спецслужб, засобів масової інформації, здійснюється в області, що охоплює політичні,

економічні, інформаційні, правові, релігійні та інші погляди (ідеї), тобто в духовній сфері.

Аналіз досвіду передових країн світу свідчить, що завдання забезпечення інформаційної безпеки держави у воєнній сфері є одним із пріоритетних напрямів та зараз вирішується системою стратегічних комунікацій [4, 5], у тому числі протидії інформаційному тероризму.

На даний час у воєнній сфері помітна недооцінка управління системою стратегічних комунікацій держави у воєнній сфері, що дає змогу структурувати проблеми, відбирати показники, оптимізувати рішення, що приймаються. Часто про управління безпекою навіть не згадують, обговорюючи забезпечення безпеки взагалі та ігноруючи той факт, що вирішити проблеми захисту цільової аудиторії, інформаційних та інформаційно-телекомунікаційних систем від інформаційного тероризму неможливо без вирішення завдань управління ними, таких як побудова моделей загрозта раннє виявлення прояв негативного тероризму, прогнозування, оцінка та аналіз ризиків і збитків (втрат), побудова моделей та профілів протидії / захисту, контроль виконання вимог та практичних заходів щодо забезпечення психологічної безпеки.

Стратегічні комунікації держави у воєнній сфері – це система використання комунікаційних дій та можливостей всіх складових воєнної сфери держави, зокрема суб’єктів сектору безпеки і оборони України, а саме, публічної дипломатії, суспільних відносин, військових суспільних відносин, інформаційних операцій та психологічних операцій, які здійснюються для реалізації інформаційної політики Уряду, Міністерства оборони України та Збройних Сил України, інших суб’єктів сектору безпеки і оборони України.

Управління системою стратегічних комунікацій держави у воєнній сфері – це організаційна та інформаційна діяльність суб’єктів військового управління, спрямована на досягнення мети стратегічних комунікацій шляхом виконання певних функцій (аналіз, прогнозування, планування, організація, мотивація, керівництво, координація, контроль, оцінка, регулювання), із застосуванням відповідних методів комунікацій та дотриманням принципів управління.

Управляти системою стратегічних комунікацій держави у воєнній сфері означає:

<u>передбачати</u> - інформаційні небезпеки у воєнній сфері (виклики, загрози, впливи); прогнозування, оцінка та аналіз ризиків і можливих збитків (втрат);

<u>організовувати</u> – створення системи протидії інформаційному тероризму та взаємодію сил реагування на нього з метою реалізації комунікативних можливостей держави у воєнній сфері; побудова

моделей загроз, раннє виявлення негативних впливів, побудова моделей та профілів захисту особового складу військ (сил);

розпоряджатися – приймати своєчасні оперативні рішення щодо проведення інформаційних та інших заходів стосовно продидії інформаційним та психологічним (кібернетичним тощо) операціям противника та захисту своїх інформаційно-телекомунікаційних систем і цільових аудиторій;

координувати – управляти процесом обміну інформацією та взаємодією органів військового управління та інших суб'єктів воєнної сфери між собою з однієї сторони, та з органами державної влади, місцевого самоврядування, об'єднаннями громадян, підприємствами, установами, організаціями незалежно від форм власності, окремими громадянами, – з іншої;

забезпечувати – проводити діяльність щодо розробки і реалізації комплексу інформаційних заходів з метою створення умов отримання та захисту в інформаційному просторі воєнної сфери необхідних інформаційних ресурсів для реалізації інформаційного забезпечення процесів управління відповідно до функцій і завдань, визначених законодавством у сфері оборони;

контролювати – забезпечувати контроль виконання та ефективність заходів, результати діяльності сил, систем і засобів забезпечення безпеки та протидії негативним інформаційним (інформаційно-психологічним) впливам.

Література

1. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold // NATO Library at:TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000, P. 97-122.

2. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): друга міжнародна наук.-практ. конф. (25-28 травня 2009 р.). – К.: НАУ, 2009. – С. 230-232.

3. Герасименко К.С. Сучасні ознаки загроз «інформаційного тероризму» // Форум права. 2009. № 3. С. 162–166. URL: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09gkczit.pdf4

4. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп. / за заг. ред. А. Баровської. – К. : НІСД, 2016. – 109 с.

5. Березенко В.В. Стратегічне управління комунікаціями як головний напрям *PR*-діяльності / В.В. Березенко // Держава та регіони. Серія: Гуманіт. науки. – 2012. – № 1. – С. 83–87.

УДК 341.45+343.326

Рогов П.Д.
кандидат технічних наук
Національний університет оборони України
імені Івана Черняховського
Ткаченко В.А.
кандидат військових наук
Національний університет оборони України
імені Івана Черняховського

ЩОДО ПИТАНЬ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ)

Події останніх років в цілому у світі та зокрема в Україні свідчать про те, що одне з важливих місць в системі морально-психологічного забезпечення (МПЗ) належить протидії негативному інформаційно-психологічному впливу (ІПсВ) на особовий склад військ (сил) і місцеве населення [1 - 4].

В системі протидії негативному інформаційно-психологічному впливу (інформаційному тероризму, який здійснюється за допомогою інформаційної збої) та забезпеченні належного морально-психологічного стану важливе місце належить захисту особового складу військ (сил) від негативного ІПсВ, який є комплексом організаційних та інформаційних дій, що проводяться в мирний і воєнний час державним та військовим керівництвом країни, командуванням, штабами, іншими органами військового управління з залученням посадових осіб, які виконують завдання щодо виявлення, запобігання, нейтралізацію, блокування та усунення наслідків негативного ІПсВ.

Основні шляхи і напрями реалізації протидії негативному ІПсВ на різні цільові аудиторії мають бути науково обґрунтовано, прийнято і реалізовано в Концепції морально-психологічного забезпечення діяльності Збройних Сил України, інших військових формувань (Концепція), що має бути розроблена. Питання Концепції МПЗ є не тільки системою офіційно прийнятих поглядів щодо інформаційних та інших питань безпеки і оборони України. Вона насамперед має бути керівництвом до активних дій. На основі положень зазначеної Концепції повинні здійснюватися широке коло теоретичних, практичних і політичних заходів інформаційного та політичного характерів. Реалізація положень Концепції, будучи логічним продовженням Стратегії національної безпеки України, має бути узгоджено з політичним керівництвом держави, деталізовано в законодавчих й

інших нормативно-правових актах у вигляді цільових державних програм, планів і проектів.

Аналіз теоретико-методологічних основ негативного ІПсВ на особовий склад військ (сил) в сучасних умовах та на перспективу дають підставу зробити висновок, що система МПЗ повинна містіть дієву систему негативного ІПсВ на особовий склад військ (сил), за якого здійснюється превентивний та надійний захист громадян в інформаційній сфері, свідомості та підсвідомості ключових цільових аудиторій.

За своєю структурою захист військ (сил) від негативного ІПсВ передбачає такі кроки: прогнозування; запобігання (попередження та профілактика); зрив (нейтралізація) та ліквідація його наслідків [2, 3, 5].

Основним змістом протидії негативному ІПсВ на особовий склад військ (сил) є [1 - 5]:

роз'яснення особовому складу прийомів і техніки ведення ворожий пропаганди, психологічних акцій та впливів для вирішення бойових завдань з метою формування психологічної стійкості;

роз'яснення особовому складу суті, цілей, завдань, тематики, форм і методів проведення психологічних операцій з боку протидіючої сторони, їх спрямованості, дійсних намірів та інтересів. Ознайомлення особового складу з фактами, що свідчать про прийоми і методи, вживані з метою впливу на індивідуальну та групову свідомість;

прогнозування тематики і символіки психологічних операцій, можливих ІПсО з метою попередження і зниження їх ефективності чи нейтралізації, розвиток стратагемного та критичного мислення військовослужбовців;

постійній аналіз колективної та суспільної думки особового складу, військових підрозділів з приводу здійснюваного на них інформаційного впливу, оцінка ступеня уразливості особового складу і підрозділів від негативного ІПсВ;

системний аналіз і узагальнення морально-психологічного стану та інформаційної обстановки (соціально-політичної, національно-етнічної, криміногенної тощо) в військових колективах (підрозділах), в цілому, в районах дислокації військ (сил) та бойових дій.

Критеріями оцінки ефективності заходів протидії негативному ІПсВ на особовий склад військ (сил) є:

готовність особового складу до виконання поставлених завдань, рівень навченості та фізичної підготовки;

вірність особового складу військовому обов'язку, військовій присязі, рівень правової свідомості військовослужбовців;

моральні цінності, рівень військової дисципліни і правопорядку;

пануючі настрої та думки військовослужбовців стосовно зовнішнього і внутрішнього життя країни та Збройних Сил;

задоволеність військовослужбовців характером військової діяльності та проходженням служби у Збройних Силах;

вплив на військовослужбовців соціально-політичних, економічних, криміногенних обставин в районі дислокації;

статус військовослужбовців у місцевого населення.

Одним з пріоритетних завдань захисту особового складу військ (сил) від негативного ІПсВ є проведення превентивних інформаційних заходів, спрямованих на особовий склад військ (сил) і місцеве населення з метою недопущення їх інформаційного відчуження, деморалізації, дезінформації та морально-психологічного придушення [2, 5].

Література

1. Онищук М.І. Протидія інформаційно-психологічному впливу противника: Навч.-метод. посібник. Київ: НАОУ, 2002. 36 с.

2. Звіт про НДР "Комунікатор - Р" (заключний). К.: НУОУ, 2012. 83 с.

3. Інформаційна безпека держави у контексті протидії інформаційним війнам. Навчальний посібник / За ред. В.Б. Толубка / К.: НАОУ. 2004. 179 с.

4. Богуш В.М. Основи інформаційної безпеки держави: Вступ до спеціальності / В. Богуш, О. Юдін. Харків: Консум, 2004. 439 с.

5. Рогов П.Д. Війна за мізки. / Рогов П.Д. Присяжнюк М.М. - Оборонний вісник, № 6, 2016. - С.20 - 25.

УДК: 355.359; 327.56

Рудніцький І.А.
кандидат технічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського
Хміль В.В.
Національний університет оборони України
імені Івана Черняховського

РОЗВИТОК СПРОМОЖНОСТЕЙ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА ЗБРОЙНИХ СИЛ УКРАЇНИ У СФЕРІ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Загрози національній безпеці в інформаційній сфері України нейтралізуються застосуванням стратегічних комунікацій [1, п. 2]. В Збройних Силах України (ЗС України) створена система стратегічних комунікацій Міністерства оборони України (Міноборони) та ЗС

України, одним із основних суб'єктів якої є цивільно-військове співробітництво (ЦВС) ЗС України за визначеним напрямом [2, п. 10]. Стратегічні комунікації в районі дислокації або зоні розгортання військових частин ЗС України спрямовані на захист національних інтересів, підрив і делегітимізацію противника та підтримку репутації ЗС України з боку різних цільових груп цивільного оточення. Виконання цих завдань вимагає розвитку спроможностей структур ЦВС ЗС України.

Тому дослідження набуття спроможностей організаційними структурами ЦВС ЗС України у сфері стратегічних комунікацій є актуальним завданням.

Розвиток спроможностей суб'єктів стратегічних комунікацій в секторі безпеки і оборони України є предметом багатьох наукових розвідок, зокрема, у роботах вітчизняних авторів В. Ліпкана, Г. Почепцова, А. Баровської, Т. Сівак, О. Кушнір, В. Петрова, де досліджується розбудова спроможностей органів державної влади та громадських організацій, у тому числі і у контексті розвитку відносин з НАТО. Водночас поза їх увагою залишився розгляд становлення спроможностей однієї із складових системи стратегічних комунікацій – ЦВС ЗС України.

Мета дослідження полягає у визначенні напрямів розвитку спроможностей структурних підрозділів ЦВС ЗС України у сфері реалізації стратегічних комунікацій.

Розбудова спроможностей складових стратегічних комунікацій ЗС України знаходиться на начальному етапі. Розпочався процес інституалізації структур та формування концептуально-доктринальних засад стратегічних комунікацій [3, 4, 5]. На ЦВС ЗС України покладено виконання таких заходів у сфері стратегічних комунікацій з урахуванням досвіду його діяльності в антитерористичній операції (АТО) та в міжнародних операціях з підтримання миру і безпеки (МОПМБ):

формування позитивного іміджу ЗС України в зоні відповідальності військового формування (контингенту) (розповсюдження друкованих видань проукраїнської спрямованості серед місцевого населення групами ЦВС;

відновлення радіомовлення у районі проведення АТО;

реалізація гуманітарних та соціальних проектів; робота із засобами масової інформації; проведення патріотичної роботи з молоддю; надання допомоги цивільному населенню);

нейтралізація негативних інформаційно-психологічних впливів;

формування позитивного міжнародного іміджу України та високої репутації ЗС України під час участі в МОПМБ та заходах між-

народного співробітництва.

Розвиток спроможностей ЦВС ЗС України у сфері реалізації стратегічних комунікацій проводиться за такими напрямами:

удосконалення нормативно-правового забезпечення діяльності ЦВС ЗС України в реалізації стратегічних комунікацій;

комплексного використання як комунікаційно-контентних засобів (телевізійні канали, інтернет-сайти, соцмережі та цифрові засоби масової інформації), так і засобів прямої взаємодії військових ЗС України з місцевим населенням та органами влади;

набуття умінь проведення заходів стратегічних комунікацій в умовах домінування держави-агресора на тимчасово-окупованих територіях та недостатньо розвиненої національної інформаційної інфраструктури;

ресурсне забезпечення – забезпечення необхідною інформаційно-комунікаційною інфраструктурою, засобами переміщення відповідно до оперативного середовища, обладнанням та запасами матеріально-технічних засобів, а також фінансове забезпечення для виконання заходів;

забезпечення організації взаємодії та координації з іншими складовими стратегічних комунікацій ЗС України;

оптимізації організаційних структур ЦВС в залежності від вимог оперативного середовища;

постійного удосконалення науково-методичного забезпечення процесів управління формування та реалізації заходів стратегічних комунікацій;

включення до стандарту підготовки персоналу ЦВС набуття уміння у сфері формування та реалізації стратегічних комунікацій ЗС України;

вивчення та впровадження передового досвіду діяльності структур ЦВС ЗС України в АТО і МОПМБ та структур ЦВС (CIMIC) НАТО та країн-партнерів;

участі в Процесі планування та оцінки сил щодо досягнення цілі партнерства G1105 “Спроможності цивільно-військового співробітництва” [6].

Отже, запропонований комплекс заходів за зазначеними напрямами дозволить сформувати спроможності ЦВС ЗС України у сфері стратегічних комунікацій.

Перспективу подальших досліджень вбачаємо в оцінці ефективності ЦВС ЗС України у доступних заходах реалізації стратегії комунікацій Міноборони та Збройних Сил України.

Література

1. Указ Президента України від 25 лютого 2017 року № 47/2017

“Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”. Урядовий кур'єр від 28.02.2017 — № 38.

2. Наказ Генерального штабу Збройних Сил України від 07 жовтня 2016 року № 374 “Про затвердження Інструкції з реалізації стратегічних комунікацій у Збройних Силах України”.

3. Наказ Генерального штабу Збройних Сил України від 08.11.2016 № 411 “Концепція розвитку цивільно-військового співробітництва Збройних Сил України”.

4. Стратегія комунікацій Міністерства оборони України та Збройних Сил України, затверджена Міністром оборони України від 18 липня 2016 року № 149/1/1.

5. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО від 22 вересня 2015 року. URL: http://mfa.gov.ua/mediafiles/sites/nato/files/Roadmap_Ukr.pdf.

6. Перелік основних заходів досягнення цілей партнерства в Міністерстві оборони України та Збройних Силах України на 2016-2020 роки. Затверджено Міністром оборони України від 16.06.2016 № 11676/з.

Селіна М.Б.

Національна академія Служби безпеки України

ЕФЕКТИВНІСТЬ ПРОВЕДЕННЯ ВЛАСНИХ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ У КОНТЕКСТІ ДОСВІДУ КОЗАЦТВА

З моменту створення Служби безпеки України одне з головних питань полягало у формуванні працездатного колективу, спроможного ефективно працювати, розв‘язувати складні завдання, гнучко й адекватно реагувати на зміни обстановки. Надважливого значення набувало патріотичне виховання працівників молодої спецслужби, яке залишається актуальним і сьогодні. Так, в умовах складної суспільно-політичної ситуації в нашій державі, а також агресії Російської Федерації проти України, одним із ключових сегментів якої є проведення спеціальних інформаційних операцій (СІО), спрямованих на дестабілізацію ситуації на всій території нашої країни, знищення української національної самоідентифікації, поширення та утвердження серед населення України інформації про відсутність історичного минулого української держави як такої та її приналежності до російської історичної спадщини, здатність співробітника спецслужби

оволодіти механізмом пізнання та аналізу складних історичних явищ стає невід‘ємним елементом його морально-психологічної стійкості. У цьому контексті, з метою виховання патріотизму та моральної стійкості у співробітників СБ України доцільно вивчати один з найвидатніших періодів нашої історії, під час якого відбувся розквіт розвідувальної та контррозвідувальної діяльності, у т.ч. з широким використанням специфічних тактичних прийомів, що мали національний характер та вживались як елемент військово-психологічного супроводу бойових дій, а саме Козацьку добу.

Так, сучасні військові спеціалісти вважають чи не найефективнішою зброєю в боротьбі з ворогом СІО. Т.Чухліб наголошує, що на території Центральної та Східної Європи проведення прототипів СІО започаткував гетьман Богдан Хмельницький, який використовував їх у багатьох битвах, особливо на початку Визвольної війни у 1648 році. Зокрема, шляхом поширення дезінформації він намагався посіяти панічні настрої серед ворожого війська, невпевненість у власних силах. Узимку 1651 року була проведена одна з найбільш грандіозних у ті часи в Європі розвідувально-психологічна операція. До Корони Польської були направлені близько двох тисяч українських шпигунів, які, зокрема, поширювали чутки про величезну бойову могутність армії Богдана Хмельницького, тим самим викликаючи панічні настрої серед місцевого населення [5].

Проте невірно стверджувати, що до цього козаки не використовували методи психологічного впливу. Так, Северин Наливайко, Петро Конашевич-Сагайдачний, Михайло Дорошенко, Іван Сулима, Дмитро Байда-Вишнивецький та ін. започаткували традиції козацького військового мистецтва т.зв. «військові хитрощі», елементи військово-психологічного супроводження бойових дій. Так, за часів козацтва сягнули високого рівня розвиток та організація польової сторожово-розвідувальної служби, зовнішньої розвідки, контррозвідувальних заходів. При цьому, завдяки всенародній підтримці стала особливо ефективною діяльність козацької розвідки, що, у свою чергу, стало можливим завдяки вміло проведеній пропаганді та формуванню позитивної думки про запорозьке військо серед місцевого населення. Дезінформація ворога вже у ті часи була одним із важливих методів зовнішньої розвідки козаків, за допомогою якого козаки поширювали панічні настрої у супротивника, організовували повстання, а також здобували розвідінформацію [2, с. 21]. Дезінформація проводилася головним чином двома шляхами: через агентів, які вдавали з себе перебіжчиків з козацького табору, та через мужніх патріотів, які потрапляли до ворога і, приймаючи мученицьку смерть на тортурах, повідомляли ворогу «необхідну» інформацію. Зокрема це спостерігалось під час

боїв під Корсунем, Старокостянтиновом, Пилявцями, Берестечкової кампанії тощо [3, с. 27-39].

За часів козацтва військова майстерність досягла значного рівня, а деякі дослідники періоду козацтва зазначають, що саме козаки вперше започаткували на теренах Центральної та Східної Європи проведення прототипів СІО. Водночас, значні військові успіхи козаків були можливі завдяки високому морально-психологічному рівню козаків. До лав козаків потрапляли найбільш патріотичні представники українського народу, спроможні на самопожертву заради рідної землі.

Зважаючи на викладене, вивчення історії козацтва набуває особливої актуальності в умовах російської агресії проти України. Так, однією із запорук успішного формування професійних та особистих рис захисника держави є пізнання ним історичного минулого України, зокрема історії українського козацтва, яка є невіддільною й органічною складовою історії України, а також всесвітньоісторичного процесу. Важливою особливістю опанування співробітниками СБУ історичними знаннями є повага до минулого, критичне розуміння позитивного та негативного досвіду. А отже, здатність співробітника СБ України до аналізу складних історичних явищ та їх розуміння, не лише стає невід'ємним елементом його професійної культури та морально-психологічної стійкості, а й дає змогу ефективно протистояти посяганням на державну безпеку нашої країни.

Література

1. Богдан Хмельницький: від державної ідеї до Української козацької держави : методичні рекомендації до 420-ї річниці від дня народження Богдана Хмельницького / уклад. Максименко М. Г. - Полтава, 2015. - 16 с. [Електронний ресурс] / М. Г. Максименко. – 2015. URL: http://libgonchar.org/images/stories/DocS/2015/Hmelnuzkuy.pdf.

2.З історії розвідки і контррозвідки в Україні за часів Київської Русі і Козацької Доби : науково-практичний посібник /[А.І.Ярмоленко, В.К.Тополенко]. – К.: Інститут підготовки кадрів Служби безпеки України, 1993. – 25с.

3.Історія розвідки та контррозвідки в Україні : курс лекцій : у ІІ ч. / [Д.В.Вєдєнєєв, В.Г.Пилипчук, В.С.Сідак, В.К.Тополенко]. – К.: Наук.-вид.відділ НА СБ України, 2010. – Ч.І. – 214с.

4.Історія інформаційно-психологічного протиборства : підруч. /[Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк, Є.ДСкулиш]; за заг.ред.д.ю..н., проф.., засл. Юриста України Є.Д.Скулиша. – К.:Наук.-вид.відділ НА СБ України, 2012. – 209с.

5. Чухліб Т. В. Отец психологических войн [Електронний ресурс] / Т. В. Чухліб // День. – 2004. URL: https://day.kyiv.ua/ru/article/ukraina-incognita/otec-psihologicheskih-voyn.

Сиволапенко Т.Л.
Державне агентство з питань
електронного урядування України

ІНФОРМАЦІЙНА ЗБРОЯ В СУЧАСНИХ ІНФОРМАЦІЙНИХ ПРОТИБОРСТВАХ

Розвиток світової спільноти наочно демонструє, що останнім часом критично важливим державним ресурсом, що надає все більший вплив на національну безпеку, стає інформація, що циркулює в автоматизованих системах управління і зв'язку. Дані системи є невід'ємним компонентом структури управління державою, економікою, фінансами і обороною. Прискорений розвиток комп'ютерних технологій не тільки в значній мірі сприяло підвищенню ефективності їх функціонування, а й відкрило додаткові можливості для навмисного деструктивного впливу на них протилежної сторони.

При демократії, суспільство контролює вибір засобів, які використовують люди в процесі своєї діяльності, в тому числі і засобів збройної боротьби. Тільки в тому випадку, якщо наміри людей мають під собою як моральну основу, так і технологічну, цей вибір буде розумний. Але якщо про моральність не замислюються, то виникає ефект доміно: втрачається підтримка з боку суспільства, не використовуються передові досягнення технології, і в результаті збройні сили залишаються без засобів збройної боротьби.

Зараз вже є засоби, що дозволяють створити інформаційну зброю, і так як інформаційна зброя є такою потужною зброєю, як війська, так і цивільне населення повинні бути захищені від нього. До впливу інформаційної зброї уразливі всі.

Уряд має прийняти рішення - розробляти засоби інформаційної зброї або переслідувати в судовому порядку тих, хто розробляє такі засоби. Це рішення повинно бути прийнято на підставі ретельного аналізу всіх деталей і з розумінням моральних і етичних ризиків інформаційної зброї. Крім врахування всіх ризиків при прийнятті рішення про створення інформаційної зброї, люди повинні розуміти принципи дії цих коштів і теорію їх використання до того як вони почнуть застосовуватися.

Під інформацією розумітимемо вміст або значення повідомлення. Метою засобів збройної боротьби є вплив на інформаційні системи ворога. У широкому сенсі інформаційні системи включають в себе всі засоби, за допомогою яких противник отримує знання або висуває гіпотези. Для військових інформаційні системи являють собою засоби, за допомогою яких противник отримує інформацію про

стан бойових дій і керує військами. У сукупності інформаційні системи є об'єднанням знань, гіпотез, процесів прийняття рішення та систем противника. Результатом інформаційних атак на будь-якому рівні є дати противнику інформацію, що змушує його припинити збройні дії.

З якої причини противник може припинити бойові дії? Існує ряд можливих причин: неможливість управляти збройними силами, деморалізація, отримання інформації (істинної чи імовірною) про те, що війська знищені, або про те, що більш вигідно припинити війну, ніж продовжувати воювати. Ці «повідомлення» про припинення війни можуть відрізнятися як по змісту, так і за змістом, як наприклад: «Ваша контратака провалилася» або «Ваші власні люди не підтримують вас у війні, в якій вбивають дітей». Хоча методи передачі повідомлень, що змушують припинити війну, можуть змінюватися, сенс повідомлень залишається незмінним - припинити війну.

У силу розвитку соціальних інститутів інформаційні системи ускладнювалися, а процеси прийняття рішення ставали все більш складними. Фінансово-промислові організації, що виникли на базі домінантних політичних структур збільшували складність систем у міру збільшення своєї діяльності. З'явилися мережі інформаційних взаємозв'язків між працівниками розумової праці - найсучасніша форма інституційної структури, і їх кількість, а також доступність засобів інформаційної технології різко збільшилася.

У міру розвитку інформаційної технології інформаційні системи привели до появи знання, або ноу-хау, яке дозволяло робити інші інституціональні форми більш ефективними.

В інформаційній війні метою є гармонізація дій на оперативному рівні з діями на стратегічному рівні, щоб об'єднані, вони змушували супротивника приймати рішення, які б приводили б до дії, які допомагали досягати нам наших цілей і заважали б супротивнику домагатися виконання своїх.

На стратегічному рівні лідерів, продумує план ведення інформаційної кампанії, потрібно знати відповіді як мінімум на три питання: по-перше, як і зв'язок інформаційної кампанії з глобальними цілями кампанії? по-друге, що ми хочемо, щоб ворожі лідери знали або передбачали по завершенню кампанії? Тобто, який бажаний епістеміологічний стан і отже критерій успіху операції? по-третє, які кошти ведення інформаційної війни є кращими для досягнення встановленого критерію успіху? Тобто як будуть пов'язані кошти з результатом?

На операційному рівні нашим лідерам також потрібно мати відповіді на ряд питань. Чи буде заборонено атакувати деякі цілі і за-

стосовувати деякі засоби в інформаційних атаках?

Досяжний чи бажаний епістеміологічний стан взагалі і всюди, або тільки існують проміжні стани, досяжні в специфічних географічних районах, у специфічній послідовності, або в специфічних секторах інформаційних бойових дій. Також, слід відповісти на питання про управління і сигналах. Крім того, лідерам на оперативному рівні потрібно знати, коли будуть завершені атаки і засоби, за допомогою яких буде переданий сигнал про припинення атаки. Це важливі питання, так як інформаційна зброя може викликати непрямий руйнування систем знань і припущень у атакуючих. У гіршому випадку відповідь противника може включати контратаки проти дружніх інформаційних систем, що за великим рахунком не відрізняється від побічних руйнувань «вогневої підтримки».

Чим більше залежить противник від інформаційних систем при ухваленні рішення, тим більше він уразливий до ворожого маніпулювання цими системами. Програмні віруси впливають тільки на ті системи, в яких є програми. Засоби радіоелектронної боротьби можуть бути застосовані тільки проти збройних сил, що використовують радіо і електроніку.

Так як інформаційна війна може вестися проти всієї епістеміології ворога в цілому, то і примітивні суспільства уразливі в інформаційній війні. По-друге, індустріальні суспільства можуть придбати більшу частину їх телекомунікаційної структури у більш розвинених постіндустріальних суспільств. У державах або групах з високим рівнем розвитку техніки набір цілей атак на стратегічному рівні дуже багатий: телекомунікації та телефонія, космічні супутники, автоматизовані засоби ведення фінансової, банківської та комерційної діяльності; енергосистеми; культурні системи; і весь набір обладнання та програм, на підставі яких ворог отримує знання.

Стратегічні інформаційні системи в високотехнологічних державах часто дублюються на оперативному рівні. Всі вони уразливі для атаки. Інформаційна війна не повинна відкладатися до тих пір, поки ворожість не стане відкритою. Лідери противника не захочуть воювати, якщо вони припускають одне з наступного: що насильство - це погано, або що у них не буде союзників, або що на них будуть накладені санкції, що перешкоджають продовженню війни, або що їх індустріальна база не зможе забезпечити перемогу в тривалій війні, або що їхні збройні сили не готові.

Чим вище технологічні можливості держави і чим більше число його взаємодій з іншими групами (включаючи внутрішні групи) або державами, тим більше держава вразливе в інформаційній війні. Ця вразливість буде зростати в міру збільшення розмірів мереж або чи-

сла і обсягу транзакцій.

Демократії не є менш вразливими, ніж тоталітарні режими, хоча демократичні соціальні системи, такі як групи, можуть бути трохи більш стійкими до виведення з ладу. Але апарат управління її економікою вразливий. Банки, фінанси, торгівля, подорожі і управління повітряним рухом стають все більш залежними від інформаційної технології. У міру того, як зростає залежність від інформаційних систем, збройні конфлікти, що організовуються терористами, релігійними екстремістами, ворожими бізнесменами, проти інформаційних систем становитимуть реальну загрозу. Інформаційна зброя в їх руках може бути направлено на енергосистеми або засоби зв'язку, які обслуговують кінцеву мету. Одночасні атаки на різні вузли можуть мати стратегічний ефект. Тобто вони можуть впливати на знання і волю лідерів.

Висновки. Наступ інформаційної ери призвів до того, що інформаційний вплив, що існував споконвіку у взаєминах між людьми, в наші дні все більш очевидно набуває характеру військових дій. В даний час накопичений значний досвід наукових досліджень у галузі інформаційного протиборства та інформаційно-психологічних війн. Який би зміст у поняття «інформаційна війна» не вкладався, воно народилося в середовищі військових і позначає, перш за все, жорстку, рішучу і небезпечну діяльність, яку можна порівняти з реальними бойовими діями. Інформація дійсно стала реальною зброєю. Вона йде вже в третьому поколінні.

В епоху інформаційного суспільства ключове значення набули засоби масової інформації, Інтернет-канали і контроль над інформаційними потоками. З представленого матеріалу очевидно, що Україна в цьому відношенні значно відстає від провідних країн світу. Для формування нового багатополярного світового порядку в Україні необхідно робити рішучі дії для прориву в інформаційній сфері і боротьбі із інформаційними війнами у практичному аспекті.

Література

1. Почепцов Г.Г. Інформаційні війни. М.: ВЦ Гарант, 2008, 453 с.
2. Проект Закону України про основні засади забезпечення кібербезпеки України (реєстр. № 2126а)/ URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9.
3. Расторгуєв С.П. Інформаційна війна. М.: Наука, 2008, 235 с.
4. Указ Президента України від 15 березня 2016 р. № 96/2016. URL: http://zakon0.rada.gov.ua/laws/show/96/2016.

Скачек Л.М.
кандидат технічних наук, доцент
Національна академія внутрішніх справ

БОРОТЬБА З КОМП'ЮТЕРНИМИ ЗЛОЧИНАМИ

В Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій у різні сфери діяльності людини, зокрема у діяльність правоохоронних органів, яку вже важко уявити собі без використання сучасних засобів обчислювальної техніки. Це призводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем, розширюються можливості несанкціонованих дій з інформацією і, поряд з цим, можливістю негласного знімання інформації.

Ринкові відносини з їх невід'ємною частиною обов'язково вимагають протидії зовнішнім і внутрішнім впливам. Об'єкти захисту в більшому чи меншому ступені, залежно від цілей зловмисника і від конкретних умов, можуть піддаватися різним нападам чи загрозам знаходитися в ситуації, в якій вони за об'єктивними причинами піддаються небезпеці. Забезпечення безпечної діяльності необхідно для будь-яких підприємств, установ, організацій починаючи від державних і закінчуючи самими малими приватними підприємствами.

Персонал використовує інформацію і відповідає на зовнішні і внутрішні запити по електронних каналах. Це дає можливість зловмисникам підібратися до співробітників, використовуючи відносну анонімність Internet і локальних мереж. Ми часто чуємо про атаки та напади на електронну пошту, спливаючих додатках і атаках, що використовують системи миттєвої передачі повідомлень, «троянські» віруси або шкідливі програми, які компрометують комп'ютерні ресурси. Від більшості подібних нападів можна вберегтися за допомогою антивірусного захисту. Тому необхідно навчити персонал, як найкраще ідентифікувати напади, і навчити як уникнути їх.

При вивченні кожної конкретної хакерської атаки враховуються кілька факторів. В першу чергу - вік хакера, його освіту, соціокультурне середовище регіону проживання і рівень його кваліфікації. Щоб визначити рівень кваліфікації, фахівці вивчають інструментарій хакера і з'ясовують, чи є там унікальні програми, написані особисто хакером, або ж він використовує стандартний софт, чужі розробки. Рівень технічної підготовки хакера оцінюється за спеціальною шкалою і вводиться в його особистий профайл. Це дозволяє певною мірою прогнозувати подальші дії зловмисника.

Тому, можна сказати, що не існує єдиного визначення поняття

«хакер», сутність цього поняття, дозволяє описати образ хакера, який поширений у масовій свідомості людей, де хакер – людина найчастіше чоловік від 15 до 45 років, яка має технологічну або математичну освіту,з високим рівнем IQ, яка професійно володіє комп'ютером, уміє працювати з різними програмами та Інтернетом, створювати власні програми, може «проникнути» до чужого комп'ютера, вкрасти цінну інформацію або навіть пошкодити комп'ютерну систему. При цьому хакер - людина зазвичай відчужена від реального світу і заглиблена у віртуальний світ, відповідальна, найчастіше скромна, наполеглива, самовпевнена, з завищеною самооцінкою, а також має певні труднощі у контактах з іншими людьми.

Література

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки / В.Л.Бурячок. – К.: Вид. НАУ, 2013 – 432 с.
2. Грайворонский М.В. Безпека інформаційно-комунікаційних систем / М.В.Грайворонский, О.М.Новіков – К.: Вид. група BHV, 2009. – 608 с.
3. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В.Ленков, Д.П.Перегудов, В.А.Хорошко. К.: Арий, 2008.

УДК 355.40

Сніцаренко П.М.

доктор технічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського

ТЕРМІНОЛОГІЧНИЙ НІГІЛІЗМ В ІНФОРМАЦІЙНІЙ СФЕРІ ТА ЙОГО НАСЛІДКИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Статтею 17 Конституції України визначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу. Незважаючи на таку сувору конституційну норму та, відповідно, потребу невідкладного втілення її в життя, лише більш ніж через десять років законодавство України нарешті визначило сутність інформаційної безпеки в такій редакції: "Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподіленні інформаційні системи, в яких обробляється конфіденційна інформація".

На думку автора, таке визначення інформаційної безпеки та висвітлення сутності її забезпечення в Україні є достатньо чітким та системно збалансованим, хоч ця норма міститься у "тілі" Закону "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", явно другорядного по відношенню до феномена інформаційної безпеки держави. В законодавчих актах України, які стосуються інформаційної сфери та набрали чинності після цього закону, інше тлумачення інформаційної безпеки або його заперечення чи уточнення відсутні. Це означає, що як теоретичні напрацювання, так і практичні заходи щодо забезпечення інформаційної безпеки України повинні реалізовуватися в межах, які окреслені вищенаведеним визначенням. На жаль так не відбувається.

Очевидною причиною цього стану є вільне ставлення до поняття "інформація", єдиного, як стверджує фундаментальна наука [1], для сфер біологічної, технічної та соціальної. Особливо негативним фактом є різне визначення цього поняття у законах України, що регламентують інформаційну сферу. Наприклад, порівняймо: "*інформація* – будь-які відомості та / або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді" (Закон України "Про інформацію") та "*інформація* – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб" (Закон України "Про телекомунікації"). Крім різного трактування, обидва наведені визначення мають принципові недоліки, які полягають у тому, що в першому інформація ототожнюється з даними, а в другому – не показано її відмінності

від даних (дані та інформація поняття нетотожні!).

Практичним наслідком зазначеного є те, що у різних галузях забезпечення інформаційної безпеки України розуміння сутності інформації, як правило, неоднакове. Це призвело до труднощів системного характеру, пов'язаних з неузгодженістю на загальнодержавному рівні позицій різних зацікавлених сторін, що не дозволило вибудувати в Україні єдину та чітку інформаційну політику та механізми її реалізації, зокрема з питань забезпечення інформаційної безпеки держави.

У доповіді наведено приклади недосконалості нормативно-правової бази та державних механізмів забезпечення інформаційної безпеки України, що спричинене неналежним ставленням до термінології в інформаційній сфері, а також надано пропозиції щодо покращення існуючого стану.

Література

1. Словарь по кибернетике: Св. 2000 ст. / Под ред. В.С. Михалевича. – 2-е изд. – К.: Гл. ред. УСЭ им. М.П. Бажана, 1989. – 751 с.

УДК 355.40: 356.35

Сніцаренко П.М.
доктор технічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського
Саричев Ю.О.
кандидат технічних наук,
старший науковий співробітник
Національний університет оборони України
імені Івана Черняховського
Хоменко Л.В.
Національний університет оборони України
імені Івана Черняховського

МЕТОДОЛОГІЧНИЙ ПІДХІД ДО СТВОРЕННЯ ПІДСИСТЕМИ ВИЯВЛЕННЯ ТА ОЦІНКИ НЕГАТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ НА ОСОБОВИЙ СКЛАД ВІЙСЬК (СИЛ) ЯК СКЛАДОВОЇ СИСТЕМИ ПРОТИДІЇ ТАКОМУ ВПЛИВУ

Забезпечення інформаційної безпеки держави є фундаментальним напрямом реалізації державної інформаційної політики України, а протидія негативному інформаційному впливу – невід'ємна складова забезпечення інформаційної безпеки, у тому числі у воєнній сфері. Протидія такому впливу, зокрема його різновиду – інформаційно-психологічному, є одним із актуальних завдань першоря-

дного значення для вирішення. Індикатором ефективності протидії негативному інформаційно-психологічному впливу, зокрема на особовий склад ЗС України, доцільно вважати рівень морально-психологічного стану військ (сил).

Для протидії виникає необхідність створення за законами кібернетики стійкої системи управління, де об'єктами управління є рівень морально-психологічного стану ЗС України та джерела негативного інформаційно-психологічного впливу. Тому запропоновано загальну кібернетичну модель такого управління (рис.1), яка може найбільш

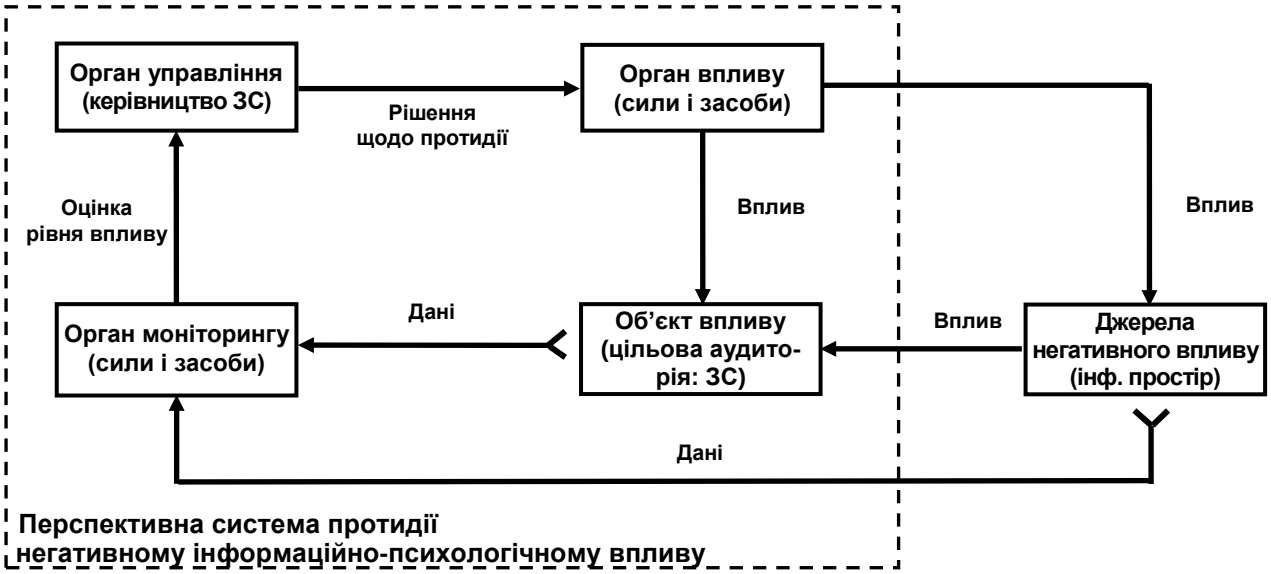

Рис.1. Кібернетична модель реалізації протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил)

повно забезпечити активну протидію негативному інформаційно-психологічному впливу на особовий склад військ (сил) з такими її обов'язковими фазами: а) виявлення впливу; б) оцінка рівня впливу; в) формування висновків із оцінки рівня впливу та рішення щодо необхідності протидії; ґ) планування заходів

протидії впливу, затвердження плану заходів протидії; д) реалізація заходів протидії впливу відповідно до плану; е) контроль дієвості реалізованих заходів протидії впливу та їх коригування.

На практиці ця модель в МО України та ЗС України частково реалізується, але лише в межах контура, обмеженого штриховою лінією. В той же час, на сьогодні оцінка рівня негативного інформаційно-психологічного впливу здійснюється за його наслідками, тобто "постфактум", без аналізу динаміки такого впливу, джерелом якого є весь інформаційний простір.

З метою підвищення ефективності реалізації зазначеної моделі в системі протидії негативному інформаційно-психологічному впливу на особовий склад ЗС України в підсистему моніторингу необхідно

запровадити механізм виявлення та оцінювання у кількісному вимірі рівня негативного інформаційно-психологічного впливу на особовий склад військ (сил) з квантуванням за ступенем його значення для морально-психологічного стану ЗС України. Це дозволить реалізувати упереджувальні компенсаційні заходи протидії з метою стабілізації морально-психологічного стану визначеної цільової аудиторії, загалом ЗС України.

Одним із підходів для реалізації такого механізму та розробки відповідної методики виявлення і оцінювання негативного інформаційного впливу може бути такий, де характеристикою (показником) дії загального деструктивного інформаційного процесу по відношенню до певної цільової аудиторії (особового складу ЗС України) вважається рівень його інтенсивності, тобто міра дії процесу в одиницю часу. Зазначене одночасно є інтегральним показником як оцінки рівня негативного впливу, так і індикатором виявлення такого впливу за величиною (значенням) рівня. Тоді динаміку ескалації інтенсивності загального деструктивного інформаційного процесу в інформаційному просторі держави за час ΔT по відношенню до особового складу військ (сил) можна умовно представити ступінчатою функцією рівнів, які слід вважати частковими показниками впливу, як це показано на рис. 2. При цьому, переходу на кожен із рівнів доцільно поставити у відповідність певний критерій за шкалою оцінок $\chi_1, \ldots, \chi_5$.

У зв'язку із цим запропоновано шість умовних якісних станів (часткових показників) загального деструктивного інформаційного процесу в інформаційному просторі держави та відповідні критерії, які можуть бути застосовані для визначення рівня його інтенсивності як міри впливу, зокрема, на особовий склад військ (сил):

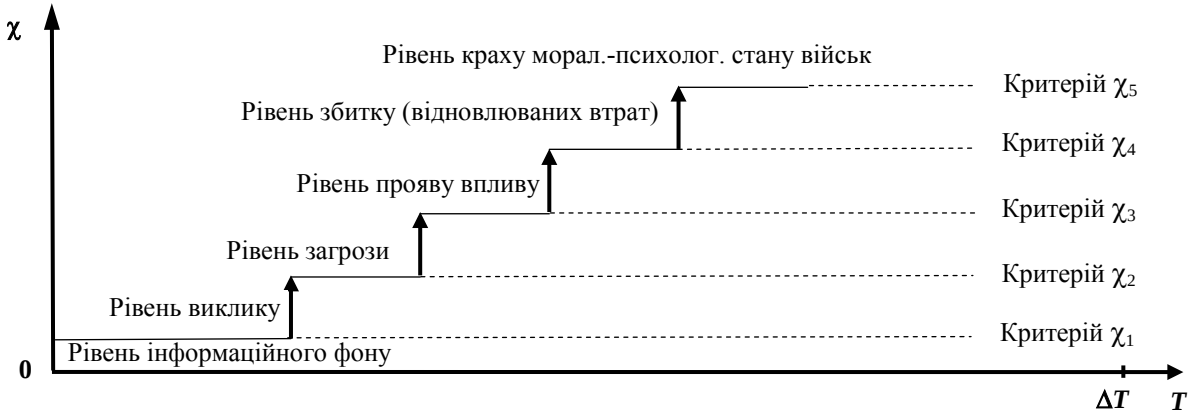

Рис. 2. Динаміка ескалації інтенсивності загального деструктивного інформаційного процесу

інформаційний фон (шум);
виклик (інформаційно-психологічний);
загроза (інформаційно-психологічна);

прояв інформаційно-психологічного впливу на особовий склад військ;

збиток (відновлювані втрати) в морально-психологічному стані військ;

крах морально-психологічного стану військ.

З використанням експертного методу на основі отриманої статистики усіх інформаційних процесів (дій, фактів) на протязі часу $\Delta T = 1$ рік отримано критерії знаходження рівня негативного інформаційно-психологічного впливу на шкалі "зваженої" інтенсивності у перерахунку їх сумарної дії.

Цей результат став основою для реалізації простої методики виявлення та оцінки інформаційно-психологічного впливу на особовий склад військ (сил). Методика діє на принципі масштабування у часі "зваженої" суми балів (відносно базового терміну $\Delta T = 1$ рік), отриманої з причини появи в інформаційному просторі держави за час $\Delta t << \Delta T$ певної кількості класифікованих інформаційних процесів (дій, фактів), тобто через набір статистики інформаційних процесів в інформаційному просторі держави та їх обробки не за період $\Delta T = 1$ рік, а за значно менший термін $\Delta t << \Delta T$, наприклад, за місяць чи тиждень.

Сєкунов С.В.
Служба безпеки України

КАТЕГОРІАЛЬНИЙ АНАЛІЗ КОНТРРОЗВІДУВАЛЬНОГО ЗАХИСТУ ДЕРЖАВНИХ ІНТЕРЕСІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів національної безпеки України. Глобалізація інформаційних процесів створює як сприятливі умови для сталого розвитку суспільства, так і реальні загрози негативних інформаційних впливів, які за відсутності дієвої системи захисту й протидії цим загрозам спроможні значно послабити або навіть зруйнувати конкуруючу державу. Зазначене актуалізує проблему регулювання суспільних інформаційних відносин, пов'язаних із формуванням національного інформаційного простору, забезпеченням інформаційної безпеки, удосконаленням правових механізмів захисту державних інтересів у цій сфері. Тому важливого значення набуває визначення понять інформаційної безпеки, державних інтересів у цій сфері, контррозвідувального захисту означених інтересів.

Незважаючи на значну кількість досліджень змісту поняття «інформаційна безпека», через його дуалістичну сутність єдиної позиції щодо правового визначення цієї дефініції до сьогодні не вироблено.

Відповідно до законодавчого визначення, інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації. Однак таке тлумачення не розкриває усіх загроз інформаційній безпеці. До того ж, на думку автора, у визначенні (тим більше нормативному) недоцільно подавати перелік загроз, адже з часом вони зникають, трансформуються, виникають нові.

Отже, автор пропонує розглядати інформаційну безпеку як захищеність життєво важливих національних інтересів від інформаційних загроз, яка забезпечується уповноваженими суб'єктами шляхом вжиття комплексу відповідних заходів. У цьому зв'язку постала потреба з'ясувати зміст життєво важливих інтересів держави в інформаційній сфері, інформаційних загроз та відповідних захисних заходів.

На думку автора, розмежування інтересів на національні та державні є досить умовним, адже держава розглядається як «виконавчий апарат нації», своєрідний інструмент, за допомогою якого забезпечуються необхідні умови для розвитку особи і суспільства. Тому під державними інтересами доцільно розуміти таку систему усвідомлених потреб українського суспільства, реалізація яких гарантує благополучне існування і сталий розвиток української держави.

Відносно життєво важливих інтересів розглядаються загрози, адже національні інтереси виступають основою для ідентифікації загроз. Узагальнена схема змісту національної безпеки та будь-якої з її складових ґрунтується на трьох базових елементах: інтереси – загрози – захист. Таким чином, загроза як реальна ознака небезпеки виступає базовою конструкцією, яка поєднує між собою інші компоненти безпеки.

Загрозами інформаційній безпеці України або інформаційними загрозами логічно визначити умови та фактори, що перешкоджають реалізації життєво важливих інтересів держави в інформаційній сфері та становлять для них небезпеку.ьПри цьому доречно оперувати не конкретними інформаційними загрозами, а їх видами. Наприклад, О.Морозов пропонує таку класифікацію загроз інформа-

ційній безпеці України відповідно до їх загальної спрямованості: 1. Загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України. 2. Загрози інформаційному забезпеченню державної політики України. 3. Загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку. 4. Загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються.

Зрештою розглянемо останній базовий елемент системи інформаційної безпеки – систему заходів із захисту інтересів держави в інформаційній сфері. Аналіз наявної інформації свідчить, що діяльність державних інституцій із забезпечення інформаційної безпеки держави відбувається на тлі активізації спеціальних служб іноземних держав, організацій, груп та окремих осіб, які використовують інформаційну сферу для здійснення розвідувально-підривної та іншої протиправної діяльності на шкоду інтересам нашої держави. Контррозвідувальна діяльність здійснюється в умовах, коли інформаційні загрози вже реалізуються в конкретних проявах – розвідувальній та іншій суспільно небезпечній, шкідливій діяльності спецслужб. Відтак завданням контррозвідувальної діяльності є активна протидія цим посяганям – контррозвідувальний захист.

На думку автора, контррозвідувальний захист державних інтересів у тій чи іншій сфері становить комплекс контррозвідувальних заходів активної протидії розвідувально-підривним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на відповідні державні інтереси. Контррозвідувальний захист інтересів держави у сфері інформаційної безпеки є важливим сегментом загальнодержавної системи забезпечення інформаційної безпеки України. Головним суб'єктом такого захисту є Служба безпеки України. Контррозвідувальний захист інтересів держави у сфері інформаційної безпеки становить комплекс контррозвідувальних заходів активної протидії розвідувально-підривним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб, які є конкретними проявами інформаційних загроз. Основною метою контррозвідувального захисту інтересів держави у сфері інформаційної безпеки є своєчасне виявлення, припинення і запобігання зазначеним інформаційним загрозам.

УДК 341.824:338.47 (043.2)

Тищук В.В.
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

ДО ПРОБЛЕМИ ПРОТИДІЇ ЗОВНІШНІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Інформаційна безпека є складовою системи національної безпеки України, та становить важливий елемент протидії розвідувально-підривній діяльності іноземних спеціальних служб в сучасних умовах зовнішньої інформаційної агресії.

Виходячи зі змісту та ролі інформації у сучасному світі, американський дослідник М. Маклуен виводить цікаву тезу: «Істинно тотальна війна – це війна за допомогою інформації».

Як зазначає Довгань О.Д. зовнішня інформаційна агресія створює реальні загрози конституційному ладу, територіальній цілісності та національній безпеці України і характеризується цілеспрямованим знищенням української інформаційної інфраструктури, здійсненням кібернетичних атак на об’єкти інфраструктури нашої держави, спробами блокування каналів поширення проукраїнської позиції в інформаційному просторі, проведенням інформаційних операцій та окремих акцій на фоні потужної пропагандистської кампанії проти України [1, с. 1-2].

Метою зовнішньої інформаційної агресії є послаблення моральних сил супротивника та посилення власних шляхом проведення заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях, а завдання полягає в маніпулюванні масами, тому одним з її видів є психологічний вплив. Доцільно навіть використовувати поняття інформаційно-психологічного впливу враховуючи, що об’єктом є індивідуальна або суспільна свідомість.

Інформаційно-психологічний вплив в поєднанні з інформаційно-комп’ютерною революцією відкриває широкі можливості для маніпулювання свідомістю та поведінкою населення навіть на віддалених просторах. Враховуючи процес глобалізації телекомунікаційних мереж, що відбувається у світі, стає зрозуміло, що саме інформаційним видам агресії буде наданий пріоритет у майбутньому. Це спостерігається на прикладі російської агресії на сході України, а також, можна визначити прояви інформаційно-психологічного впливу на населення прикордонних районів, що межують з Угорщиною та Румунією.

Необхідно зазначити, що стосується конфлікту на сході Украї-

ни, то Російська Федерація здійснює деструктивний інформаційно-психологічний вплив на населення з використанням майже повного спектру каналів комунікацій, в першу чергу це: традиційні ЗМІ (орієнтовано старше покоління); електронні ЗМІ, телебачення (орієнтовано старше покоління); Інтернет ЗМІ (орієнтовано на молодь); соціальні мережі (орієнтовано на молодь).

Тривала багатолітня інформаційна пропаганда, яка передувала анексії Криму та окупації Донбасу, сформувала в населення цих регіонів світоглядні та інші стереотипи вигідні ворогу. Належної протидії зовнішній інформаційній агресії в нашій державі не здійснювалось, це дало можливість іноземним спеціальним службам нанести суттєву шкоду національній безпеці України. На жаль Україна продовжує бути об’єктом зовнішньої інформаційної агресії, тобто фактично захищається, але ж ефективна протидія передбачає активні заходи направлені на супротивника та перетворення з об’єкта в суб’єкта інформаційного протиборства. В той же час, Російська Федерація продовжує спроби подальшого просування в ментальному та культурному просторі України з метою формування світоглядних стереотипів шкідливих для української державності, з використанням таких форм інформаційної агресії, як: дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби; маніпулювання суспільною свідомістю соціальних груп населення з метою створення політичної напруженості та хаосу; створення атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини.

Таким чином, забезпечення інформаційної безпеки не можливе без контррозвідувальної складової, тому як просування ворожої пропаганди здійснюють не тільки інтернет блогери та хакери, більшість яких знаходиться за межами України, а також конкретні особи на телебаченні та радіо, що намагаються поширювати російські медіа-продукти з метою формування серед населення України проросійського культурного прошарку представники якого в подальшому позитивно реагують на відповідну пропаганду. Так, наприклад, в багатьох телевізійних розважальних та інших популярних проектах, під виглядом демократичної критики, у виступи артистів та журналістів включається дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління. На ці, на перший погляд не суттєві, на фоні ескалації конфлікту на Донбасі, виклики, повинна бути дієва протидія з боку суб’єктів контррозвідувальної діяльності.

Отже, існує низка проблем в сфері інформаційної безпеки, се-

ред яких найбільш нагальними є: недостатній рівень здійснення інформаційно-психологічного впливу направленого на супротивника; не повністю реалізовано потенціал контррозвідувального забезпечення медіа простору.

У подальших дослідженнях зазначеної проблематики доцільно звернути увагу те, що на території України сформувався найпотужнішій, в порівняні з іншими країнами колишнього СРСР, потенціал спеціалістів ІТ технологій. Враховуючи, що значна частина цих спеціалістів в повній мірі не задіяна, то фактично є можливість правильно організувати їхню діяльність, створити відповідні спеціальні центри та спрямувати основні зусилля на забезпечення інформаційної безпеки нашої держави.

Література

1. Довгань Олександр Дмитрович УДК 340.132: [351.746.1+004.9](477)(043.3) «Теоретико-правові основи забезпечення інформаційної безпеки України» автореферат дисертації на здобуття наукового ступеня доктора юридичних наук.

УДК 341.824:338.47 (043.2)

Ткаченко О.П.
Служба безпеки України

ЩОДО ПОТОЧНОГО СТАНУ РЕАЛІЗАЦІЇ СБ УКРАЇНИ ТРАСТОВОГО ФОНДУ УКРАЇНА-НАТО З ПИТАНЬ КІБЕРБЕЗПЕКИ

Згідно з п.4.4 «Річної національної програми співробітництва Україна – НАТО на 2017 рік», затвердженої Указом Президента України від 8 квітня 2017 року №103, Служба безпеки України визнана головним виконавцем заходів щодо проведення подальших переговорів з НАТО у форматі експертних консультації Україна-Нато з питань кібербезпеки та продовження у взаємодії з НАТО роботи з реалізації заходів Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [1]. Основним завданням Трастового фонду визначено посилення технічних спроможностей України у сфері кібербезпеки через реалізацію проектів, спрямованих на розширення можливостей у забезпеченні кібернетичної безпеки держави та захисту критичної інфраструктури України від кібернетичних атак з боку Російської Федерації [2]

Наприкінці 2016 року укладено та оголошено Наказом ЦУ СБ України від 26.01.2017 №46 додаткову угоду з РСІ Румунії щодо пос-

тачання та передачі обладнання та програмного забезпечення до СБУ. [3] Вказана угода є додатком до «Угоди про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки», що була укладена між Службою безпеки України та Румунською службою інформації 23.07.2015 року. Основною метою укладання додаткової угоди є деталізація порядку та умов постачання та передачі обладнання українській стороні в особі СБ України та створення юридичних підстави для отримання пільг із сплати митних платежів, що передбачені законодавством для товарів, які постачаються Україну в рамках проектів НАТО. На першому етапі реалізації Трастового фонду передбачається створення Ситуаційних центрів з протидії кіберзагрозам на базі СБ України та Державної служби спеціального зв'язку та захисту інформації з розгалуженою мережею автоматизованих датчиків подій, імплементованих в інформаційно-телекомунікаційних мережах об'єктів критичної інформаційної інфраструктури, що підлягають захисту у реальному часі, а також відповідних лабораторій для розслідування інцидентів у кібернетичній сфері.

Зазначені Центри мають стати базовим організаційними та технічними рішенням для розбудови загальнодержавної інтегрованої системи управління безпекою та реагування на кіберінциденти, що має бути у подальшому масштабована до рівня інших складових сектору безпеки та оборони [4]. Роботу вказаних Центрів з функціональністю Центрів управління/врегулювання кіберінцидентів (IMC – Incident Management Center) передбачається запровадити, у тому числі, у форматі груп оперативного реагування на інциденти кібербезпеки на підставі даних, що мають надходити від автоматизованих датчиків подій, імплементованих в інформаційно-телекомунікаційних мережах об'єктів критичної інформаційної інфраструктури, що підлягають захисту у реальному часі.

З урахуванням того, що протягом 2016-2017 років інформаційні ресурси МЗС України неодноразово піддавались кібернетичним атакам, а також зважаючи на те, що в них циркулює інформація, так званого, «чутливого характеру», за погодженням з Держспецзв'язку об'єктом першочергового захисту визначено інформаційно-телекомунікаційні системи МЗС України. Станом на 17.05.2017 року реалізація першого етапу Трастового фонду Україна –НАТО з питань кібербезпеки знаходиться на стадії оформлення румунською стороною необхідних експортних документів для постачання обладнання та програмного забезпечення в Україну. Предметом закупівлі є комп'ютерне й телекомунікаційне обладнання, а також спеціальне

програмне забезпечення, для розбудови двох Ситуаційних центрів (центрів управління/врегулювання кіберінцидентів) на базі СБ України та Держспецзв'язку, програмно-апаратні пристрої для розбудови кінцевих датчиків подій, імплементованих в інформаційно-телекомунікаційних мережах МЗС України, а також обладнання для реалізації стаціонарних та мобільних складових мережевої та криміналістичної лабораторій для розслідування інцидентів у кібернетичній сфері. Проект ТФ також включає в себе реалізацію навчально-методичних та консультативних заходів із адаптаційним підходом, які базуються на інтересах як союзників, так і України та виходить з вимог у сфері безпеки і оборони України.

Наразі, у рамках подальшого розвитку та практичного наповнення ТФ СБ України здійснюються заходи щодо розробка та реалізації впродовж 2017 року програми поглиблених навчальних та практичних курсів у сфері протидії кіберзагрозам, орієнтованої на представників безпекового сектору України: СБ України, Державна служба спеціального зв'язку та захисту України, МВС України, Міністерство оборони України. Орієнтовне тематичне наповнення такої програми СБ України попередньо опрацьовано з Міжнародним Секретаріатом НАТО під час робочої зустрічі, що відбулась в м.Києві у квітні 2017 р [5].

Література

1. Указ Президента України «Про затвердження Річної національної програми співробітництва Україна – НАТО на 2017 рік» від 8 квітня 2017 року № 103/2017/ Президент України. URL: http://www.president.gov.ua/documents/1032017-19779

2. Щодо заснування Трастового Фонду Україна-НАТО з питань кібербезпеки, н.с.129, т.1, с.123, 2014.

3. Наказ Центрального Управління СБ України від 26.01.2017 №46 «Щодо оголошення додаткової угоди з РСІ Румунії щодо постачання та передачі обладнання та програмного забезпечення до СБ України в рамках реалізації Трастового Фонду Україна-НАТО з питань кібербезпеки», К., СБ України, 2017.

4. Щодо заснування Трастового Фонду Україна-НАТО з питань кібербезпеки, н.с.129, т.1, с.124, 2014.

5. Щодо виконання СБ України заходів передбачених Річної національної програми співробітництва Україна-НАТО на 2017 рік, н.с. 132, т.2, с145.

УДК 004.056.5:004.738.5

Толюпа С.В.
доктор технічних наук
Київський національний університет
імені Тараса Шевченка
Пархоменко І.І.
кандидат технічних наук
Київський національний університет
імені Тараса Шевченка

ЗАСОБИ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання кіберзагроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках діяльності установи [1].

На сьогодні системи виявлення вторгнень і кібератак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем кібербезпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення кібератак (СВКа) стали необхідним компонентом інфраструктури безпеки більшості організацій [2].

Наприклад SYN-flood кібератаки, відомі також як TCP-flood атаки, звичайно реалізовуються проти серверів. Даний тип атаки можна змоделювати за допомогою мережі Петрі-Маркова. Визначення елементів цієї мережі приведені нижче, s_j – позиції, t_j – переходи:

s_1– С готовий, s_2– А готовий прийняти пакети SYN з неіснуючою адресою в чергу невідкритих з'єднань,

t_1 – запуск та налаштування додатку для SYN-flood,

s_3– програма запущена на налаштована,

t_2 – відправка пакетів SYN та постановка їх в чергу А,

s_4– запити поставлені в чергу очікуваних з'єднань А,

t_3– переповнення черги А ,

s_5– А не має здатності опрацювати інші запити,

t_4– перехоплення та аналіз трафіку А.

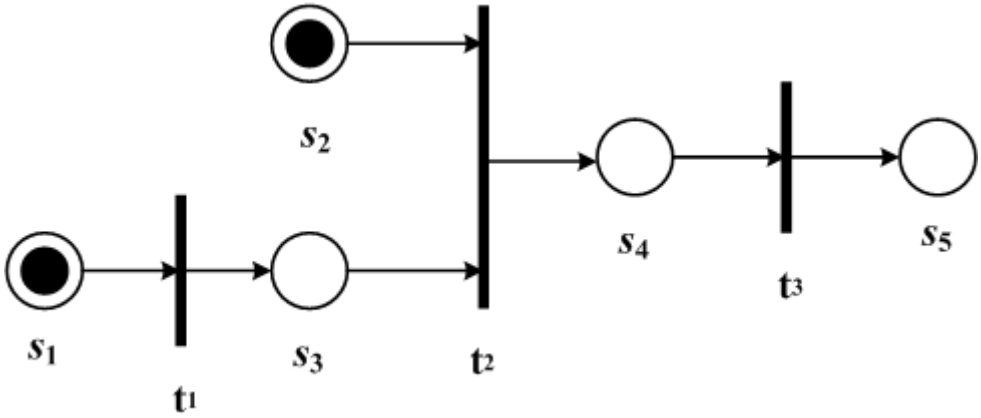

Рис. 1 Мережа Петрі-Маркова етапів реалізації атаки SYN-flood

Особливу увагу потрібно приділити тому, що залежність вірогідності реалізації атаки SYN-flood від часу враховує етап запуску і налаштування програми, який має значно більший середній час, ніж вся решта етапів [3].

В даний час робота по протидії таким кібератакам покладена на міжмережеві екрани. Коли ззовні приходить SYN-пакет, міжмережевий екран не пропускає його у внутрішню мережу, а сам відповідає на нього від імені сервера призначення.

При динамічному збільшенні черги запитів час і можливостей реалізації кібератаки визначається ресурсами системи. Відомо, що для підтримки одного напіввідкритого з’єднання в черзі ОС може бути потрібна пам'ять до 30 кбайт тому за наявності на хості серверної ОС є можливість підтримки очікування достатньо великого числа з'єднань [4].

Аналізуючи дані положення про здійснення кібернетичних атак, можна дійти висновку, що розглянуті вище можливості захисту даних не будуть у повній мірі ефективні якщо їх не використовувати у єдиному комплексі.

Кібернетичні атаки на інформаційну систему реалізуються головним чином за рахунок даних атак: аналіз мережевого трафіку, сканування мережі, загроза виявлення пароля, підміна довіреного об’єкту мережі і передача по каналах зв’язку повідомлень від його імені з привласненням його прав доступу, нав’язування помилкового маршруту мережі, несанкціоноване введення об’єкту мережі, відмова в обслуговуванні, видалений запуск додатків,

Засоби виявлення кібернетичних атак забезпечують одержання даних з мережі про зловмисну активність в зрозумілу інформацію, яка може бути використаний для усунення підтверджених порушень безпеки і забезпечення відповідності нормативним документам. Набір зручних у використовуванні апаратних засобів віддзеркалення загроз дозволяє адміністраторам централізований знаходити, визначати

пріоритетність і відображати загрози за допомогою вже упроваджених в інфраструктуру мережних пристроїв і пристроїв захисту [5].

Отже, з урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципу гарантування безпеки інформації до принципу інформаційної безпеки.

Література

1. Бугайский К. В. Проблемы построения систем информационной безопасности // “Information Security/ Информационная безопасность”. – М.: BHV, 2008. – 250 с.
2. Масюк М. И. НСД: теория и практика // “Специальная Техника”. – К.: Рута, 2003. – 300 с.
3. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО «ТИД ДС», 2001. – 688 с.
4. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть // Вісник Київського університету імені Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46–48.
5. Гуцалюк М. Л. Інформаційна безпека України: нові загрози // Бізнес і безпека, 2012. – № 5. – С. 2–3.

УДК 004.912

Хатян О.А.

Міжрегіональна академія управління персоналом

МОДЕЛЬ ВИЯВЛЕННЯ PR-ВПЛИВУ ЯК ПРОВІДНИКА ІНФОРМАЦІЙНОЇ ЗАГРОЗИ ЧЕРЕЗ ЕЛЕКТРОННІ ЗМІ

ЗМІ є найпотужнішою складовою системи масової комунікації, елементи якої складають основний інструментарій стратегічних комунікацій сучасного суспільства. Перманентній інформаційний тиск (інформаційна загроза) протягом останніх років, фактично перейшов у фазу агресії військової, яка постійно підтримується інформаційною (ознака гібридної війни). Провідником інформаційної загрози є акт інформаційного впливу через інформаційні джерела ЗМІ, який ми називаємо спрямованим або «PR-впливом». Отже, ефективна модель виявлення інформаційних впливів є основою механізму виявлення та протидії інформаційним загрозам та агресіям.

У роботі, свідомо спрямований вплив ми характеризуємо як засіб зміни якісної оцінки чи відношення до певних фактів або об’єктів цільовою аудиторією. Аналіз завдань, методів та механізмів

роботи PR-служб [1,2] дозволив сформулювати поняття «PR-вплив» як засіб реалізації певних інтенцій через публікації в Інтернет ЗМІ та визначити його особливості, критерії, оціночні характеристики. Нами встановлено, що оптимальними для реалізації «PR-впливу» є матеріали орієнтовані не на констатацію фактів, подій чи стосунків (позначаємо їх множину як EV), а спрямовані на їхній аналіз та оцінювання (позначаємо – NEV). Цю характеристику ми називаємо «ступінь подієвості».

Найбільш ефективним механізмом здійснення «PR-впливу» є використання маніпулятивних технік, що базуються на певній лексіці у повідомленнях Інтернет ЗМІ. Серед інших, а на нашу думку найбільш значимими ознаками такого впливу є:

- «емоційнійсть» / «не емоційність» (позначимо *EM* та *NEM*);
- «маніпулятивність» / «не маніпулятивність» (позначимо *MA* та *NMA*).

Сутність моделі виявлення «PR-впливів» демонструє наступний модельний приклад. Якщо відрізняти діяльність PR-служб, що мають на меті впровадження впливу, та незалежного журналістського корпусу (НЖК), цілями якого умовно є «об'єктивне» інформування, тоді інформаційним продуктом діяльності PR-служб є множина PR-повідомлень або PR-послідовностей (позначимо як $PR = \{pr_1, pr_2, \dots, pr_i, \dots, pr_n\}$), а результатом діяльності НЖК є множина НЖК-повідомлень або НЖК-послідовностей (позначимо як $IJC = \{ijc_1, ijc_2, \dots, ijc_i, \dots, ijc_n\}$). Таким чином, множина повідомлень що висвітлює в інформаційному просторі подієвий план складається з об'єднання множин НЖК- та PR- повідомлень ($M = PR \cup IJC$).

За цих умов ми сформулювали гіпотезу щодо можливості розпізнавання PR – послідовностей, покликаних впровадити акт навмисного штучного впливу у загальному інформаційному потоці:

Для деякої множини повідомлень $\widehat{M} = \{m_1, m_2, \dots, m_i, \dots, m_n\}$ інформаційного потоку $I = (M, \gamma)$, де відношення квазіпорядку $\gamma = M \times M$, впорядкованою за $T = \{t_1, t_2, \dots, t_n\}$ існує можливість виділення множини $PR = \{pr_1, pr_2, \dots, pr_i, \dots, pr_n\}$ – PR-послідовність, для якої:

$$P(\widehat{M}, A, T) = \begin{cases} p_i \geq \alpha,\ m_i \in PR; \\ p_i < \alpha,\ m_i \notin PR; \end{cases}\Bigg|_{|PR| \to max;\ \Delta t \to min}, \qquad (1)$$

із статистичною достовірністю, що не перевищує α.

При цьому,

$$P(\widehat{M}, A, T) = \{p_i, i = \overline{1, n}\}$$

є ймовірність події $A = \{\alpha_i, i = \overline{1, n}\}$, яку, в свою чергу, обчислюємо

як нормалізовану інтегральну складову лінгво-статистичних [3] ознак:

$P_{NEV}(m_i)$ – ймовірність, що повідомлення m_i є неподієвим;

$P_{EM}(m_i)$ – ймовірність, що повідомлення m_i є емоційним;

$P_{MA}(m_i)$ – ймовірність, що повідомлення m_i є маніпулятивним.

Тобто,

$$P(a_i) = \overline{\sum \{P_{NEV}(m_i), P_{EM}(m_i), P_{MA}(m_i)\}}. \quad (2)$$

Отже, (1,2) формалізують модель виявлення PR-послідовності на множині повідомлень інформаційного потоку M, покликаної до впровадження певної множини впливів (багатовекторність) у різних сферах життя суспільства. Тоді, галузеве розмежування та/або сюжетно-об'єктові патерни отримаємо шляхом «накладення» на отриману множину повідомлень відповідної топології галузевих рубрик та/або тем дня. За умови ж звуження потоку до галузевого $\widehat{M}$, отримуємо окрему PR-послідовність ймовірного акту впливу.

Таким чином, запропонована нами модель покликана виявити факт наявності контенту, спрямованого на впровадження свідомого інформаційного «PR-впливу», як провідника інформаційної загрози. Крім того, на нашу думку, під час інформаційної агресії даний підхід надасть змогу оцінювати можливі варіанти її розвитку та впроваджувати відповідні запобіжні заходи. То ж, саме на вивчення аспектів прикладного застосування моделі виявлення PR-впливу і будуть спрямовані наші подальші дослідження.

Література.

1. Кравченко Н.П. Использование pr-технологий в информационной работе пресс-служб. / Н.П. Кравченко / Методическое пособие для работников пресс-служб, руководителей средств массовой информации, органов государственной власти и местного самоуправления. Выпуск №21 – Краснодар, 2011г. – 153с. С. 17., Иванченко Г.В. Реальность Паблик Рилейшнз. / Г.В. Иванченко — М: Смысл, 1999.

2. White J., Blamphin J. What we need to know //Journal. The Institute of Public Relations. - 1995. - Vol. 13. - N 8.

3. Панченко В. М. Лінгвостатистичні ознаки маніпулювання суспільною свідомістю в засобах масової комунікації / В. М. Панченко [Текст] // Modern information technologies development in the Sphere of Security and Defence. 2009. – № 1 (4). – С. 81–85.

УДК 519.816

Циганок В.В.
доктор технічних наук,
старший науковий співробітник
Інститут проблем реєстрації інформації НАН України

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПОБУДОВІ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ

Термін «інформаційні операції» (ІО) набув значне поширення на початку нинішнього століття, коли інформація стала найважливішим стратегічним ресурсом, нестача якого призводить до значних втрат у всіх сферах життя. У розсекречених документах Департаменту оборони США, а саме в «Дорожній карті інформаційних операцій» [1], термін ІО був визначений як «Інтегроване застосування основних засобів радіоелектронної боротьби, операцій у комп'ютерних мережах, психологічних операцій, військового маскування й операцій по забезпеченню безпеки, у концепції з пов'язаними з ними можливостями, з метою надання впливу, руйнування, знищення або захоплення в супротивника керування процесом прийняття рішень (як особистісного, так і автоматизованого) при одночасному захисті своїх засобів». Зміст, що закладається в термін ІО, охоплює й розкриває інформаційний вплив на масову свідомість (як на ворожу, так і на дружню), вплив на інформацію, доступну ворогові й необхідну йому для прийняття рішень, а також на інформаційно-аналітичні системи супротивника [2].

Зазначимо, що одним із основних компонентів оборонної ІО, є стратегічне планування. Очевидно, не існує єдиного «стандартного» плану проведення ІО. Можна лише розглянути зразкову, отриману шляхом узагальнення деяких уже реалізованих ІО, послідовність дій при їхньому здійсненні. Причому вибір оптимального набору таких заходів у певний момент часу залежить у першу чергу від наявності ресурсів для їхнього проведення в цей певний момент, а також від результатів виконання раніше обраних заходів. Оптимальність тут варто розглядати з погляду ефективності досягнення цілей проведення тієї, або іншої оборонної ІО.

У контексті даної роботи було поставлено завдання: розробити комплексну методику підтримки прийняття рішень (ППР), що дозволяє підвищити якість процесу стратегічного планування оборонної ІО. Пропонуються методика формальної побудови стратегії ІО із залученням групи фахівців, компетентних у цій області. На основі сучасних методів експертної ППР пропонується можливість най-

більш повного й без спотворень одержання знань від фахівців, і використання їх для побудови адекватної моделі предметної області.

Як відомо, у загальному розумінні стратегія являє собою не деталізований план дій, розрахований на тривалий період часу й спрямований на досягнення певної головної мети. У той же час, план повинен бути гнучким, конструктивним, стійким до невизначеності умов середовища й таким, що передбачає конкретизацію шляхом декомпозиції цієї головної мети.

Не виникає сумнівів у тім, що при створенні таких стратегічних планів потрібно опиратися на всі наявні знання в певній предметній області, у тому числі на знання, отримані від експертів. Щоб мати реалістичні довгострокові плани, їх потрібно адаптувати до неминучих змін поточної ситуації й ураховувати наявність ресурсів для їхнього здійснення, необхідних у кожний поточний момент. Тому стратегічні плани можуть бути раціональними лише на певному інтервалі часу.

З огляду на це, технологія побудови стратегії передбачає наступні етапи:

1) Побудова бази знань (БЗ) – етап дозволяє особі, що приймає рішення (ОПР), інженерам по знаннях і експертам працювати віддалено у веб-орієнтованому середовищі для створення БЗ без необхідності збиратися разом. Цей етап включає ряд під-етапів:

а. Підбір груп експертів для проведення експертизи – У рамках експертизи при вирішенні різних питань ОПР та на інженерами по знаннях формуються різні групи фахівців, найбільш компетентних у кожній певній області.

б. Побудова (у ході діалогу з експертами) ієрархії цілей, що описує предметну область – тут ОПР формулює стратегічну мету, наприклад, «Забезпечити достатній рівень протидії інформаційним атакам», що, у ході проведення експертиз інженерами по знаннях, підлягає декомпозиції на локальні цілі (фактори), які істотно впливають на її досягнення. Створена програмна система дозволяє різним експертним групам працювати одночасно, при цьому кожний з експертів може бути включений до складу різних груп. Рішення про достатній рівень деталізації й припинення подальшої декомпозиції стратегічної мети приймають організатори експертизи у випадку, коли нижній рівень ієрархії цілей будуть складати тільки лише цілі (фактори), що являють собою готові до реалізації конкретні заходи (проекти).

в. Оцінка відносних впливів цілей в ієрархії – визначається інженером по знаннях у випадку наявності достовірних знань про рівень даного впливу на досягнення певної цілі, або ж, у іншому випадку, – групою експертів шляхом парних порівнянь впливів цілей

(факторів).

2) Визначення оптимальної стратегії – Очевидно, що чим більше вагомість певного проекту, або заходу, тим істотніше він впливає на досягнення стратегічної мети. Тому, направлення ресурсів на цей проект буде приносити більш вагомі й відчутні результати. У той же час, немає сенсу виділяти на проект ресурсів менше, ніж необхідно для його старту й існування. Отже, в якості оптимальної стратегії пропонується обирати оптимальний варіант розподілу ресурсів між проектами (тобто той, котрий забезпечує найбільш ефективне досягнення стратегічної мети) [3].

Список рекомендованих дій для ОПР у вигляді набору проектів/заходів протидії інформаційним впливам з розрахованими об'ємами фінансування буде базисом для оптимального стратегічного плану у довготерміновій перспективі за умови забезпечення певною кількістю фінансових ресурсів.

Дослідження виконані в рамках проекту Ф73/23558 «Розробка методів і засобів підтримки прийняття рішень при виявленні інформаційних операцій» Державного фонду фундаментальних досліджень України.

Література

1. Information operations roadmap. DoD USA, 30 october 2003, 78p. Retrieved 20/04/17 http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf .
2. Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. –К.: Інтертехнологія, 2009, 164с.
3. Циганок В.В. Проблема розподілу ресурсів, як розширення можливостей систем підтримки прийняття рішень *Реєстрація, зберігання і обробка даних*. 2010, т.12, №2, С.232-237.

УДК 316.776.33

Черниш Ю.О.
Військовий інститут телекомунікацій та інформатизації
Штонда Р.М.
Військовий інститут телекомунікацій та інформатизації
Мальцева І.Р.
Військовий інститут телекомунікацій та інформатизації

СТРАТЕГІЧНІ КОМУНІКАЦІЇ – МЕХАНІЗМ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІЙНАМ

З початку 60-х років XX століття триває бурхливий розвиток

інформаційних технологій, які набули глобального характеру. В світі відбувається стрімке формування інформаційного суспільства. Головною його особливістю є те, що стратегічним ресурсом стає інформація, яка здатна взаємодіяти не тільки з матеріальним, а й з духовним світом людини.

Вже три роки Україна знаходиться в стані неоголошеної війни. «Гібридна» війна, яку розв'язано проти демократії ведеться одразу на декількох «фронтах» одним з яких є, інформаційний. На сьогоднішній день стає все більш зрозумілим, що результатом конфлікту буде не тільки здобуття перемоги, а й чия сюжетна лінія – буде більш переконлива та зможе пояснити події аргументовано, з якої можна дійти висновку щодо виникнення конфлікту.

З кожним роком ці ідеї все більше набувають поширення у військовій думці і практиці. Інструментом для реалізації цих ідей та думок виступають стратегічні комунікації. Стратегічні комунікації перед усім стають інструментом гармонізації тем, ідей, образів та дій. Вони передбачають діалог і підхід до побудови відносин на основі уважного ставлення до культурних та історичних особливостей, місцевих способів ведення справ та виявлення місцевих лідерів думок [1,с.74]. Особливої ваги зазначене набуває саме зараз, у період коли в державі відбувається диверсифікація контенту, загострюється битва за інформаційні ресурси [2]. Тому стратегічні комунікації необхідно спрямовувати на підрив авторитету противника способом підтримки своїх дій зі сторони місцевого населення ворогуючої сторони, своєї держави та світової спільноти. Перемога за уявлення людей про такі операції і є метою реалізації стратегічних комунікацій.

Можливо саме через брак уваги до теми стратегічних комунікацій і недослідженість її в науковій площині наша держава і виявилась неспроможною вчасно відвернути від себе агресію й відповісти на сучасні загрози, зокрема «гібридні» війни [3,с.14]

На сьогоднішній день необхідно остаточно усвідомити, що стратегічні комунікації є, не додатковими діями, а невід'ємною частиною планування та реалізації усіх військових операцій та видів діяльності.

Література

1. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: К. : НІСД, 2016. URL: www.niss.gov.ua.

2. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. URL: http://goal-int.org.

3. Сутність гібридної війни проти України / В.А.Ліпкан // Імперативи розвитку цивілізації 2015-№2.

УДК 32.019.51:328.16

Чеховська М.М.
доктор економічних наук, професор
Національна академія Служби безпеки України
Лісовська О.Л.
кандидат економічних наук, доцент
Національна академія Служби безпеки України
Крапівіна Н.В.
Національна академія Служби безпеки України

КРИЗОВІ КОМУНІКАЦІЇ ЯК ЕЛЕМЕНТ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ

Надзвичайно важливим аспектом комунікаційної політики державних органів є організація впливу на громадську думку під час так званих кризових ситуацій. Кризовою ситуацією визнається подія, що ставить під загрозу стабільність організації, призводить до порушення нормальної її діяльності і потенціально націлена зашкодити її репутації. Така подія, як правило, супроводжується не завжди доброзичливою увагою ЗМІ та інших контактних аудиторій. Наведемо кілька рис, які, на думку науковців, неминуче дадуть про себе знати під час кризової ситуації: раптовість; недостатність інформації; ескалація подій; втрата контролю; наростання втручання зовнішніх сил; ментальність загнаного у глухий кут; паніка [1].

Безпосередньо провадження комунікаційної політики під час кризової ситуації має базуватися на наступних позиціях:

- зайняти чітку, недвозначну позицію; проте організація не повинна виглядати надто прямолінійно, комунікаційна політика повинна бути достатньо гнучкою, щоб реагувати на зміни в розвитку подій, не допускається ухилення або неправда, які породжують ще більші проблеми;
- залучити до активних дій найвище керівництво: керівник повинен бути не лише втягнутим у розв’язання кризових ситуацій, що на практиці трапляється завжди, а й наочно доводити іншим свою участь у подоланні кризи. Чим серйознішою є кризова подія, тим доступнішим для мас-медіа повинен стати керівник;
- активізувати підтримку з боку “третьої партії”: необхідна підтримка своєї позиції з боку відомих аналітиків, провідних каналів інформації, авторитетних вчених та ін., хто користується великою повагою та має великі повноваження;
- організувати присутність на місці подій;

- централізувати комунікації;

- дивитися на кризу широко: низька активність на початку кризи може виявитись не менш небезпечною, ніж надмірна реакція на її посилення і зайве нагнітання окремих ситуацій;

- заздалегідь думати про позиціювання організації після подолання кризи;

- здійснювати постійний моніторинг та оцінку проходження кризи.

Окремо слід відзначити необхідність роботи в умовах кризової ситуації з цільовими аудиторіями. Так, дослідниками відзначається важливість доведення до громадської свідомості і міцного закріплення в ній чітко запрограмованих тез: створений антикризовий комітет для захисту інтересів потерпілих; прийняті необхідні рішення, по яким виконання та гласність роботи жорстко відстежуються; запропонований проект, який передбачає значні покращання і з цього приводу організовані спеціальні громадські заходи [2]. Такого роду стратегія дозволяє зменшити негативну реакцію, зберегти, наскільки можливо, а потім закріпити імідж організації чи проекту в очах його співробітників, партнерів і громадськості. Більше того, в кризовій ситуації виникає непогана можливість показати громадськості, що організація не бездушний механізм, а структура, яка складається з порядних та дієздатних людей, що, без сумніву, здатне підвищити репутацію відомства в цілому.

Ще одним доволі важливим аспектом всієї антикризової кампанії є висунення власної версії кризової ситуації, при чому слід відмітити, що така проблема постає в більшості випадків, незалежно від характеру події. Власна версія – це, в першу чергу, можливість взяти вирішення проблеми під свій інформаційний контроль, що попередить виникнення не вельми бажаних сторонніх версій.

Висунення версії повинно відбутися якомога швидше, на думку експертів, відсутність будь-якої реакції з боку організації в перші 24 години значно послаблює можливість контролював ситуацію в подальшому [3]. Якщо ж організація взагалі відмовчується, намагаючись уникнути негативної інтерпретації подій в ЗМІ, то такі інтерпретації все рівно з’являться, при чому громадська думка, швидше за все прийме позицію ЗМІ, повірить у звинувачення.

Слід відзначити, що з огляду на те, що в нашому суспільстві більшість конфліктів мають під собою економічний, соціальний та політичний ґрунт загальнодержавного рівня, самостійно жодна з інституцій розв’язати їх не здатна. Тому завдання в сфері формування

громадської думки стосовно діяльності державних органів влади має полягати безпосередньо в реалізації завдань з виявлення, відстеження та мінімалізації конфліктів, а не в їх розв'язанні з огляду на певну нереальність виконання останнього.

Література

1. Бодуан Ж.-П. Управление имиджем компании. Паблик рилейшнз: предмет и мастерство / Ж.-П. Бодуан. – М. : ИНФРА-М, ИМИДЖ-Контакт, 2001. – 233 с.

2. Чумиков А.Н. Связи с общественностью / А.Н. Чумиков. – М. : Дело, 2001. – 272 с.

3. Морозова Е.Г. Политический рынок и политический маркетинг: концепции, модели, технологи / Е.Г. Морозова. – М. : РОССПЭН, 1999. – 246 с.

УДК 321:351.74(477)

Шиповський В.В.
Національний університет оборони
імені Івана Черняховського

КІБЕРАТАКА ЯК ВИД ЗАСТОСУВАННЯ У СЕКТОРІ БЕЗПЕКИ ТА ОБОРОНИ: DDOS-АТАКИ

Сучасна армія потребує сучасних засобів захисту від ворожого застосування та засобів впливу на потенційного ворога. Сьогодні кожен військовослужбовець користується всесвітньою мережею інтернет, мобільним зв'язком та іншими здобутками розвитку інформаційних технологій. Листування через соціальні мережі та електронну пошту та ін. все частіше містять інформацію, яка не може бути розголошена для загалу задля безпеки військових підрозділів. Все частіше під час ознайомлення з останніми новинами, ми зустрічаємо слова *кібератака, кібербезпека,* тощо. Зазначені (відносно нові) терміни потребують уваги та вивчення також в секторі безпеки та оборони.

Щодо заходів запобігання кіберзлочинів в нашій державі, в жовтні 2015 році було засновано підрозділи кіберполіції, та внесені деякі зміни у закон України «Про основи національної безпеки України». У Міністерстві оборони України створено підрозділи, напрямком роботи яких є кібербезпека. Але проблема потребує більш ретельного дослідження та подальшої праці у зазначеному напрямку роботи. Відсутність спеціалістів у сфері кіберзахисту у секторі безпеки та оборони виникла перш за все – недостатнім фінансуванням українських фахівців даної області, в той час як інші держави виділяють належну фінан-

сову підтримку для забезпечення належного рівня спроможності захиститись від кібератаки та нанести удар у відповідь.

23 грудня 2015 року відбулась досить масштабна та одна з найбільш відомих в нашій країні кібератака . Об'єктами атаки стали інфраструктурні та енергетичні об'єкти України у Прикарпатті, Київській та Черновецькій областях. Як наслідок – 220 000 споживачів електроенергії лишись обезструмленими. У результаті розслідування було виявлено, що операція була ретельно спланована, мала певну послідовність та готувалась досить тривалий час спеціалістами сфери інформаційних технологій. Атака складалась з трьох кроків, і перший крок був здійснений за пів року до самої події:

крок 1: *Розвідка.* 13 травня 2014 оператори підприємств отримали електронні листи, які привели до зараження технічних засобів. Файл містив інформацію про перелік шкідливих паролів, які необхідно обов'язково змінити для захисту даних підприємства. В результаті активації на комп'ютери автоматично була встановлена троянська програма **Backdoor.Fonten.Win32.4**., що містила в собі модуль, який збирав інформацію про систему та мережу і відсилав інформацію на віддалений центр, яким керували зловмисники, що відкрило їм доступ до інформації про облікові данні, режими використання ПК, графіки робіт та ін.;

крок 2: *Активне зараження*. З червня 2014 року по жовтень 2015 року ворожі хакери почали розсилати заражені файли з назвами, які могли зацікавити операторів та працівників підприємств (інформація зі списками працівників, які нібито будуть мобілізовані, про зв'язки народних депутатів з сепаратистами на сході та ін.). Насправді документи містили в собі небезпечне програмне забезпечення, який надавав змогу віддаленого керування роботою підприємства. 23 грудня близько 15.30 хакери перейшли до активної фази операції: дистанційно вимикали струм на підстанціях, видаляли інформацію, що зберігалась на жорстких дисках та намагались перевантажити телефонну мережу для позбавлення працівників зв'язку (за попередніми даними дзвінки велись з території Російської Федерації). Було пошкоджено декілька серверів та робочих станцій що викликало проблеми з налагодженням та відновленням роботи станцій.

крок 3: *Ставка на дурня.* 20 січня 2016 року оператори отримували excel-документи з важливою інформацією про "Укренерго"; насправді документ містив в собі вірус, який мав активуватись разом з активацією макросів. Вірус мав блокувати керуючий сервер – але набутий працівниками досвід попередив чергову загрозу.

Окрім енергетичної галузі атака була спрямована на інші важ-

ливі об'єкти: телевізійні канали 1+1 и СТБ, аеропорт Бориспіль, ряд інших державних підприємств та ін .

Розвинуті країни вже більш ніж десять років приділяють значну увагу проблемі кібербезпеки після багатьох випадків атак зловмисників цифрового світу. 7 травня 2011 року було Міністерство фінанфсів Фрації стало об'єктом ретельно підготовленої кібератаки: за допомогою троянських вірусів хакери взяли під контроль 150 робочих станцій . 26 липня 2016 року за допомогою створення фейкового сайту була спроба кібеатаки проти демократичної партії США.

Найбільш поширенішим в останні часи стали досить поширеними Dos та Ddos – атаки, спрямовані на відмову в обслуговуванні, при успішній реалізації яких, блокується доступ користувачів інформаційних систем до ресурсів серверів, що у свою чергу може призвести до припинення роботи усієї системи та втрати інформації. Різниця між Dos-атакакою та Ddos- атакою, полягає в тому, що під час Ddos- атаки задіяні декілька джерел впливу та сервер, якій підлягає нападу (*з англ. Ddos: (Distributed) Denial-of-service attack),* тобто розподілений напад.

Одним зі шляхів застосування Ddos – атак, є відправлення великої кількості хибних запитів, при чому в даному випадку можуть використовуватись персональні комп'ютери осіб, які навіть не підозрюють, що стали співучасниками атаки. Основними причинами популярності цього виду кібератаки:

1) легкість у виконанні;
2) проблематичність відстеження;
3) малі витрати на виконання.

Що ж до сфери використання, людей та організацій, які можуть використовувати чи бути жертвами подібних атак – перелік може бути нескінченним. Будь-то конкуруючі торгівельні компанії, будь-то підприємства чи служби та ін. Сайт Міністерства освіти став жертвою Ddos-атаки, сайт Укрзалізниці, Міністерства фінансів. 13 грудня 2016 року сайт Міністерства оборони був атакований – певні матеріали було викрадено та оприлюднено у мережі Інтернет.

У ситуації, що склалася в нашій країні, державні та приватні підприємства які мають стратегічне значення або належать до оборонного сектору мають бути захищенні не тільки від фізичних атак, але й інформаційних. Тому треба приділяти особливу увагу до відбору працівників, які мають доступ до важливої інформації, особовий склад повинен бути підготовленим до кіберзагроз шляхом інструктажів та навчання та допуску до роботи через здачу заліків, робочі станції та сервера підприємств повинні мати необхіднийе програмне забезпечення для належного рівня кібербезпеки. Кібербе-

зпека обов’язково повинна зайняти певну кількість годин серед предметів навчання сучасних навчальних закладів (навіть не технічних напрямків). Інформація в сучасності являє собою зброю і захист одночасно, тож навчатись краще на помилках інших, не допускаючи їх у майбутньому нашої держави.

Література

1. http://blog.i.ua
2. http://workfrom.home.ua
3. http://all.news.ua

УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

УДК 621.391

Блавацька Н.М.
кандидат технічних наук, доцент
Національна академія Служби безпеки України
Юрх Н.Г.
Національна академія Служби безпеки України

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ РОЗПІЗНАВАННЯ МОВЛЕННЯ

Потреба в розпізнаванні мовлення обумовлена нагальними вимогами людської цивілізації, багато в чому обмеженими природними особливостями комунікативних функцій людського організму. З одного боку ці функції забезпечують можливості швидкого прийому інформації через зорові і слухові органи, з іншого боку видача інформації назовні можлива за допомогою вербальних органів (словесне спілкування) і засобів немовленевого спілкування, які значно поступаються цим органам в швидкості. "Спілкування" за допомогою немовленевих засобів спілкування з механічними пристроями, апаратурою і приладами більше відстає в швидкості в порівнянні з вербальним контактом. Так, наприклад, нам швидше віддати команду голосом, надиктувати текст, повідомити словами про своє рішення, ніж робити це руками за допомогою елементів управління пристроєм.

Поряд з автоматичним розпізнаванням змісту повідомлення і синтезом мовлення, дослідники мовленевих сигналів успішно вирішують завдання: автоматичного розпізнавання особи, що говорить (тобто системи розпізнавання мовлення можуть виконувати функції систем захисту від несенкціонірованного доступу), автоматичної верифікації, тих що говорять (підтвердження того, що цю фразу промовила конкретна людина), оцінювання за голосом емоційного стану оператора, розпізнавання мовлення, яке здійснено в іншому повітряному середовищі (гелієве мовлення), визначення по мовленевому сигналу патології органів мовотворення, розробки досконаліших методів викладання іноземних мов (вироблення правильного

акценту та інтонації відповідно до картини "еталонних" параметрів мовленевого сигналу), допомоги особам з дефектами органів слуху і мовотворення, очищення та аналізу затупленого мовлення, створення систем вузькополосної перешкодостійкості зв'язку, а також ряд інших завдань.

У зв'язку з цим розвиток систем розпізнавання мовлення являється пріоритетним.

Зазвичай під розпізнаванням мовлення розуміють весь комплекс послуг по трансформації мовленевого сигналу в завершений і функціональний набір визначальних відомостей про передане повідомлення. Але те, що на теперішній час використовується в голосовому інтерфейсі деяких пристроїв, в принципі не є комплексом таких послуг. Насправді часто йдеться про систему розпізнавання звуків, фонем або ж певних звукових зразків в мовленевому сигналі. Справжнім розпізнаванням мовлення слід називати симбіоз двох систем: розпізнавання звуків і розуміння мовлення.

Система розпізнавання звуків стикається з такими труднощами: особливості голосу диктора (тембр, шумові вкраплення, обумовлені будовою мовного тракту), різні манери промовляння тих чи інших звуків (прискорення або уповільнення темпу, "проковтування" деяких звуків, тимчасове зміщення тональності, неусвідомлена вставка незначущих призвуків між словами), специфічна артикуляція – все це накладає відбиток на спектральний склад мовленевого сигналу. А спектр, треба відзначити, при таких умовах змінюється істотно, причому на його основі система розпізнавання звуків намагається відрізнити переходи звуку в звук, і з цих причин важко сформувати універсальні еталони звуків, порівняння з якими не залежало б від непередбачених спотворень в спектрі. Крім того, теорії розпізнавання зазвичай базуються на аналогіях людської здатності розуміти мовлення, але немає жодного способу реально побачити або виміряти, як це все працює всередині людини.

Так що на сьогоднішній день поки зарано говорити про створення повноцінних систем розпізнавання мовлення, які могли б відповідати людському механізму розпізнавання. Але справа не стоїть на місці. Вже є працюючі голосові системи, придатні для вузькому кола завдань.

Література

1. Обжелян Н.К., Трунин-Донской В.Н. Машины, которые говорят и слушают. Кишинёв: Изд-во Штиинца, 1987. 176 с.

2. Винцюк Т.К. Анализ, распознавание и интерпритация речевых сигналов: моногр. Київ: Наук. думка, 1987. 264 с.

3. Деркач М., Гумецкий Р., Мишин Л. Восприятие речи в распознающих моделях. Львов: Изд-во Льв. ун-та, 1971. 186 с.

УДК 008;130.2

Видрич Н.М.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»
Жарук Д.М.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»

МЕДІАВІРУСИ В ІНТЕРНЕТІ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

Медіа віруси - поширювані по інфосфері меми та мемокомплекси, що змінюють сприйняття локальних і глобальних подій. Наукова дисципліна, що вивчає вірусні і менш впливові меми, називається меметика, плодами якої і користувався Дуглас Рашкофф для формування концепції «медіавірусів». Оболонкою медіавірусу як фактора, який розкриває складність і повноту зв'язків інфосфері, може бути: подія, винахід, технологія, наукова теорія, філософська система, сексуальний скандал, поп-зірка, публікація на інтернет-сайті.

Медіавірус (англ. Media virus) - термін, введений американським фахівцем в галузі засобів масової комунікації Дугласом Рашкоффим, для позначення медіа подій (де медіа - імітація відповідного англійського терміна, що означає в перекладі на українську мову засоби комунікації), що викликають прямо чи опосередковано певні зміни в житті суспільства [1].

Можна виділити наступні етапи формування та впливу медіавірусів на національну безпеку:

перший етап - створення активного незадоволеного даним політичним режимом соціального сегмента;

другий етап - інтенсивна інформаційна пропаганда цієї незадоволеності в інформаційному просторі;

третій етап - блокування соціальних груп, які не розділяють ідеологію даного соціального сегменту.

При цьому повинні вирішуватися наступні задачі:

- розбудити (підняти) активність масової свідомості;
- утримати активність (агресивність) на певному рівні, не виходячи за його межі;
- озброїти своїх прихильників аргументацією для бесід з їхніми супротивниками.

Вже зараз потенціал медіавірусів є достатнім, аби з їх допомогою влаштувати повномасштабний соціальний катаклізм, загальнонаціональну акцію, організувати громадський або політичний рух тощо.

Також необхідно зазначити на суттєвий вплив поширення медіавірусів на політику. Соціальні мережі полегшують можливість об'єднання осіб, що ставлять перед собою захоплення влади, у тому числі і незаконного. Інтернет простір може використовуватися як місце спілкування, розробки і обговорення злочинних планів. Таке спілкування набагато безпечніше «фізичних» зустрічей в оффлайні. Крім того це може непомітно підривати деякі державні основи шляхом створення так званих «віртуальних держав», що мають майже усі атрибути держави за винятком території [2].

Сьогодні однією з сфер розповсюдження медіавірусів є Інтернет. Існують і досить специфічні прийоми в інформаційно-психологічному протиборстві, що дозволяють домогтися переваги, не маючи початкових ресурсів. Один з найцікавіших - створення «медіавірусів», які є яскравими запам'ятовуються образами, які впливають за принципом «троянського коня» на політичну свідомість виборця. Мета - відволікання від реального стану речей або закріплення чітко визначеної реакції на якогось політика чи ідею (часто на підсвідомому рівні). «Медіавірус» може ґрунтуватися на реальних подіях або ж бути сформованим штучно від початку до кінця. В більшості випадків «медіавіруси» стають частиною Інтернет-культури і не надають будь-якого впливу на конкретні політичні події, якщо не стали інформаційним приводом або політичною реакцією. Однак якщо «медіавірус» розробляється з політичною метою - він стає одним з найефективніших видів зброї в *інформаційно-психологічному протиборстві* [3].

Медіа-активізм (Англ. Media activism) - явище, особливо характерне для кількох останніх десятиліть, але передумови якого, ймовірно, можна було спостерігати протягом усього розвитку засобів комунікації між людьми. Медіа-активістів можна назвати «партизанами інформаційної війни», бо існуючі організовані групи або окремі індивіди ведуть спеціальну роботу по створенню медіавірусів. Серед найбільш відомих медіа-активістів або, принаймні, людей, які запустили ряд стали відомі медіавірусів, можна назвати американського вченого Тімоті Лірі, з яким Дуглас Рашкофф був знайомий особисто. Сьогодні політичні діячі та інші публічні персони - цілком ймовірно, знайомі з меметикою і принципами поширення мемів - будучи природними ньюсмейкерами для засобів масової інформації, часто стають авторами різних вірусних мемів [4].

Література

1. Рашкофф Д. Медиавирус. Как поп-культура тайно воздействует на ваше сознание / Пер. с англ. Д. Борисова. — М.: Ультра. Культура, 2003. — С. 368.

2. Алексеева, И. Ю. Проблема интеллектуального суверенитета в информационном обществе // Информационное общество. – 2001. Вып. 2. – С. 5–9.

3. [Електронний ресурс]. – Режим доступу: http://www.telekritika.ua/daidzhest/2008-09-29/40893?theme_page=1440&

4. Циховська Е. Інформаційні віруси: картина як інтернет-мем // Актуальні проблеми іноземної філології. Серія: Лінгвістика та літературознавство: зб. наук. статей. – Бердянськ: БДПУ, 2013. – Вип.VIII. – Ч.1. – С. 152-158.

УДК 94 /930.85

Гуз А.М.
доктор історичних наук, професор
Національна академія Служби безпеки України
Гоц О.В.
Національна академія Служби безпеки України

ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ У СТАРОДАВНЬОМУ ЄГИПТІ

Інформація, яку потрібно зберігати у таємниці, з'являється ще на додержавних стадіях розвитку людства. Ці відомості були пов'язані насамперед з військовою справою. Збір і зберігання інформації проводився стосовно місць розташування військових формувань – своїх і сусідів, їх кількості, мобільності й рівня військової вправності. Оскільки загрози не були постійними й виникали під час підготовки до війни, охорона цієї інформації актуалізувалася лише на період військових конфліктів і не провадилася на постійній основі. Відсутність безперервних загроз не викликала необхідності у визначенні таємної інформації як окремого виду, а її охорона здійснювалася хаотично, без будь-яких нормативних обґрунтувань.

Державна таємниця та відповідні інститути її збереження виникають у період розвитку держав. Функції цих інститутів формуються, вдосконалюються і змінюються відповідно до динаміки реалізації державою своїх потреб та інтересів (зовнішніх і внутрішніх). Зміни пріоритетів у державній політиці щодо власної безпеки з питань захисту таємної інформації зумовлювали створення або ліквідацію відповідних державних інститутів, зміну їхньої структури та функцій.

У період могутнього зростання держави стародавніх єгиптян таємна інформація, а особливо її надійне зберігання і вміле використання під час заколотів та міжетнічних конфліктів, дало змогу єгипетським фараонам без особливих зусиль об'єднати навколо себе

цілу низку вільних племен. Стародавні єгипетські воєначальники завдяки тактиці дезінформування своїх найближчих сусідів – ефіопів, карфагенян, вавилонян та ассірійців –розпалюють між ними таємну ворожнечу[1]. Організована на самому вищому рівні, як на той час, психологічна війна дозволила їм захопити всю Північно-Східну Африку, розширити державні кордони на східному узбережжі Середземного моря. Таємні операції стародавніх єгиптян проти своїх ворогів, за оцінками військових експертів, навіть для наших часів вважаються високопрофесійними і результативними. У Стародавньому Єгипті вперше на державному рівні було створено добре організовану професійну і досить надійну структуру для захисту державних таємниць. Усі повноваження із забезпечення захисту державних таємниць покладалися на храми. Головні жерці у храмах Стародавнього Єгипту виконували функції, говорячи сучасними термінами, уповноважених режимно-секретного органу. Вони та їх підлеглі були основними носіями секретної інформації. Їх місія вважалась священною і непорушною. В окремих випадках, залежно від важливості інформації, її носій після безпосередньої передачі даних з уст в уста, аби запобігти можливому розголошенню, підлягав фізичному знищенню[1].

З виникненням у єгиптян писемності, на рівні знаків та символів інформація також відображається за допомогою ієрогліфів. Ще до сьогодні значення не всіх ієрогліфів з'ясовано. Одним із найвизначніших винаходів стародавніх єгиптян стали перші у світі носії інформації на папірусі. Із до паперових носіїв інформації Стародавнього Єгипту, крім вирізьблених на камені, до наших днів (завдяки археологічним розкопкам) також дійшли різні за розмірами дерев'яні та металеві таблички. Окремі з них – із дорогоцінних металів, зокрема золота[2].

Аналіз стану охорони державної таємниці у Стародавньому Єгипті дає підстави виділити три основні види таємної інформації, яка охоронялася. Першим, найважливішим, видом таємної інформації стародавніх єгиптян були відомості, що стосувалися життєдіяльності самих фараонів, їх спадкоємців і найближчого оточення. Визначивши місце майбутнього захоронення фараона, розпочинали будівництво його усипальниці – піраміди. Перед початком будівництва всі його учасники давали клятву зберігати таємниці, які стануть відомі під час робіт.

Другим за вагомістю видом таємної інформації у стародавніх єгиптян були відомості, пов'язані з діяльністю своїх і ворожих військових формувань, а також дані спостереження за політичним та економічним життям найближчих сусідів. Збереженню військових

таємниць стародавні єгиптяни приділяли особливу увагу. Супроводжуючи фараона у військових походах, жерці готували карти військових дій, збирали інформацію в тилу ворога, опікувались удосконаленням озброєння[1]. При храмах працювали також школи підготовки охоронців, про вправність яких складалися легенди. Методика підготовки охоронців також належала до категорії державної таємниці. У Стародавньому Єгипті вміло шифрувалися й легендувалися місця золотих, алмазних, мідних, залізних копалень.

До третього виду таємної інформації належали відомості, зазначені у стародавніх єгипетських картах руху планет, календарі розливу єдиної водної артерії країни Нілу та у посівних календарях, а також дані про місця гребель і зберігання продовольчих запасів. Під завісою секретності перебували способи вирощування окремих сільськогосподарських культур, деякі з котрих так і не дійшли до наших часів. При стародавніх єгипетських храмах знаходились також таємні лабораторії із виготовлення отрути та наркотичних засобів, котрі використовувались як засоби лікування, так і умертвлення[1]. З метою запобігання нападам грабіжників на торгові каравани, стародавні єгиптяни засекречували їх маршрути і час руху.

Необхідність охорони таємниці у Стародавньому Єгипті зумовлювалась постійним страхом за власне життя. Водночас, варто зазначити, що саме у стародавні часи закладається і розуміння важливості системної охорони державних таємниць, її зразки для наступних історичних періодів.

Література

1. Черезов Е. Секреты древнего Египта: моногр. / Є. Черезов – Черновцы: ЧГУ. – 1974. – 95 с.

2. Хотон Б. Великие тайны и загадки истории / Б. Хотон. – Харьков: Книжный клуб. – 2009. – 414 с.

УДК 340.134: [351.86+004.75]

Доронін І.М.
кандидат юридичних наук, доцент
Науково-дослідний інститутінформатики
і права НАПрН України

ПРАВОВІ ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ РОЗПОДІЛЕНОЇ ОБРОБКИ ДАНИХ ДЛЯ ДЕРЖАВНИХ РЕЄСТРІВ

Використання систем розподіленої обробки даних для вирішення різного роду технічних завдань застосовується досить давно. Перші програми використання потужностей електронно-

обчислювальних машин для проведення спільних обчислень з'явились понад 40 років тому практично одночасно зі створенням комп'ютерних мереж. Розвиток такої технології відбувався паралельно з розвитком технологій побудови і використання комп'ютерних мереж. При цьому особливості існування цих технологій тривалий час не створювали якихось специфічних проблем правового характеру, оскільки суто технічна специфіка завдань, які вирішувались при створенні та експлуатації зазначених систем, не викликала необхідності у відповідному нормативно-правовому регулюванню цієї діяльності.

У подальшому з'явилась технологія розподілених реєстрів (*Distributed Ledger Technology, DLT*). Не вдаючись в технічні деталі, можливо стверджувати, що сутність зазначеної технології полягає у відсутності якогось одного фізичного носія інформації (сервера чи системи серверів), що зберігає усю інформацію, або її частину. Інформація, яка зберігається, перебуває одночасно у всіх учасників системи, при цьому жоден з них не контролює ані усю інформацію, ані якусь критично важливу частину. Звичайно, що існують різні технічні рішення такого завдання. З огляду на критичну важливість для такої системи проблеми захисту інформації перспективними для прикладного використання поза сферою наукових обчислень є системи, які використовують криптографічний захист і конструювання блоків. Зазначена технологія наразі відома як «блокчейн» (від англомовного терміну *block chain* – ланцюг блоків) і використовується насамперед як розподілена система даних, що закладена в основу «криптовалют» (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента), найвідомішою з яких на сьогодні є система «Біткойн».

Попри досить невелику історію використання «криптовалют», з часу впровадження їх вільного обміну на звичайні грошові кошти та введення котирування на деяких валютних біржах, різного роду атаки на систему є постійними. В основному це робиться для викрадання «криптовалют», при цьому такі атаки бувають і успішними у випадках, коли об'єктом є не система або її частина під час функціонування, а конкретний визначений користувач, що «зберігає криптовалюту» (яка так би мовити «існує» тільки у віртуальному вигляді) на власних носіях інформації. Іншою метою атак є намагання встановити контроль над емісією «криптовалют» одного користувача (або групи, що об'єднана змовою). Оскільки в основі системи є розподілення інформації та криптографічний захист усіх транзакцій на усіх етапах система є стійкою за умови, якщо електронно-обчислювальні машини, які складають систему, продовжують роботу. У випадку обігу «криптова-

лют» їх робота зумовлена необхідністю здобування «криптовалюти», яка виробляється внаслідок проведення обчислювальних операцій учасниками усієї системи. Таким чином учасників системи тримає у ній їх власний економічний інтерес.

За останні два роки зазначений вид технологій розподіленої обробки даних став дуже популярним в основному в сфері мас-медіа. З огляду на таку популярність, імідж «блокчейн» став використовуватись у політичних цілях та у рекламній компаній деяких продуктів, у т.ч. ніяк не пов'язаних з цими технологіями. Останній рік інформація про впровадження «блокчейн»-технологій в банківську сферу з'являється постійно, розповсюджується пі-ар службами відомих банків і усіляким чином просувається у засобах масової інформації, хоча насправді мова йде про використання інших видів технологій розподіленої обробки даних (GRID, або навіть «хмарні» сервери), оскільки жодна комп'ютерна система банку не буде відкритою для усіх користувачів.

Використання «блокчейн» та інших технологій розподіленої обробки даних для ведення державних реєстрів та у діяльності державних органів визнана перспективною фахівцями з державного стратегічного планування провідних країн світу. В Україні починаючи з 2016 року, у прессі згадувалось принаймні про два проекти застосування технології «блокчейн» саме для ведення різного роду державних реєстрів – проект Фонду інновацій та розвитку спільно з Державною службою України з питань геодезії, картографії та кадастру та спільний проект Державного агентства з питань електронного урядування України і фірми «Bitfury». В обох випадках проекти перебувають на стадії підготовки. Попри досить активну кампанію в ЗМІ саме «блокчейн»-технології ще ніде в світі не реалізовано в рамках біль-менш великого проекту у сфері державних реєстрів. Значна популярність ідеї застосування «блокчейн»-технології для державних реєстрів зумовлена насамперед недовірою суспільства до діяльності державних органів, а також іншими соціальними факторами впливу (медійна популярність теми, недовіра до закритості інформації, лібертаріанські ідеї тощо).

На наш погляд при використанні таких технологій неодмінно слід вирішити ряд проблем загального правового характеру до числа яких слід віднести: - питання відповідальності держави за функціонування системи (у випадку класичної «блокчейн»-технології ніхто не контролює всю систему), - питання стимулів для підтримки функціонування системи користувачами (у випадку «криптовалют» таким стимулом є економічний); - питання захищеності інформації (насамперед від втрати та спотворення). У будь-якому разі впрова-

дження технологій розподіленої обробки даних для потреб управління державою потребуватиме значного оновлення законодавства і вирішення дуже серйозних правових проблем.

УДК 94 /930.85

Жевелєва І.С.
Національна академія Служби безпеки України

ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ У КИТАЙСЬКІЙ НАРОДНІЙ РЕСПУБЛІЦІ

Охорона державної таємниці у Китайській Народній Республіці (далі – КНР) регулюється Законом КНР «Про захист державної таємниці» (中华人民共和国保守国家秘密法) від 29.04.2010. Відповідно до ст. 10 цього Закону, державна таємниця (далі – ДТ) у Китаї за ступенем секретності поділяється на три рівні: цілком таємна (绝密); таємна (机密); конфіденційна (秘密).

Цілком таємна інформація – це найважливіша ДТ, розголошення якої може завдати дуже значну шкоду національній безпеці та національним інтересам.

Таємна інформація – це важлива ДТ, розголошення якої може завдати значну шкоду національній безпеці та національним інтересам.

Конфіденційна інформація – це ДТ, розголошення якої може завдати шкоду національній безпеці та національним інтересам [1].

Спеціально уповноваженим органом захисту ДТ є Національна адміністрація по охороні державної таємниці КНР (中共中央保密委员会办公室) – орган державної влади КНР, який відповідає за захист ДТ. Поряд з державним органом із захисту ДТ, в КНР також існує аналогічний партійний орган – Центральний комітет із захисту державної таємниці, що підпорядковується Центральному комітету Комуністичної партії Китаю. В особливих адміністративних районах Китаю – Гонконгу і Макао – діє своя система класифікації та захисту секретної інформації [2].

Особливе місце в Законі відведено врегулюванню питання безпеки ДТ в інформаційних системах. Жодна організація або приватна особа не має права здійснювати наступні дії (в сфері управління інформаційними системами):

- приєднувати комп’ютер або запам’ятовуючий пристрій, що містить секретну інформацію, до інтернету або до інших суспільних інформаційних мереж

Рисунок. Система адміністративних органів, що відповідають за охорону державних таємниць в КНР

- обмінюватися інформаційними повідомленнями між інформаційними системами, пов’язаними з секретністю та інтернетом або іншими громадськими інформаційними мережами, не вживши при цьому заходів захисту

- використовувати несекретні комп’ютери для обробки інформації, що містить державну таємницю

- демонтувати або змінювати захисну програму або програму управління, пов’язану з секретними інформаційними системами, без дозволу

- дарувати, продавати, викидати або змінювати мету використання секретного комп’ютера або пов’язаного з секретністю запам’ятовуючого пристрою, який більше не використовується, і який не оброблявся з використанням технологій безпеки [3].

Відповідно до ст. 25 Закону КНР «Про захист державної таємниці» жодна організація або приватна особа не має права здійснювати наступні дії в сфері управління джерелами секретної інформації:

- нелегально придбавати або зберігати носії секретної інформації

- передавати предмети, що містять державну таємницю через канали, що не мають захисту безпеки

- купувати, продавати, передавати або особисто знищувати які б

то не було носії секретної інформації

- посилати або відправляти поштою предмет, що містить державну таємницю, за межі Китаю

- вивозити або передавати будь-який носій секретної інформації за межі Китаю без дозволу відповідних органів [3]:

Кримінальна відповідальність за порушення законодавства в сфері ДТ в КНР передбачає суворі покарання, включаючи страту.

Література:

1. Law of the People's Republic of China on Guarding State Secrets (2010 Revision). URL: http://en.pkulaw.cn/display.aspx?id=8039&lib=law&SearchKeyword=&SearchCKeyword=

2. State Secrets China's Legal Labyrinth. URL: http://www.lapres.net/statesecrets.pdf.

3. О защите государственной тайны: закон КНР. URL: http://www.asia-business.ru/law/law3/secret/

УДК 351.746

Козій О.М.

Національна академія Служби безпеки України

МОДЕЛІ ОЦІНКИ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ПІДРОЗДІЛУ В УМОВАХ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ

Подібність імовірнісної форми подання показників ефективності запропонована у [1,2] виду

$$E = P(\tau_{(in)} \le \tau_{(\max)}). \qquad (1)$$

та

$$E_{(зіб)} = P\left(\tau_{(зіб)} \le \tau_{(в)}\right), \qquad (2)$$

а також класичної функції розподілу імовірностей має ряд суттєвих переваг, пов'язаних із можливостями застосування методів класичної теорії імовірностей [3] для дослідження інформаційної діяльності підрозділу.

Результатом проведених досліджень, метою якого було вирішення завдання оцінки заходів із забезпечення інформаційної безпеки шляхом комбінування методів імітаційного та аналітичного моделювання, отримані вирази [4] показників виду (1) та (2).

В основу цих аналітичних виразів покладено узагальнену інтегральну формулу виду:

$$P(x \le y) = 1 - P(y < x) = 1 - \int_{0}^{\bar{x}} (z)dz \qquad (3)$$

у якій $\overline{x} - x_{(1)} \circ x_{(2)} = \int_0^\infty y \int_0^\infty f_{(1)}(u-v) f_{(2)}(v) dv du$ (4)

де $f_{(1)}$, $f_{(2)}$ та $f_{(y)}$ – щільності розподілу випадкових величин $x_{(1)}$, $x_{(2)}$ та y відповідно, а знак $\circ$ позначає композицію (згортку) цих випадкових величин.

Разом із тим є ряд обмежень на застосування виразів виду (4) для моделювання інформаційної діяльності підрозділу в умовах виникнення каналів витоку інформації:

1) величина $\overline{x}$ у виразі (4) являє собою середнє значення комбінації не більше двох випадкових величин:

$\overline{x} - x_{(1)} \circ x_{(2)}$,

тоді як величина часу $\tau_{(зіб)}$ забезпечення функцій інформаційної безпеки, що входить у вираз (2) та величина часу $\tau_{(in)}$ реалізації інформаційних процесів у підрозділі, що входить до виразу (1) є комбінаціями більше двох випадкових величин;

2) випадкові величини $x_{(1)}$ та $x_{(2)}$ можуть апроксимуватися рівномірним, експоненціальним або нормальним законом розподілу;

3)випадкова величина y апроксимується експонентним законом розподілу.

Аналіз можливості застосування наведених виразів при вирішенні завдань оцінки ефективності заходів із забезпечення інформаційної безпеки дозволив з урахуванням розглянутих обмежень сформулювати наступні положення.

Положення 1. Обмеження 3 є прийнятним для використання виразу (3) із метою визначення показників виду (1) та (2). Це забезпечується за рахунок того, що вхідна у виразу (1) та (2) величина y, що інтерпретує критичний час реалізації процесів у складних системах, з достатнім ступенем достовірності апроксимується експоненціальним законом розподілу.

Положення 2. Обмеження 1 не є істотним, оскільки число випадкових величин, що входять до виразів (1) та (2) перевищує чотири. Враховуючи це для знаходження композиції випадкових величин можливо застосовувати центральну граничну теорему теорії імовірностей і апроксимувати композицію нормальним законом розподілу імовірностей. Отже обмеження 2 втрачає сенс.

Враховуючи викладене, представимо вираз для визначення середнього значення часу $\tau_{(in)}$ реалізації інформаційних процесів у підрозділі у вигляді:

$$\bar{\tau}_{(in)} = \frac{\sum_{m=1}^{M} p_m \tau_m^{(nin)}}{M} \qquad (5)$$

де $\tau_i^{(nin)}$ – реалізація процедури інформаційного процесу, а p_i - імовірність виконання *i*-ої, $i = 1,2,...,|A|$ процедури інформаційного процесу, що обумовлена наступним правилом:
формується множина:

$$W = \{w_k, |k = 1,2,...,|W||\}$$

елементів матриці порядку проходження процедур $\|Q\|$, позначення яких відповідає позначенню *i*-ої процедури;

2)

кожному елементу $w_k, k = 1,2,...,|W|$ множини W ставиться у відповідність елемент матриці імовірностей переходів $|P|$, який має ті ж координати (номер рядку і номер стовпця), що й елемент $w_k, k = 1,2,...,|W|$.

Отримана множина імовірностей $p_k, k = 1,2,...,|W|$ відповідає ймовірностям переходів на *i*-ту процедуру.

3) Значення p_i визначається за формулою:

$$p_i = 1 - \prod_{k-1}^{|W|} (1 - p_k)$$

Вираз для визначення середнього значення часу $\tau_{(зіб)}$ забезпечення функцій інформаційної безпеки у підрозділі представляється у вигляді:

$$\bar{\tau}_{(зіб)} = \frac{\sum_{i=1}^{I} \tau_i^{(зіб)}}{I} \qquad (6)$$

Базуючись на сформульованому раніше Положенні 2, узагальнена інтегральна форма (3) для визначення показників виду (1) та (2) представляється у вигляді:

$$E = P(x \le y) = 1 - P(y - x) = \exp\left(-\frac{x - y_{\min}}{y}\right) \qquad (7)$$

У випадку застосування виразу (7) для оцінки показника виду (1) змінна *x* відповідає середньому значенню $\bar{\tau}_{(in)}$ часу реалізації інформаційних процесів у підрозділі, змінна *y* – середньому значенню $\bar{\tau}_{(\max)}$ максимального часу реалізації інформаційних процесів у підрозділі, а $y_{(\min)}$ – його мінімальному значенню $\tau_{(\max)\min}$.

Якщо вираз (7) застосовується для оцінки показника виду (2) змінна *x* відповідає середньому значенню $\bar{\tau}_{(зіб)}$ часу реалізації процедур забезпечення інформаційної безпеки підрозділу, змінна *y* – се-

редньому значенню $\bar{\tau}^{(c)}_{(кві)}$ часу існування каналу витоку інформації, а $y_{(\min)}$ – його мінімальне значення $\tau^{(c)}_{(кві)\min}$.

Література

1. Оценка информационной безопасности телекоммуникационных систем: учебное пособие для системы высшего профессионального образования МВД России / [Заряев А. В., Асяев П. И., Обухов А. Н. и др.]. – Воронеж: Воронежский институт МВД России, 2003. – 91с.

2. Основные направления совершенствования методологии оценки защищенности информационно-телекоммуникационных систем от угроз их информационной безопасности. / [Пеньшин И. В., Дмитриев Ю. В., Сушков П. Ф. и др.]. // Информация и безопасность: Материалы межрегиональной научно-практ. конф. – Информация и безопасность. – Выпуск 2. – Воронеж: ВГТУ, 2002. - С. 103-105.

3. Теорія ймовірностей та математична статистика. [5-те видання]. – Київ: Центр учбової літератури, 2010. – 424 с.

4. Вероятностная модель алгоритма расчета показателя эффективности систем информационной безопасности. / Джоган В. К., Думчев В. Н., Здольник В. В.// Вестник ТГТУ. 2008. Том 14. №2 – С. 71 – 276.

УДК 342.951 : 351/354

Корж І.Ф.
доктор юридичних наук,
старший науковий співробітник
Науково-дослідний інститут інформатики
і права НАПрН України

ПРАВОВІ ПРОБЛЕМИ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Держава прагне до найбільш раціонального використання потенціалу суспільства у процесі розв’язання проблем, що виникають як усередині держави, так і за її межами. Сучасна доба характеризується прагненням світу до відкритості економічних, культурних, наукових зв’язків на основі новітніх інформаційно-комунікаційних технологій. За таких умов дедалі більше зростає значення інформації, що становить державну таємницю.

В усі часи найважливішим завданням держави була охорона державної таємниці. В інтересах охорони державної таємниці в Україні встановлена загальнодержавна система організаційно-правових, інженерно-технічних, криптографічних та оперативних заходів, спрямованих на запобігання захисту інформації.

На сьогодні наукові розвідки в основному обмежуються дослідженням окремих аспектів у сфері законодавства про державну таєм-

мницю – як складну систему, як сукупність взаємозумовлених елементів. Водночас на сьогодні недостатня, на нашу думку, увага приділяється розробці та втіленню в життя нормативних документів, що регламентують діяльність, пов'язану безпосередньо з державною таємницею, враховують сучасну геополітичну, політико-правову, соціальну та релігійну ситуації, які склалися як в Україні, так і навколо неї, технологічні досягнення, тенденції щодо ускладнення соціального життя тощо.

З огляду на зазначене, існує нагальна необхідність у напрацюванні нового законопроекту про державну таємницю, в якому б враховувалися зазначені вище критерії.

Насамперед, потребує уточнення саме визначення поняття «державна таємниця», розкриття якого б відповідало вимогам сьогодення. Зазначимо, що результати наукових досягнень дозволяють поставити на один щабель не лише відповідну обмежену інформацію, а й самі її носії (матеріальні носії), яким теж можуть надаватися статус «державної таємниці». Таким, наприклад, є система радіолокаційного розпізнавання «свій» - «чужий», тобто апаратно-програмний технічний комплекс для автоматичного розрізнення своїх військ і озброєнь від ворожих (літаки, підлодки тощо). Крім того, на практиці є непоодинокі випадки, коли людина теж є як носієм відповідних секретів, так і сама по собі є засекреченим суб'єктом, тобто є державною таємницею.

Нинішнє законодавство до «державно таємниці» відносить «вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою» [1]. Це при тому, що Закон України «Про основи національної безпеки» [2] передбачає більш ширший діапазон наявних сфер, де може бути застосовано термін «державна таємниця», включаючи інформаційну сферу. Таким чином, зазначений термін має бути переглянутий і наповнений сучасним змістом.

Наступна проблема, пов'язана із «державною таємницею», – це питання ефективності функціонування такого інституту «державної таємниці», як допуск до державної таємниці за посадою, що передбачено частиною шостою статті 27 Закону [1].

Як вже зазначалося, коли чинний нині Закон приймався парламентом, то його розробниками не припускалося існування такої ситуації, що нині склалася в Україні, коли відверті антидержавники, які здійснювали підривну діяльність, і навіть відверті іноземні агенти будуть працювати у державній владі. Показовою у цьому відношенні є поведінка колишнього депутата України 3-го скликання Коновалюка В. І., коли ним в залі засідань парламенту публічно бу-

ли розкриті секретні матеріали співробітництва України і Грузії у воєнній сфері, з якими він ознайомився і непомітно зняв на телефон. При цьому ним, з метою розкриття і поширення даного документу у суспільстві, було завуальовано гриф «таємно» документа, з яким він попередньо працював. За зазначені дії його не було притягнуто до відповідальності, як це передбачено законодавством. Тим самим було знівельовано дію правового принципу невідворотності відповідальності за вчинений злочин. Можна і інші навести подібні факти. Тому є очевидним, що існує нагальна необхідність в перегляді змісту зазначеного інституту.

Інше питання, що потребує удосконалення, це питання здійснення належної і своєчасної перевірки документів кандидатів на допуск до державної таємниці, враховуючи той факт, що посади заступників міністрів, згідно із новим Законом України «Про державну службу», як і міністри є політичними, і які, після зміни влади, практично одночасно приступають до виконання службових обов'язків. Як показує практика попередніх років, перевірка таких осіб здійснюється прискорено (під політичним тиском) і з недоліками, що виявляються пізніше.

Таким чином, державна політика щодо державної таємниці є складовою засад внутрішньої та зовнішньої політики, за визначенням ВРУ, тому питання захисту державної таємниці в Україні, на нашу думку, потрібно удосконалити та підняти на той рівень, який би забезпечив нормальні умови її функціонування, сприяв би закриттю можливих каналів витоку секретних відомостей, запобіганню втрати матеріальних носіїв секретної інформації та забезпечував би невідворотність відповідальності за правові порушення.

Література:

1. Про державну таємницю : Закон України від 21 січня 1994 р. // Відомості Верховної Ради України. 1994. № 16. Ст. 93.

2. Про основи національної безпеки : Закон України від 19 червня 2003 р. // Відомості Верховної Ради України. 2003. № 39. Ст. 351.

Михайлов А.А.
Служба безпеки України

ПЕРСПЕКТИВИ РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ

Важливою складовою національної безпеки за наявних зовнішніх та внутрішніх викликів, що активізувалися упродовж останнього часу і становлять загрозу для державного суверенітету і територіальної цілісності країни, є захист інформації.

Передусім зазначене стосується державної таємниці, як виду

інформації, розголошення якої може завдати істотної шкоди національній безпеці України.

Вбачається, що існуюча на сьогодні в державі система охорони та захисту відомостей з обмеженим доступом, яка сформована на основі нормативних актів колишнього СРСР, не повною мірою відповідає сучасним вимогам інформаційної безпеки і потребує суттєвого доопрацювання.

Так, унаслідок відсутності єдиних підходів та уніфікованої системи забезпечення охорони секретної та службової інформації в державних органах, на підприємствах, в установах і організаціях не забезпечується гарантований рівень збереження зазначених відомостей, що може завдати шкоди державі та призвести до порушення конституційних прав і свобод людини і громадянина.

Нагальною є також потреба в адаптації національного законодавства у сфері забезпечення безпеки інформації до загальноприйнятих у країнах ЄС та НАТО норм і стандартів.

Зокрема, результати проведеного аналізу вимог стандартів безпеки інформації країн євроатлантичної спільноти та практики застосування національного законодавства України свідчать про наявність потреби у забезпеченні належного рівня державного контролю за дотриманням нормативних вимог з питань віднесення інформації до службової та її надійного збереження. Також потребують удосконалення процедури віднесення інформації до державної таємниці та її розсекречування у частині функціонування інституту державних експертів з питань таємниць, дозвільний порядок провадження діяльності, пов’язаної з державною таємницею, механізм здійснення перевірки громадян у зв’язку з допуском їх до державної таємниці тощо.

З метою адаптації та гармонізації національного законодавства до стандартів безпеки НАТО та ЄС, відповідно до положень Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 № 287/2015, Службою безпеки України розроблено проект Концепції реформування системи охорони державної таємниці та службової інформації (далі – Концепція). Цей проект було погоджено переважною більшістю заінтересованих державних органів, що безпосередньо відповідають за стан охорони інформації, витік якої може завдати шкоди національним інтересам України (зокрема, Адміністрацією Держспецзв’язку, МВС, Міноборони, Мінінформполітики, Мінекономрозвитку, Мінфіном, Адміністрацією Держприкордонслужби, Нацполіцією, УДО, ДФС, СЗР України, а також Національним інститутом стратегічних досліджень).

Разом з тим, Адміністрацією Президента України та Апаратом Ради національної безпеки і оборони України запропоновано враху-

вати у положеннях проекту Концепції питання, пов'язані із захистом державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації тощо.

Враховуючи, що вирішення таких питань виходить за межі повноважень Служби безпеки України, наразі прийнято рішення щодо продовження роботи з реформування національного законодавства у сфері захисту інформації з обмеженим доступом на площадці Апарату Ради національної безпеки і оборони України.

Втім, наведене стосується перспективного законодавства, тоді як умови сьогодення вказують на необхідність врегулювання окремих проблемних питань вже у короткостроковій перспективі.

Саме тому Службою безпеки України ініційовано внесення змін до Закону України «Про державну таємницю» та Кодексу України про адміністративні правопорушення з метою врегулювання таких питань як:

- розширення переліку підстав для відмови у наданні громадянам допуску до державної таємниці, у разі наявності інформації про їх причетність до діяльності, спрямованої проти національних інтересів та національної безпеки України (загрози посягань на державний суверенітет та територіальну цілісність, прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України, міжнародний тероризм, порушення антикорупційного законодавства, поширення організованої злочинної діяльності);

- унормування порядку виїзду секретоносіїв на територію, особливий правовий режим якої визначається законодавством (запроваджується окрема норма, за якою громадянин, у разі виїзду на територію АР Крим або територію непідконтрольній Україні територію Донецькій та Луганській областей, зобов'язаний письмово повідомити про це керівника, що надав йому доступ до державної таємниці або РСО за місцем провадження ним діяльності, пов'язаної з державною таємницею);

- можливість надання або переоформлення спецдозволу державним органам, підприємствам, установам, організаціям у разі призначення іноземця на керівну посаду, за умови взяття ним письмово зобов'язання щодо збереження державної таємниці та надання йому на підставі відповідного розпорядження Президента України та дозволу Служби безпеки України доступу до державної таємниці;

- удосконалення заходів адміністративного впливу до порушників законодавства про державну таємницю.

Крім того слід зауважити, що наразі у Верховній Раді України за № 6130 зареєстровано законопроект «Про внесення змін до деяких законодавчих актів щодо врегулювання питань організації та

забезпечення охорони державної таємниці», яким, серед іншого, передбачено встановлення юридичної відповідальності за наявність у громадян України громадянства (підданства) іншої держави (держав) та підстав для відмови таким громадянам у наданні допуску, доступу до державної таємниці або його скасування.

Література

1. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII;

2. Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI;

3. Політика безпеки НАТО С-М (2002)49 від 17.06.2002;

4. Правила безпеки для охорони інформації з обмеженим доступом ЄС від 23.09.2013 (2013/48/EU);

5. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015;

6. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 № 47/2017.

УДК 343.3

Олійник В.І.
кандидат юридичних наук
ВНЗ «КРОК»

КРИМІНАЛЬНО-ПРАВОВИЙ ЗАХИСТ ДЕРЖАВНОЇ ТАЄМНИЦІ У ФРАНЦІЇ

Події, що розгортаються в Україні протягом трьох останніх років, змушують по-новому поглянути на захист державної таємниці. Стратегією національної безпеки України визначено, що серед сучасних загроз існують загрози безпеці інформаційних ресурсів, що виражаються у фізичній і моральній застарілості системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1]. Також введено у дію рішення Ради національної безпеки і оборони України «Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій і Луганській областях» [2], все це визначає проблему національного характеру.

Зазначене примушує шукати нових шляхів недопущення витоку таємної інформації, а також досліджувати досвід іноземних держав, аналізуючи як їх позитивний досвід, так і моменти, які стають на заваді. Увагу буде прикуто до кримінально-правового захисту власних секретів Францією – державою, якій, як і Україні, притаманна

континентальна система права.

Як і в Україні тут діють норми кодифікованого кримінального права, що серед іншого регулюють питання захисту державної таємниці.

Отже, у Франції класифікація секретних даних визначена статтею 413-9 Кримінального кодексу [3], зокрема виділяються три рівні:

Très Défense (цілком таємний захист): розголос такої інформації є надзвичайно шкідливим для національної оборони, стосується урядових пріоритетів у національній обороні. Часткове або повне відтворення такої інформації суворо заборонено.

Défense (таємна): розголошення інформації вважається шкідливим для національної оборони. Така інформація не може бути відтворена без дозволу влади, крім виняткових надзвичайних ситуацій.

Confidentiel Défense (конфіденційний захист): розголошення інформації є потенційно шкідливим для національної оборони, або це може привести до розкриття інформації, класифікованої в більш високому рівні безпеки.

Кримінальним кодексом Франції у книзі 4 розділі 1 «Зазіхання на основні інтереси нації» передбачається відповідальність за найтяжчі політичні злочини – зраду і шпигунство. Низка ж статей Кодексу стосується безпосередньо захисту державної таємниці.

Відмітимо, що у Франції застосовується принцип, який полягає в тому, що інформація вважається, насамперед, фактором національної безпеки, а основним критерієм засекречування є критерій «таємниця в галузі національної оборони».

Ст. 413-7 безпосередньо стосується порушення таємниці у сфері національної оборони. Так, шістьма місяцями ув'язнення і штрафом у розмірі 50 тис. франків карається діяння, вчинене в публічних або приватних службах, що мають оборонне значення, і виразилося таке діяння в проникненні без дозволу всередину приміщень або закритих територій, на яких заборонене вільне пересування і які делімітовані для забезпечення охорони установок, техніки або таємниці досліджень, проектних робіт або виробництва [3].

Заслуговує на окрему увагу той факт, що у зазначеній нормі суб’єктами злочину визнаються також і службовці приватного сектору, які часто виконують завдання на замовлення держави. На сьогодні дане питання є актуальним і для України та потребує окремого теоретичного дослідження.

Ст. 413-10 передбачено, що сім'ю роками ув'язнення і штрафом у розмірі 700 тис. франків карається діяння, вчинене будь-якою особою, яка у зв'язку зі своїм становищем або професією, володіє будь-якими відомостями, технологіями, предметами, документами, інформаційними даними або даними картотек, які мають характер таємниці національної оборони, що виразилося в їх знищення, викраденні, вилученні або відтворенні, або в ознайомленні з ними широкого

загалу або окремої особи, яка не має на це права [3]. Так само карається діяння, вчинене особою, що допустила знищення, викрадення, вилучення, відтворення або розголошення відомостей, технологій, предметів, документів, інформаційних даних або даних картотек, зазначених у попередньому абзаці, які перебували в її розпорядженні.

Якщо говорити про систему організації захисту секретної інформації, то, слід зазначити, що вона у Франції досить розгалужена (Генеральний секретаріат національної оборони, Міжміністерський комітет з розвідки у сфері захисту державних секретів, Вища рада оборони, Головне управління зовнішньої безпеки, управління із забезпечення оборонної безпеки, Управління державної безпеки тощо). Вважаємо, що вітчизняному законодавцю слід взяти до уваги низку положень.

Література:

1. Верховна Рада України : сайт. Стратегія національної безпеки України : затверджено Указом Президента України від 26 травня 2015 р. № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». URL: http://zakon5.rada.gov.ua/laws/show/287/2015?nreg=287%2F2015&find=1&text=%F2%E0%BA%EC%ED%E8%F6&x=0&y=0

2. Верховна Рада України: сайт. Указ Президента України від 30 березня 2015 р. № 184/2015 Про рішення Ради національної безпеки і оборони України від 12 березня 2015 року «Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях» URL: http://zakon0.rada.gov.ua/laws/show/184/ 2015

3. Уголовный кодекс Франции / науч. ред. Л.В. Головко, Н Е. Крыловой; [перевод с французского и предисловие Н. Е. Крыловой] – СПб. : Издательство «Юридический центр Пресс», 2002. - 650 с.

Павлюк І.С.
Житомирський військовий інститут
імені С. П. Корольова

ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В ОСОБЛИВИХ УМОВАХ

В умовах російської агресії, ведення нею гібридної війни проти України перед нашою державою постав цілий ряд серйозних викликів і загроз. Особливої актуальності набуло питання захисту інформації.

В Україні розроблено та застосовується ряд нормативно-

правових документів, які регламентують забезпечення охорони інформації, що є власністю держави, в тому числі і такої, що становить державну таємницю, але значна їх частина потребує доопрацювання та вдосконалення враховуючи сучасні умови.

Законом України “Про державну таємницю” визначено, що охорона державної таємниці - це комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

Пропонується звернути увагу на організаційно-правові заходи забезпечення охорони державної таємниці, які пов’язані зі певними труднощами їх реалізації військовими частинами Збройних Сил України та іншими військовими формуваннями держави, які здійснюють режимно-секретну діяльність в особливих умовах. Під особливими умовами слід розуміти умови, які суттєво відрізняються від повсякденних, в тому числі, - ведення бойових дій в зоні проведення антитерористичної операції на території Донецької та Луганської областей.

Проблемними питаннями охорони державної таємниці в особливих умовах, що потребують нормативно-правового врегулювання, є:

- отримання, переоформлення або поновлення дії дозволу на провадження діяльності, пов’язаної з держаною таємницею;
- погодження призначення осіб на посади начальників режимно-секретних органів та їх заступників з органами Служби безпеки України;
- оформлення (переоформлення) та надання військовослужбовцям допуску до державної таємниці;
- невизначеність особливостей виготовлення, користування, збереження, передачі та обліку матеріальних носіїв секретної інформації;
- невизначеність особливостей забезпечення вимог режиму секретності;
- не в повній мірі визначено особливості організації та здійснення технічного захисту інформації.

Чітке нормативно-правове врегулювання питань забезпечення охорони державної таємниці в особливих умовах дозволить значно підвищити результативність та ефективність заходів у відповідному сегменті національної безпеки України.

УДК 35.072.6:351.746.1 (477)

Романенко І.В.
кандидат юридичних наук
Національна академія Служби безпеки України

ДОПУСК ДО ДЕРЖАВНОЇ ТАЄМНИЦІ ЯК ПРАВОВИЙ ІНСТИТУТ

Сучасний стан вітчизняного законодавства характеризується активним розвитком. Мова йде не лише про вдосконалення правових норм, їх перебудови, але й про формування багатьох нових правових інститутів, що відповідають критеріям правової держави, міжнародним стандартам захисту прав і свобод людини і громадянина. Правовий інститут об’єднує різні правові норми задля включення їх у механізм правового регулювання конкретних видів суспільних відносин. На сьогодні, в системі забезпечення охорони державної таємниці можна стверджувати про виокремлення такого правового інституту як інститут допуску до державної таємниці.

Юридична енциклопедія визначає інститут права як групу взаємопов’язаних юридичних норм, що регулюють окремий вид суспільних відносин; елемент системи права [1, 701,702]. Державна таємниця невід'ємно пов'язується з існуванням правових норм, що регулюють суспільні відносини з приводу надання, переоформлення та скасування допуску до державної таємниці (далі також – допуск). Ці норми, хоча і закріплені у різних нормативних актах, але регулюють один вид суспільних правовідносин – правовідносини з приводу ознайомлення та провадження діяльності, пов’язаної з державною таємницею фізичними особами. Все зазначене вище дозволяє говорити про існування інституту допуску до державної таємниці як правового інституту. Його головне завдання, як і будь-якого інституту права – забезпечити суцільне, відносно закінчене регулювання відповідних суспільних відносин.

Такі правовідносини мають певну структуру і складаються з об’єкту (те, з приводу чого виникає і здійснюється діяльність суб'єктів), суб'єктів (сукупність осіб, які беруть участь у правовідносинах), змісту (суб’єктивні права, юридичні обов’язки, повноваження, юридична відповідальність) та юридичних фактів (підстав виникнення, зміни і припинення правовідносин).

Об’єктом правовідносин, що розглядаються, є самостійна система яка включає порядок надання, переоформлення та скасування особі права на ознайомлення та провадження діяльності, пов’язаної з державною таємницею.

Суб’єктами, виходячи зі змісту Закону України "Про державну таємницю"[2], - є органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховна Рада Автономної Республіки Крим, Рада міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, громадські об'єднання (далі – органи державної влади, органи місцевого самоврядування, підприємства, установи та організації), громадяни України, іноземці та особи без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Змістом правовідносин є: компетенція органів державної влади, місцевого самоврядування, підприємств, установ та організацій усіх форм власності, громадських об'єднань; права й обов’язки громадян України, яким надано допуск до державної таємниці, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Таким чином, *інститут допуску до державної таємниці* – це група взаємопов’язаних правових норм у сфері забезпечення охорони державної таємниці, що регулюють порядок надання, переоформлення та скасування особі права на ознайомлення та провадження діяльності, пов’язаної з державною таємницею. Особливий правовий режим такого допуску формується з метою захисту національної безпеки.

Характерним для конкретного інституту права є його функціонування на основі певних, властивих лише даному інституту принципів: максимального обмеження кількості осіб, яким надається право провадження діяльності, пов’язаної з державною таємницею; принцип добровільності; прийняття додаткових зобов’язань; збільшення відповідальності; недопущення осіб, які можуть завдати шкоди охороні державної таємниці; обмеження ознайомлення.

Розглянуті принципи не діють ізольовано, вони доповнюють загальні принципи правового регулювання сфери охорони державної таємниці, до яких належать: принцип законності, принцип пріоритету міжнародного права над національним, принцип забезпечення прав та інтересів фізичних та юридичних осіб, діяльність яких пов’язана з державною таємницею, принцип взаємної відповідальності держави та особистості; принцип економічної доцільності.

За результатами запропоновано визначення інституту допуску до державної таємниці як групи взаємопов’язаних правових норм у сфері забезпечення охорони державної таємниці, що регулюють порядок надання, переоформлення та скасування особі права на ознайомлення та провадження діяльності, пов’язаної з державною таєм-

ницею з метою захисту національної безпеки, а також розкрито основні принципи та структуру цього інституту.

Література

1. Юридична енциклопедія: В 6 т. /[Редкол.: Ю.С.Шемшученко та ін.] –К.: "Українська енциклопедія", 2001. – Т.2. – С. 701-702.

2. Закон України "Про державну таємницю" від 21.01.1994 р. № 3855-XII. URL: http://zakon.rada.gov.ua/laws/show/3855-12/

Семенюк О.Г.
кандидат юридичних наук
Служба безпеки України

ЩОДО НЕОБХІДНОСТІ ЗМІН У ПІДХОДАХ ДО КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

1. Вперше кримінальна відповідальність за «листування з ворогом і повідомлення йому відомостей, які б могли завдати шкоди державі» була встановлена Третім статутом князівства Литовського у 1588 році. З часів потрапляння української держави під вплив Московського царства (середина XVII ст.) кримінально-правові норми, що встановлювали відповідальність за державну зраду, шпигунство, розголошення державної і військової таємниці, а також втрату їх матеріальних носіїв, здобули собі постійну «прописку» серед так званих політичних злочинів та стали дієвим інструментом у ліквідації або, щонайменше, ізоляції інакодумців та інших потенційних супротивників правлячому режиму. В послідуючому зазначені кримінально-правові норми були використані в якості зразка для наслідування радянською правовою системою та активно використовувалися при розправі зі своїми політичними супротивниками.

2. Завершення формування діючої на даний час системи кримінальних заборон у сфері охорони державної таємниці відбулося із прийняттям Закону СРСР «Про кримінальну відповідальність за державні злочини» (1958 р.), який остаточно закріпив перелік злочинів у цій сфері та визначив їх структуру як злочинів із формальним складом. У подальшому із незначними змінами у диспозиціях деяких із цих статей, всі вони були відтворені у КК УРСР (1961 р.) та КК України (2001 р.). На даний час до них належать статті 111, 114, 328, 329, 422 КК України.

3. Комплексний аналіз теорій про об’єкт злочину та диспозицій статей 111, 114, 328, 329, 422 КК України доводить, що безпосереднім об’єктом цих злочинів, є умови безпечного існування людини,

суспільства та держави. Додатковий факультативний злочинів, передбачених статтями 111, 114, 328 (ч. 1), 329 (ч. 1), 422 (ч. 1 та ч. 2) КК України, є територіальна цілісність та недоторканість України, її суверенітет, політична та економічна незалежність, бойова готовність Збройних Сил та інших військових формувань, життя, здоров'я та гідність людини, майно або інші цінності. Для злочинів, передбачених статтями 328 (ч. 2), 329 (ч. 2), 422 (ч. 3) КК України, зазначені наслідки становлять додатковий обов'язковий об'єкт.

4. Відсутність єдиної методики оцінювання можливої шкоди внаслідок несанкціонованого витоку інформації, що підлягає експертизі на предмет наявності чи відсутності в ній державної таємниці, призводить до того, що рішення державних експертів з питань таємниць за результатами проведення таких експертиз носять суб'єктивний характер, а унормована на даний час процедура їх проведення унеможливлює винесення об'єктивних, достовірних та науково-обґрунтованих висновків з цього питання та, як наслідок, винесення обґрунтованих судових рішень при розгляді кримінальних справ.

5. Жодним нормативним актом у сфері охорони державної таємниці не передбачено таке поняття, як відомості військового характеру, що становлять державну таємницю, тому ст. 422 КК України, яка встановлює кримінальну відповідальність за розголошення такої інформації або втрату її матеріальних носіїв, має бути декриміналізована – такі діяння не можуть бути вчинені в зв'язку з відсутністю предмета цього злочину.

6. Конструювання диспозицій статей 111, 114, 328 (ч. 1), 329 (ч. 1), 422 (ч. 1 та ч. 2) КК України як формальних складів злочинів, відповідно до яких кримінальна відповідальність наступає лише за створення достатніх умов для завдання шкоди територіальній цілісності та недоторканості України, її суверенітету, політичній та економічній незалежності, бойовій готовності Збройних Сил та інших військових формувань, життю, здоров'ю та гідності людини, майну або іншим цінностям у результаті потрапляння державної таємниці до сторонніх осіб або тимчасового виходу такої інформації з володіння особи, якій вона була довірена, суперечить загальному принципу криміналізації тільки суспільно небезпечних діянь (таких, що заподіюють або створюють реальну загрозу заподіяння шкоди об'єктам кримінально-правової охорони). Тому ці злочини мають бути не з формальним, а з матеріальним складом, оскільки лише настання суспільно небезпечних наслідків у вигляді визначеної та закріпленої законодавцем у диспозиції цих статей шкоди особі, суспільству чи державі можуть бути підставою криміналізації таких діянь. Крім цього, залишення законодавцем суспільно небезпечних

наслідків за межами складу цих злочинів, а отже за межами свідомості особи, унеможливлює з'ясування ставлення до них та, відповідно, встановлення наявності чи відсутності вини у її діях.

7. З урахуванням появи нових загроз у сфері охорони державної таємниці, які полягають у розширенні переліку осіб, зацікавлених у протиправному заволодінні секретною інформацією, необхідно відмовитися від закріплення у диспозиції статті, що передбачає відповідальність за шпигунство, визначення спеціального адресата такої інформації (іноземна держава, іноземна організація або їх представники) та встановити відповідальність за протиправне заволодіння державною таємницею незалежно від того, хто є виконавцем, замовником або кінцевим адресатом такої інформації.

8. Предметом державної зради у формі шпигунства (ч. 1 ст. 111 КК) та шпигунства (ст. 114 КК) є відомості, що становлять державну таємницю. Оскільки така інформація охороняється державою та не знаходиться у вільному обігу, її неможливо зібрати, тобто отримати доступ до неї без порушення встановлених правил поводження з секретною інформацією. Тому кримінальна відповідальність має наступати не за збирання, а за протиправне заволодіння відомостями, що становлять державну таємницю.

9. З метою оптимізації кримінального законодавства та використання для опису протиправних дій таких понять, які за своїм змістом більш точно відображають характер події, що пов'язується саме з витоком таємної інформації, необхідно відмовитися від одночасного застосування у Кримінальному кодексі України понять «передача» та «розголошення» відомостей, що становлять державну таємницю, та залишити у законодавчому обігу тільки поняття «розголошення» відомостей, що становлять державну таємницю. За таких умов, об'єктивну сторону шпигунства мають становити дії, які полягають лише у протиправному заволодінні державною таємницею, оскільки Кримінальний кодекс вже містить окрему статтю за розголошення державної таємниці.

10. Визначальною суб'єктивною ознакою суспільної небезпечності розголошення відомостей, що становлять державну таємницю, та втрати її матеріальних носіїв має бути не усвідомлення секретоносієм неминучості чи можливості несанкціонованого витоку секретної інформації внаслідок умисного або необережного порушення встановлених правил поводження з державною таємницею, а усвідомлення чи можливість передбачення завдання шкоди особі, суспільству чи державі внаслідок несанкціонованого витоку такої інформації.

11. Подальше залишення у диспозиції цієї статті спеціальної мети, яка не має певного юридичного наповнення для правильної

кваліфікації кожного конкретного випадку, та ігнорування правозастосовцями положення щодо обов'язковості її доведення, дає широкий простір для вільного тлумачення цього поняття, відкриває можливості до свавілля та порушення прав людини. Крім цього, конституційний принцип рівності всіх громадян перед законом вимагає відмови від законодавчого розмежування відповідальності за державну зраду у формі шпигунства (ч. 1 ст. 111 КК) та шпигунство (ст. 114 КК) за ознаками громадянства при повній ідентичності об'єктивної сторони цих злочинів.

12. Кримінальна відповідальність повинна наступати не за державну зраду у формі шпигунства, а за розголошення державної таємниці (для секретоносіїв) або/та протиправне заволодіння державною таємницею (для осіб, які не мають доступу до державної таємниці) не залежно від їх громадянства. При цьому мета цих протиправних діянь (користь або завдання шкоди особі, суспільству чи державі) може розглядатися виключно як обтяжуюча вину обставина, а не обов'язковий елемент складу злочину.

13. З метою приведення закріплених на даний час у диспозиції статей 328 та 329 КК ознак спеціального суб'єкта цих злочинів у відповідність до змін, що відбулися у законодавстві про охорону державної таємниці, а також враховуючи, що підстави та порядок отримання доступу до секретної інформації можуть із часом змінюватися, необхідно закріпити більш універсальне поняття суб'єкта цих злочинів, а саме: «особа, якій ці відомості були довірені або стали відомі в порядку, передбаченому законодавством».

14. Суспільну небезпеку розголошення секретної інформації або втрати її матеріальних носіїв становлять не лише дії осіб, яким ці відомості були довірені або стали відомі в порядку, передбаченому законодавством, а також дії осіб, які отримали доступ до такої інформації випадково або навмисно заволоділи нею у протиправний спосіб, та усвідомлювали, що такі відомості становлять секретну інформацію. Тому перелік суб'єктів кримінальної відповідальності за розголошення державної таємниці або втрату її матеріальних носіїв має бути розширений за рахунок включення до нього також осіб, які отримали доступ до секретної інформації у протиправний спосіб та усвідомлювали, що ці відомості становлять державну таємницю.

15. З урахуванням конституційного гарантування державою безпеки особистості, суспільства та держави, а також з метою формування єдиного механізму кримінально-правового захисту різних видів таємної інформації пропонується обрати в якості узагальнюючого об'єкта кримінально-правової охорони таке поняття, як «чужа таємниця», що охоплює таємницю фізичної особи, комерційну та держав-

ну таємниці. За цих умов, а також з урахуванням зроблених висновків щодо необхідності вдосконалення кримінально-правових норм у сфері охорони державної таємниці, кримінальна відповідальність за порушення порядку поводження з інформацією, несанкціонований витік якої може завдати шкоди особі, суспільству або державі, має наступати за вчинення таких злочинів, як «Протиправне заволодіння чужою таємницею», «Розголошення чужої таємниці», «Втрата матеріальних носіїв інформації, що містять чужу таємницю».

16. Кримінальна відповідальність за розголошення чужої таємниці та втрату її матеріальних носіїв має наставати лише у випадку завдання шкоди особі, суспільству чи державі. За відсутності таких злочинних наслідків та доведеного умислу на їх завдання, зазначені діяння повинні вважатися кримінальним проступком і кваліфікуватися як умисне або необережне порушення правил поводження з чужою таємницею, яке призвело до витоку такої інформації.

УДК 65.012.8 (477)

Сидоренко С.М.
Національна академія Служби безпеки України

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ЛАТВІЙСЬКОЇ РЕСПУБЛІКИ

Законодавство Латвійської Республіки про державні таємниці ґрунтується на базовому Законі про державну таємницю від 1 січня 1997 року зі змінами від 26 лютого 2004 року, а також – на нормативних актах, прийнятих на рівні Уряду Латвійської Республіки, оскільки будь-які питання не врегульовані законом, визначаються виключно нормативно-правовими актами Уряду (постанови Кабінету Міністрів від 25 червня 1997 р. № 225 «Положення про охорону державної таємниці» і від 25 червня 1997 р. № 226 «Перелік відомостей, що складають державну таємницю») [3, 4, 5].

Організаційно-правові засади охорони державної таємниці Латвійської Республіки включають формулювання поняття державної таємниці та встановлення порядку зберігання, використання та організації захисту даних, які складають державну таємницю. Зокрема, стаття 2 Закону Латвії про державну таємницю містить пункт, який визначає, що положення про державну таємницю у повній мірі розповсюджуються на засекречені відомості Організації Північноатлантичного договору (НАТО), Європейського союзу, іноземних та міжнародних організацій і структур, якщо це не передбачено іншими нормативними актами [3, с.11].

За ступенями секретності відомостей, що складають державну таємницю латвійське законодавство про державну таємницю здійснює поділ таким же чином як і українське законодавство: «особливої важливості», «цілком таємно» і «таємно» [3, с.4]..

За дотримання режиму секретності і забезпечення захисту державної таємниці в державних органах відповідають в межах своєї компетенції керівники цих органів або їх відповідних структурних підрозділів. Дані посадові особи відповідають за те, аби їх підлеглим, робота (служба) яких пов'язана з відомостями, що складають державну таємницю, були створені відповідні умови для такої роботи у відповідності з постановами Кабінету Міністрів. За заявою керівника відповідного органу для забезпечення режиму секретності можуть бути залучені співробітники органів державної безпеки [3, с. 3].

Порядок отримання, передачі і використання засекречених (особливої важливості, цілком таємних і таємних) відомостей іноземних держав, міжнародних організацій і їх структур регламентується постановами Кабінету Міністрів.

Органом національної безпеки Латвійської Республіки, який здійснює і контролює обмін засекреченими відомостями з іноземними державами, міжнародними організаціями і їх структурами, а також приймає заходи по захисту такого роду відомостей є Бюро по захисту Конституції Латвійської Республіки [2, с. 7].

Доступ до відомостей, що складають державну таємницю, дозволяється особам, які відповідно до своїх посадових (службових) обов'язків або конкретного робочого (службового) завдання повинні виконувати роботу, пов'язану з використанням або захистом відомостей, що складають державну таємницю, і які відповідно до Закону, отримали допуск до державної таємниці. Перевірочні заходи по відношенню до таких осіб проводяться до початку трудових (службових) відносин з ними.

Особливістю латвійського законодавства щодо оформлення допуску до державної таємниці є питання, пов’язані з тим, що рішення про відмову в допуску може бути оскаржене у директора Бюро по захисту Конституції протягом 10 днів з моменту, коли відповідна особа дізналася про таке рішення. При цьому, рішення Генерального прокурора є остаточним і оскарженню не підлягає [2, с. 5].

Література

1. Конституція Латвійської Республіки зі змінами та доповненнями, проголошеними 17 травня 2007 року. URL: www.ves.lv.

2. Закон Латвійської Республіки «Про національну безпеку», ухвалений 14 грудня 2000 року, зі змінами та доповненнями від 11 травня 2005 року. URL: www. ves.lv.

3. Закон Латвійської Республіки «Про державну таємницю» від 1 січня 1997 року, зі змінами та доповненнями від 26 лютого 2004 року. URL: www. ves.lv.

4. Постанова Уряду Латвійської Республіки від 25 червня 1997 року № 225 «Про затвердження Положення про охорону державної таємниці». URL: www. ves.lv.

5. Постанова Уряду Латвійської Республіки від 25 червня 1997 року № 226 «Про затвердження переліку носіїв, що складають державну таємницю». URL: www. ves.lv.

УДК 654.02

Скіцько О.І.
кандидат технічних наук,
старший науковий співробітник
Національна академія Служби безпеки України

ДЕЯКІ АСПЕКТИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МОБІЛЬНИХ ПРИСТРОЇВ В МЕРЕЖІ

Мобільні пристрої змінила життя сучасних людей та намітили нові напрямки розвитку інформаційних технологій. Завдяки їм сьогодні немає необхідності знаходитись на робочому місці, чи переїжджати з міста в місто для обговорення важливих робочих питань. Використання сучасних мобільних пристроїв – в основному смартфонів та планшетів – дозволило отримувати віддалений доступ до даних та пошти, спілкуватись на відстані у реальному часі та зберігати інформацію на віртуальних носіях. В той же час застосування мобільних пристроїв і технології хмарних обчислень висуває підвищені вимоги до їх безпеки, збереження і захисту даних, у тому числі від несанкціонованого розповсюдження цієї інформації. При використанні технології хмарних обчислень за моделлю на віддаленому сервері і центрах обчислення даних "спеціалізованого" провайдера зберігається критично важлива для компанії інформація, наприклад "звіт". Працівники, що мають доступ до неї можуть дублювати її на своїх персональних мобільних пристроях, що в свою чергу знижує рівень інформаційної безпеки. У цьому випадку потрібно передбачити заходи щодо захисту або знищення цих даних при втраті або крадіжці мобільного пристрою. Також до катастрофічних наслідків може призвести передача інформації по незахищених каналах зв'язку. В основному проблемами захисту мобільних пристроїв займаються виробники, що користуються базовими засобами

захисту, які передбачені в сучасних операційних системах, таких як iOS, Android, Windows Phone. Поряд з SMS-троянськими програмами особливу небезпеку для користувачів представляють DDoS-атаки. Зросли як їх число, так і потужність. Основну групу ризику в нашій країні складають компанії нафтогазової галузі, енергетики, а також сектори "спеціалізованого" машинобудування та інжинірингу, фінансовий сектор [1].

Мобільні засоби часто є об'єктами крадіжки і зараження шкідливими програмами з метою викрадення грошових коштів або цінної інформації, здійснення хакерських атак, спрямованих на нанесення економічної чи моральної шкоди. Щоб захиститися від таких загроз, недостатньо антивірусних програм, що встановлюються на мобільні пристрої. Убезпечити може тільки комплексна система управління інформаційною безпекою.

Для захисту трафіку мобільних пристроїв потрібно користуватись послугою оператора зв'язку віртуальної приватної мережі (VPN). У цьому випадку весь трафік мобільних пристроїв передається по закритих каналах оператора зв'язку і не потрапляє в Інтернет, що виключає ризик перехоплення зловмисниками.

Для мобільних користувачів інформаційна безпека забезпечується:

- готовими рішеннями, які встановлюються на мобільний апарат, щоб обмежити можливість витоку інформації;
- засобами, що надають захищену взаємодію співробітників компанії;
- засобами, що дозволяють реалізувати віртуальне робоче місце на мобільному терміналі з можливістю централізованого управління його безпекою;
- ефективним застосуванням вже існуючих сертифікованих засобів захисту.

За статистикою в світі викрадають в середньому 1 лептоп кожні 53 секунди. Тому набирає популярність тенденція (Bring Your Own Device – BYOD) – «принеси свій власний пристрій», що дає співробітникам свободу у виборі власних засобів телекомунікації. Дана концепція відповідає на питання «що робити з особистими мобільними пристроями співробітників при їх використанні» [1].

У випадку використання пристрою, що належить співробітнику, в робочих цілях виникає ряд питань, що стосуються конфіденційності користувача, контроль пристрою, порядку використання пристрою, політик безпеки та захисту даних, відповідь на які дозволить забезпечити захищеність даних.

У зв’язку з цим пропонуються деякі загальні правила захисту

мобільних пристроїв [2, 3]:

1. Блокування пристрою.

У разі втрати мобільного пристрою необхідно блокувати пристрій паролем (стійким або з обмеженою кількістю спроб введення), після яких дані на пристрої стираються або пристрій блокується.

2. Використання криптографічних засобів.

Необхідно використовувати шифрування змінних та вбудованих карт пам'яті – всього, до чого може отримати доступ зловмисник.

3. Заборона на збереження паролів в браузері мобільного пристрою.

4. Заборона використання менеджерів паролів для облікових записів.

5. Заборона на установку програмного забезпечення з неперевірених джерел.

6. Використання політик захисту та засобів антивірусного захисту.

7. Обмежити список даних, які можна передавати через хмарні сервіси.

Також не потрібно забувати про Mobile Device Management (MDM) – «управління мобільними пристроями». Використання рішень класу MDM дозволяє здійснити управління і контроль над різними типами мобільних пристроїв. MDM – це технологія управління всіма мобільними пристроями, а технологія BYOD – орієнтована на специфіку управління пристроями співробітників в корпоративному середовищі. BYOD ближче до тактичного і в деяких аспектах стратегічного рівня управління інформаційними технологіями та інформаційною безпекою, тоді як MDM передбачає прикладну технічну реалізацію, і знаходиться скоріше на операційному рівні [4].

Можна зробити висновок, що при сучасному розвитку інформаційних технологій та широкому використанні мобільних пристроїв, вищезазначені рішення дають широкий вибір можливостей по управлінню мобільними пристроями, що використовуються у службовій діяльності. Вони дозволяють керувати доступом до пристрою, синхронізувати передачу та отримання даних, обмежити доступ до інформації, функцій та додатків, надають адміністратору зручний користувацький інтерфейс.

Однак, перш ніж почати впровадження технологій MDM чи BYOD в службову діяльність, треба зрозуміти, від яких загроз доведеться захищатися та оцінити їх. Таким чином, захист від зовнішніх атак повинен здійснюватися комплексно, системи управління інформаційною безпекою мобільних пристроїв повинні складатись з розроблених методів захисту, моделей прийняття рішень, що пов’язані

з запобіганням та виявленням атак в мобільній мережі і відповідною реакцією на них.

Література

1. Жованик М.О. Загальні принципи захисту мобільних пристроїв в корпоративній мережі // «Молодий вчений», № 5 (20), Частина 1. - 2015 р. - С. 39 – 42.

2. Міночкін А.І., Романюк В.А. Безпека мобільних радіомереж // Збірник наукових праць № 5. – К.: ВІТІ НТУУ "КПІ". – 2004. – С. 116 – 126 .

3. Мобільна безпека: Захист мобільних пристроїв в корпоративній мережі. URL: https://xakep.ru/2011/10/13/57058.

4. MDM и BYOD – змішати, але не збовтати. [Електронний ресурс]. - Режим доступу: http://www.volgablob.ru/blog/?p=101

УДК. 340.132.668

Шепета О.В.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

АНАЛІЗ МІЖНАРОДНИХ УГОД УКРАЇНИ ПРО ВЗАЄМНУ ОХОРОНУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Основу сучасних міжнародних відносин у світі складають міжнародні договори. Для кожної держави, зокрема для України, питання договірного оформлення відносин із зовнішнім світом посідає одне з найголовніших місць. Так, одним з перших питань, що виникли після проголошення незалежності України, яка стала повноправним суб'єктом міжнародного права, були угоди про встановлення дипломатичних відносин з іншими країнами зарубіжжя.

Україна як незалежна європейська держава стала повноправним суб'єктом міжнародного спілкування, заявила власну позицію і в міжнародних організаціях, в тому числі шляхом вступу у договірні відносини. Сфера її зовнішньополітичної діяльності стає все більш широкою, наповнюється новим змістом.

Службою безпеки України як спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці, здійснюється діяльність, спрямована на створення правової бази для обміну та взаємного захисту інформації з обмеженим доступом між Україною та країнами світового співтовариства.

Наразі Україною підписано 50 міжнародних договорів у сфері охорони інформації з обмеженим доступом: 2 угоди з міжнародними організаціями (НАТО, ЄС); 48 двосторонніх договорів з інозем-

ними державами, у тому числі: 22 – з державами-членами НАТО (Албанія, Болгарія, Великобританія, Греція, Естонія, Іспанія, Італія, Латвія, Литва, Македонія, Німеччина, Норвегія, Польща, Румунія, Словаччина, Словенія, США, Туреччина, Угорщина, Франція, Хорватія, Чехія); 24 – з іншими країнами (Азербайджан, Алжир, Білорусь, Вірменія, В'єтнам, Грузія, Екваторіальна Гвінея, Ізраїль, Індія, Йорданія, Казахстан, Кіпр, Киргизія, Китай, Корея, Лівія, Македонія, Молдова, ОАЕ, Пакистан, Таджикистан, Туркменістан, Узбекистан, Шрі-Ланка); 2 угоди денонсовано (з Словацькою Республікою – 01.12.2008, Російською Федерацією – 21.05.2015).

Відповідно до вимог законодавства Верховною Радою України ратифіковано 46 угод. На даний час здійснюються заходи з підготовки до ратифікації міжнародного договору з Іспанією.

Готуються до підписання проекти міжнародних договорів з Бельгією та Португалією. Також, за ініціативи іноземної сторони, здійснюються заходи з внесення змін до угод з Молдовою та Великобританією.

Крім цього, через Міністерство закордонних справ України ініційовано питання щодо вивчення можливості укладення угод з Австралією, Аргентиною, Бразилією, Канадою, Монголією, Нідерландами, Перу, Саудівською Аравією, Японією [13].

Такі договори як правило складаються з наступних структурних елементів: преамбула, в якій визначаються сторони і загальні цілі угоди; погодження термінів і визначень, що використовується в угоді; таблиці узгодження грифів обмеження доступу, що використовуються у матеріальних носіях інформації, яка вступає в транскордонний обіг; обов'язки сторін щодо взаємного захисту інформації; процедури передачі інформації між сторонами і зазначенням державних органів кожної із сторін, які за це відповідають; процедури забезпечення захисту переданої інформації в ході її обігу; процедура організації взаємного контролю за режимом охорони переданої інформації стороною одержувачем; порядок дії сторін на випадок порушення умов договору [1-12].

Проаналізувавши угоди, можна стверджувати, кожна сторона має певний перелік обов'язків щодо захисту інформації, а саме: захист секретної інформації, переданої або створеної в процесі співробітництва Сторін; не змінювати гриф секретності, наданий організацією держави Сторони, що здійснила передачу, без письмової її згоди; упроваджені з отриманою секретною інформацією вживати такі ж заходи захисту , що використовується по відношенню до власної секретної інформації, ступені секретності якої порівнянні відповідно до таблиці узгодження грифів; користуватися секретною

інформацією, отриманою від організації держави іншої Сторони , винятково в передбачених при її передачі цілях; не надавати третій стороні доступ до секретної інформації без попередньої письмової згоди Сторони , що її передала; надавати доступ до секретної інформації тільки особам, яким ознайомлення з даною інформацією необхідне для виконання службових обов'язків з метою , передбаченою при її передачі або її спільному створенні; надавати доступ до секретної інформації лише тим особам, які мають відповідний допуск до секретної інформації і пройшли перевірку для оформлення допуску , що відповідає тій , яка необхідна для одержання допуску до прирівнюваної таємної інформації власної держави; забезпечувати на території власної держави проведення необхідних інспекційних перевірок та дотримання норм захисту таємної інформації [1-12].

Забезпечення інтересів держав на захист їх інформації досягається шляхом взяття державами на себе та виконання ними міжнародних зобов'язань, які стосуються взаємного визнання статусу інформації з обмеженим доступом, наданим у ході співробітництва іноземною стороною матеріалам.

Забезпечення належного режиму охорони цієї інформації за час перебування у розпорядженні іноземної сторони, інформування про факти розголошення наданої іноземною стороною інформації та забезпечення належного розслідування цих фактів та покарання винних у цьому осіб.

Проаналізувавши дані угоди можна дійти висновку, що при співробітництві з іноземними державами та ЄС, Україна доклала великих зусиль щодо захисту національної безпеки і державних інтересів у сфері захисту інформації з обмеженим доступом.

Література

1. Угода між Кабінетом Міністрів України та Урядом Грузії про взаємну охорону секретної інформації : Угоду ратифіковано Законом N 625-IV (625-15) від 06.03.2003 [Електронний ресурс]. Режим доступу : http: // zakon2.rada.gov.ua / show /268_001

2. Угода між Кабінетом Міністрів України та Урядом Республіки Вірменія про взаємну охорону секретної інформації : Угоду ратифіковано від 19.06.2003 [Електронний ресурс]. Режим доступу: http: // search.ligazakon.ua / l_doc2.nsf / link1 / MU02135.html

3. Угода між Кабінетом Міністрів України та Урядом Республіки Казахстан про взаємний захист секретної інформації : Угоду ратифіковано Законом N635-VI (635-17) від 30.10.2008 [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/398_053

4.Угода між Кабінетом Міністрів України та Урядом Республіки Молдова про взаємний захист секретної інформації : Угоду ра-

тифіковано 07.09.2005 [Електронний ресурс]. Режим доступу: http: // search.ligazakon.ua / l_doc2.nsf / link1 / MU04153.html

5. Угода між Кабінетом Міністрів України та Урядом Республіки Польща про взаємну охорону секретної інформації : Угоду ратифіковано Законом N 173-IV(173-15) від 26.09.2002 [Електронний ресурс]. Режим доступу: http: // zakon4.rada.gov.ua / laws / show / 616_028

6. Угода між Кабінетом Міністрів України та Урядом Туркменістану про взаємну охорону секретної інформації : Угоду ратифіковано від 10.01.2002 [Електронний ресурс]. Режим доступу: http: // search.ligazakon.ua / l_doc2.nsf / link1/MU01060.html

7. Угода між Урядом України та Урядом Китайської Народної Республіки про взаємну охорону секретної інформації : Угоду ратифіковано 20.11.2000 [Електронний ресурс]. Режим доступу: http://zakon.nau.ua/doc/?code=156_038

8. Угода між Кабінетом Міністрів України та Урядом Республіки Хорватія про взаємну охорону секретної інформації : Угоду ратифіковано 26.07.2006 [Електронний ресурс]. Режим доступу: http://zakon.nau.ua/doc/?code=191_016

9. Угода між Кабінетом Міністрів України та Урядом Федеративної Республіки Німеччина про взаємний захист таємної інформації : Угоду ратифіковано Законом N 2937-III (2937-14) від 10.01.2002, ВВР, 2002, N 23, ст.157 [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/276_008

10.Угода між Кабінетом Міністрів України та Урядом Латвійської Республіки про взаємну охорону секретної інформації : Угоду ратифіковано Законом N 2126-IV (2126-15) від 22.10.2004. URL: http://zakon4.rada.gov.ua/laws/show/428_025

11. Угода між Україною та Республікою Індія про взаємну охорону секретної інформації : Угоду ратифіковано 07.04.2004 [Електронний ресурс]. Режим доступу: http://www.yur-info.org.ua/doc/1743835/Ugoda-mizh-Ukrainoiu-ta-Respublikoiu-Indiia-pro-vzaiemnu-okhoronu-sekretnoi-informatsii

12. Угода між Урядом України та Урядом Словацької Республіки про взаємний захист таємної інформації та матеріалів : Угоду затверджено Постановою КМ N 1434(1434-98-п) від 14.09.98). URL: http://www.yur-info.org.ua/doc/1630730/Ugoda-mizh-Uriadom-Ukraini-ta-Uriadom-Slovatskoi-Respubliki-pro-vzaiemnii-zakhist-taiemnoi-informatsii-ta-materialiv

13. Щодо підготовки міжнародних договорів у сфері охорони інформації з обмеженим доступом [Електронний ресурс]. Режим доступу: https://ssu.gov.ua/ua/pages/172

ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ

УДК 004.056

Аміров М.Г.
Державний ВНЗ «Національний гірничий університет»
Тимофєєв Д.С.
Державний ВНЗ «Національний гірничий університет»

ПРОБЛЕМАТИКА НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ УКРАЇНИ

Разом із всеохоплюючим використанням інформаційних технологій, невід'ємною частиною вимог до ведення господарської та адміністративної діяльності стає потреба у обов'язковому запровадженні комплексного аудиту забезпечення інформаційної безпеки (ІБ). На даний момент в Україні відсутня єдина, затверджена державою, методика щодо аудиту інформаційної безпеки на об'єктах інформаційної діяльності.

Для підтвердження виконання вимог щодо забезпечення інформаційної безпеки в організації, стандарт ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013) вимагає від організацій регулярного проведення перевірок ефективності системи управління інформаційною безпекою на основі результатів вимірювань її ефективності, та вимірювання ефективності мір і засобів контролю та управління ІБ[2].

До нормативної бази перевірки систем управління інформаційною безпекою і оцінки діяльності по управлінню інформаційною безпекою можна віднести наступні міжнародні (національні) стандарти:

- ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT);
- ДСТУ ISO/IEC 27006:2015. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT);
- ISO/IEC 27007:2011. Guidelines for information security management systems auditing;

- ISO/IEC 27008:2001. Guidelines for auditors on information security controls;

- ДСТУ ISO/IEC 19011:2012. Настанови щодо здійснення аудитів систем управління (ISO/IEC 19011:2011, IDT).

Запровадження регулярного аудиту інформаційної безпеки дозволить реалізувати наступні цілі для об’єктів інформаційної діяльності:

- вироблення практичних рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів інформаційної безпеки;

- запровадження процесу управління ризиками;

- оцінка динаміки та поточного рівня захищеності об’єкту;

- локалізація причин виникнення проблем в системі захисту інформації;

- оцінка відповідності існуючим вимогам законодавства, стандартів, нормативних документів в галузі інформаційної та кібербезпеки, а також політики безпеки інформації організацій, що перевіряються.

Незважаючи на наявність міжнародної бази стандартів з аудиту ІБ, національна нормативно-правова база в сфері інформаційної безпеки не є остаточно узгодженою, що призводить до розходжень у процедурі аудиту та неоднозначності трактовки висновків.

Узгодження нормативно-правової бази України в сфері інформаційної безпеки є одним з найбільш важливих чинників комплексної протидії реалізації кібератак на об’єкти інформаційної діяльності різних форм власності. Серед основних завдань на даному етапі можна виділити наступні:

- створення узагальнених та галузевих практичних рекомендацій для підвищення рівня захисту об’єктів інформаційної діяльності;

- узгодження вимог стандартів ISO 27–ї серії, законодавства України та відповідних НД ТЗІ і перехід до аудиту на основі впровадження комплексної методики перевірки об’єктів критичної та важливої інфраструктури, на базі кращих світових практик;

- підвищення рівня підготовки за відповідними компетенціями та розширення кола сертифікованих фахівців з провадження аудиту та контролю інформаційної та кібербезпеки.

Література

1. ISO/IEC 27000:2016. Information technology — Security techniques — Information security management systems — Overview and vocabulary. URL: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

2. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи

захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

Андріяшик І.В.
Національна академія Служби безпеки України

НЕПРАВОМІРНЕ ВИКОРИСТАННЯ ФОТОГРАФІЙ У СОЦІАЛЬНИХ МЕРЕЖАХ

XXI століття – епоха бурхливого розвитку інформаційних технологій та систем масових комунікацій, яка перетворилася в найпотужніший ресурс об'єктів інтелектуальної власності.

Проте, з розширенням нових можливостей та інформатизацією суспільства, розширюється й кількість порушень авторських прав у зазначеній сфері, тому досить актуальним є питання дотримання авторських прав користувачами Інтернет-простору.

Якщо уважно придивитись до закону України «Про авторське право та суміжні права», виявиться, що вся мережа Інтернет – суцільне правопорушення [1].

У соціальних мережах «Вконтакте», «Одноклассники», «Facebook» та «Twitter» люди без побоювання публікують все – свої особисті дані, інформацію про своїх родичів, захоплення, вподобання тощо. Крім, того дають оцінку тим чи іншим подіям та явищам.

Мільйони користувачів кожного дня викладають на своїх сторінках безліч фотографій, та мало хто задумується про те, чи захищені ці фото авторським правом і що робити, якщо одного дня Ви побачите свої фотографії під чужим іменем.

Розміщення громадянином фотографій в Інтернеті не надає права іншим особам використовувати їх без згоди правовласника.

В той же час обставини розміщення громадянином свого зображення в мережі можуть свідчити про вираження такою особою згоди на подальше використання цього зображення, наприклад, якщо це передбачено умовами користування сайтом, на якому громадянином розміщено знімок.

Наприклад, така функція, як «репост», наявна в соціальних мережах, може трактуватися як згода на розповсюдження того чи іншого зображення. Якщо ж функція «репост» буде відключена, чуже фото не можна буде використовувати.

Учасник колективного фотознімку зможе використовувати це зображення на власний розсуд без отримання згоди від інших зображених на знімку осіб, якщо вони не заборонили таке використання і якщо зображення не містить інформацію про приватне життя

інших людей.

Згода на використання зображення не потрібна, якщо громадянин є публічною фігурою. Правда, тільки у тому випадку, якщо метою їх поширення не є обнародування приватного життя особи та для отримання прибутку. Не потрібно згоду відомої особи, якщо знімок зроблений в публічному місці, у тому числі у відкритих судових засіданнях або на різноманітних заходах [2].

Відповідно до статті 307 ЦКУ «Захист інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок» фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру.

Фізична особа, яка погодилася на знімання її на фото-, кіно-, теле- чи відеоплівку, може вимагати припинення їх публічного показу в тій частині, яка стосується її особистого життя. Витрати, пов'язані з демонтажем виставки чи запису, відшкодовуються цією фізичною особою.

Стаття 308 ЦКУ «Охорона інтересів фізичної особи, яка зображена на фотографіях та в інших художніх творах» передбачає, що фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за згодою цієї особи.

Якщо фізична особа позувала авторові за плату, фотографія або інший художній твір може бути публічно показаний, відтворений або розповсюджений без її згоди.

Фізична особа, яка позувала авторові фотографії за плату можуть вимагати припинення публічного показу, відтворення чи розповсюдження фотографії, іншого художнього твору за умови відшкодування автору або іншій особі пов'язаних із цим збитків.

Фотографія може бути розповсюджена без дозволу фізичної особи, яка зображена на ній, якщо це викликано необхідністю захисту її інтересів або інтересів інших осіб.

На даний час, способом особі захистити свої права законним шляхом є звернення до суду. Однак, незважаючи на вкрай незначну практику розгляду спорів про захист авторських на об'єкти розміщені в мережі Інтернет буде доволі складно захистити свої права, оскільки для того щоб подати позов до суду, перш за все необхідно знати прізвище, ім'я, по-батькові порушника, його адресу та телефон, якщо у Вас буде така інформація можна подавати позов до суду. Також, при зверненні до суду за захистом авторських прав фотографа, останній повинен довести, що є автором фотографій, а також

що саме йому належать майнові авторські права на фотографії, які були незаконно використані відповідачем. Відповідно до законодавства, автором твору вважається громадянин, чиє ім'я зазначено на оригіналі або примірнику твору. Тобто при подачі позовної заяви фотографу необхідно представити роздруковані фотографії, на яких буде зазначено його ім'я (розміщення на цифровому фотоапараті характеристики про фотографічні матеріали) або підтвердження показаннями свідків. У той же час, звертаючись до суду необхідно довести, що відповідач незаконно здійснив несанкціоноване використання об'єктів авторського права [4].

Отже, викладаючи власні фото та інформацію в соціальні мережі варто задуматись: чи хотіли б Ви бачити своє фото під ім'ям іншої людини, чи доклали Ви максимум зусиль для захисту власних даних та чи знаєте Ви яким чином можливо захистити власні права. Адже проблема плагіату в мережі Інтернет з кожним роком набуває все більшого значення, і вирішення її переноситься на перший план.

Література

1. Беляєва Яна. Селфі мавпи: методи захисту і казуси авторських прав в інтернеті. URL: http://platfor.ma/magazine/text-sq/media-innovations-lab/monkey-selfie/

2. Гроводська О.П. Правила використання в соціальних мережах авторських фотографій. URL: http://go-advocate.com/pravyla-vykorystannya-v-sotsialnyh-merezhah-avtorskyh-fotohrafij/

3. Томарова Ольга. Публікація в соціальній мережі як доказ в суді: практика і аналітика. URL: http://www.legalshift.com.ua/?p=35

4. ХОГО «Подільська правова ліга». Як захистити авторське право на матеріали опубліковані в мережі Інтернет. URL: http://pravoonline.org.ua/site/kbase/c/20/category/dovidkova-informaciya/t/188/title/yak-zahistiti-avtorske-pravo-na-materiali-opiblikovani-v-mer

УДК 342.9:343.3

Бачинський О.В.
Служба безпеки України

ЗАХИСТ КОМЕРЦІЙНОЇ ТАЄМНИЦІ – ВАЖЛИВИЙ ЕЛЕМЕНТ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Україна перебуває в непростих умовах, знаходячись фактично в стані гібридної війни, розв'язаної Російською Федерацією, під час якої неабиякої актуальності набувають питання інформаційної безпеки. Попри безперечну важливість боротьби із інформаційними

впливами, дезінформацією, пропагандою, а також першочерговою необхідністю запобігання спрямуванням іноземних спецслужб на здобуття даних, які містять державну таємницю, важливим є інформаційна безпека у секторі захисту інформації, що становить комерційну таємницю.

На перший погляд, може скластись враження, що державні та правоохоронні органи не повинні мати відношення до процесу захисту вказаної категорії інформації, забезпеченого приватними структурами, оскільки він захищає виключно їхні комерційні інтереси. Проте, аналіз змісту відомостей, що містять комерційну таємницю та наслідків їх втрати, дозволяє зробити висновки про необхідність участі спецслужби та правоохоронних органів в організації та проведенні її захисту.

Відповідно до ст. 505 Цивільного кодексу України, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів, щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію[1].

До таких даних найчастіше відносять: 1) відомості наукового характеру (ідеї, винаходи, відкриття; окремі формули; програмне забезпечення; результати наукових досліджень); 2) відомості технологічного характеру (конструкторська документація, креслення, схеми, записи; описи технологічних іспитів; «ноу-хау»; нові або унікальні вимірювальні комплекси, прилади, верстати й устаткування); 3) відомості ділового характеру (відомості про укладені або заплановані контракти, конфіденційні переговори; дані про постачальників та клієнтів; калькуляція витрат, структури цін, маркетингові дослідження; плани розвитку та інвестицій [3].

Як показує практика, такими відомостями намагаються заволодіти не тільки конкуренти, а й іноземні держави та спецслужби. Унікальність та складність інформації, що становить комерційну таємницю дозволяє окремим суб’єктам, у разі заволодіння такими даними, кардинально змінити ситуацію на ринку, витіснити, навіть знищити конкурента. Оскільки суб’єктом посягання є українське підприємство, установа чи організація, наслідки стосуються не тільки втрат конкретного суб’єкта, а й держави в цілому. Крім того, що втрата частини ринку, або погіршення конкурентоспроможності окремого суб’єкта впливає на поступлення коштів в державний бюджет, завдається удар по розвитку підприємства та, нерідко, всієї

галузі в межах держави. А сукупність таких випадків підриває економічний та науковий потенціал держави, формує несприятливий інвестиційний клімат і негативний імідж на міжнародній арені.

Вищенаведені тези підтверджують окремі події, які відбувалися під час окупації Луганської та Донецької областей, а саме викрадення більше 20 підприємств, серед яких найбільш відомими є устаткування заводу «Топаз», на якому виготовлялись комплекси «Кольчуга» та «Мандат», крім того до РФ переміщено унікальні штампи-лекала Сніжнянського машинобудівного заводу, які визначають точність виробництва лопаток для авіатурбін. Звичайно, ключовими при захопленні були саме відомості технологічного і наукового характеру, які дозволяли створювати передову унікальну продукцію та були захищені як комерційна та державна таємниця.

Вказані події підтверджують, що будь-яка інформація з обмеженим доступом, в тому числі конфіденційна інформація становить неабиякий інтерес не тільки для окремих організацій, груп та осіб, а й для цілих держав та їх спецслужб, які часто не обмежуються в методах її отримання.

Якщо звернутись до американського досвіду, то ще в 1990 р. Президент США Джордж Буш у своїй доповіді «Стратегія США в галузі національної безпеки» проголосив економічну розвідку пріоритетним напрямком у діяльності американських спецслужб. Наприкінці 1993 р. Біл Клінтон дав вказівку керівництву розвідувального співтовариства США про поглиблення досліджень у сфері економічної розвідки та економічної контррозвідки. [4].

Саме тому, на нашу думку, питання захисту комерційної таємниці є більш глобальним, ніж може здатись на перший погляд та повинно розглядатися в комплексі, разом із проблемами захисту іншої інформації з обмеженим доступом. Динаміка розвитку суспільних відносин, технологічний прогрес та посягання на українську державність постійно ставлять нові завдання перед органами що забезпечують захист інформації з обмеженим доступом. Водночас наслідки, які можуть бути спричинені витоками конфіденційної інформації та можливості їх використання спецслужбами іноземних держав, повинні спонукати до пошуку елементів співпраці між правоохоронним органами та комерційними структурами з даних питань.

Література

1. Цивільний кодекс України [Електронний ресурс] : від 16.01.2003 № 435-IV // Верховна Рада України: офіц. веб-портал. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/435-15– Назва з екрана.

2. Про інформацію, Закон України [Електронний ресурс]: від

02.10.1992 № 2657-XII // Верховна Рада України : офіц. веб-портал. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12 – Назва з екрана.

3. Сліпачук О. Комерційна таємниця на підприємстві [Електронний ресурс]: від 08.11.2006 / О. Сліпачук // HR-Лига: бібліотека статтей. URL: http://hrliga.com/index.php?module=profession&cid=18 – Назва з екрана.

4. Управління захистом комерційної таємниці: курс лекцій / Укладач: Суярова О.О. – Суми: Вид-во СумДУ, 2009. –73 с.

Голубєв О.В.
Національна академія державного управління
при Президентові України

ІНСТРУМЕНТ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ – СТРАТЕГІЧНІ КОМУНІКАЦІЇ

Значною мірою нехтування пропаганди після закінчення холодної війни, використання інформації і громадської дипломатії з метою впливу на аудиторію та сприяння досягненню національних цілей робить повернення цих технологій актуальними. [1].

Згідно з інтерв'ю з українськими військовослужбовцями, деякі українські канали мають проросійськи тенденції, такі як «Інтер», який показує деморалізованих військовополонених, не бажання мобілізуватися резервістів і недоглянуті об’єкти військової інфраструктури. На думку чиновників і радників Міністерства інформаційної політики України і експертів ЗМІ, контроль над теле- і радіо- вежами є важливим методом Росії для підтримки своєї інформаційної діяльності. Соціальні медіа особливо впливові, але різні портали, сайти і інтернет-ЗМІ також відіграють важливу роль, велика кількість веб-сайтів і порталів були створені в 2014 році і російські ЗМІ почали регулярно звертатися до них. Паніку і страх поширювалися через операторів мобільного зв'язку як частина російських психологічних операцій. Найбільш широко використовували оператора «Київстар» в антитерористичні операції (АТО), що належить російському бізнесу. Інформаційні центри в так званій «Новоросії» реєстрував номера телефонів людей, які відвідали район АТО. Також широко використовувалась смс - розсилка. Ще один ефективний спосіб швидко і ефективно контролювати людей на Донбасі є використання гучномовців. Інформація, передана через гучномовці для українських солдатів на лінії фронту зменшує їх готовність вести війну і впливає на їх моральний дух. Широка і ефективна мережа російських агентів

під керівництвом ГРУ та ФСБ діяла ще до того як почався військовий конфлікт. Вони стали поширювати неправдиву інформацію, створювали паніку, страх і ненависть. Психологічний вплив на людей був проведений надзвичайно методологічно та системно. [7].

Задовольнити вимоги, що їх висувають експерти та громадяни до інформаційної протидії держави, є можливим через застосування стратегічних комунікацій. У найбільш широкому розумінні стратегічні комунікації є процесом інтеграції досліджень сприйняття аудиторії та зацікавлених сторін (стейкхолдерів) та врахування отриманих результатів під час планування і реалізації політики та вжиття окремих заходів. Стратегічні комунікації спрямовані на підрив і делегітимізацію противника у спосіб набуття підтримки й визнання з боку місцевого населення, електорату своєї країни, міжнародної громадськості та усіх інших цільових груп. Сутність стратегічних комунікацій полягає в тому, що сформульовані для різних цільових аудиторій меседжі не конфліктують один з одним. Відтак, змістовим ядром стратегічних комунікацій є формування наративу – переконливої сюжетної лінії, яка може пояснити події аргументовано та з якої можна дійти висновків щодо причин знаходження держави в конфлікті, значення цього становища та щодо перспектив держави у разі успішного виходу з нього. Щоб бути ефективними, стратегічні наративи мають входити в резонанс із цінностями, інтересами і забобонами цільових аудиторій. Стратегічні наративи формулюють кінцеві стани і пропонують спосіб досягнення мети, забезпечуючи громадськість розумінням і сенсом подій, пов’язаних із застосуванням воєнної сили.[5]

Виходячи з вищевикладеного потрібно зробити висновок, що дієвим спротивом України в інформаційній сфері має бути впровадження такого інструменту як стратегічні комунікації. Стратегічні комунікації спрямовані на підрив і делегітимізацію противника у спосіб набуття підтримки й визнання з боку місцевого населення, електорату своєї країни, міжнародної громадськості та усіх інших цільових груп. Завдяки впровадженню цієї практики можлива побудова системи протидії пропаганді Російської Федерації, оскільки її впливи засновані на використанні негуманних методів ведення інформаційної війни.

Література:

1. Seip M. Harnessing Communications and Public Diplomacy [Electronic resource] // Brent scowcroft center on international security January 2016. – Mode of access: http://www.stratcomcoe.org/mark-seip-harnessing-communications-and-public-diplomacy – Title from the screen.

2. Snegovaya M. Putin's information warfare in Ukraine. Soviet origins of Russia's hybrid warfare [Electronic resource] // Institute for the study of war September 2015 – Mode of access: http://www.stratcomcoe.org/msnegovaya-putins-information-warfare-ukraine – Title from the screen.

3. Mark Galeotti, "The 'Gerasimov Doctrine' And Russian Non-Linear War," [Electronic resource] July 6, 2014, – Mode of access: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ – Title from the screen.

4. Сивак Т. Аналіз передумов становлення системи стратегічних комунікацій в державному управлінні [Електронний ресурс]: Глобальна організація союзницького лідерства 2016, - Режим доступу: http://goal-int.org/analiz-peredumov-stanovlennya-sistemi-strategichnix-komunikacij-v-derzhavnomu-upravlinni/

5. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської – К. : НІСД, 2016. – 109 с

6. Ліпкан В.А. Стратегічні комунікації : словник / Т.В. Попова, В.А. Ліпкан / за заг. ред. В.А. Ліпкана. – К. : ФОП О.С. Ліпкан, 2016. – 416 с.

7. Dr. Vladimir Sazonov, M.A. Kristiina Müür and Dr. Holger Mölder Russian Information Campaign Against the Ukrainian State and Defence Forces [Electronic resource] 2016, – Mode of access: http://www.stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces-0 – Title from the screen.

Гончаренко Д.Б.
Національна академія Служби безпеки України

КОНКУРЕНТНА РОЗВІДКА – НЕОБХІДНІСТЬ СУЧАСНОГО БІЗНЕСУ

Щоб вижити в умовах запеклої конкурентної боротьби, необхідно знати хоч щось про найближчих конкурентів і про те, що може чекати тебе завтра. Подібні актуальні відомості про ділове оточення і конкурентному середовищі навколо підприємства, спеціально орієнтовані на прийняття стратегічних рішень, можна отримати за допомогою інструментів конкурентної розвідки.

Сучасний бізнес передбачає гнучкість і швидкість реакцій на стрімко мінливі зовнішні умови. Але для того, щоб швидко прийняти правильне рішення, необхідно володіти перевіреною інформацією про поточний стан справ.

Розглядаючи поняття «конкурентна розвідка», будемо додержуватися визначень вітчизняних енциклопедичних джерел, в яких розвідка визначається як:

1.Дії, здійснювані певними людьми й групами людей для одержання необхідної інформації про явища й об'єкти, що входять у сферу їхніх професійних інтересів.

2.Організації (організаційні одиниці), що відають спеціальним вивченням різних аспектів будь-яких явищ, пов'язаних з наукою, виробництвом, економікою, політикою, війною й суспільними відносинами всередині країни та за її межами в рамках завдань, розв'язуваних цими організаціями.

3.Сукупність прийомів та методів вивчення об'єктів і явищ, що входять у сферу інтересів конкретних людей, професійних груп та організаційних одиниць [1].

Цілі конкурентної розвідки прості - виявлення реальних і потенційних чинників, які впливають або можуть вплинути на здатність фірми успішно конкурувати на даному ринку. За допомогою інструментів конкурентної розвідки виявляються нові можливості і загрози бізнесу: як краще зробити інвестиції, яким чином розвивати бізнес, яких дій варто чекати від конкурентів, партнерів, клієнтів і держави.

Джерела інформації в конкурентній розвідці можуть бути первинні і вторинні. В якості первинних виступають люди (спілкування на виставках, конференціях та інших профільних заходах). Вторинні - це різні дослідження ринків, бенчмаркінг, статистичні дані і т.д [3].

Говорячи про методи конкурентної розвідки, необхідно відразу обумовити - це не шпигунські ігри. Тому злом комп'ютерів, установка «жучків», стеження за конкурентами, підкуп співробітників тут не використовуються.

Основні методи конкурентної розвідки засновані на логіці і зборі легальної інформації, тобто інформації, яка знаходиться у відкритому доступі. Методів цих досить багато.

Прості методи збору інформації для конкурентної розвідки: бесіди зі співробітниками фірми конкурента (теми будь-які: про погоду, про навчання і заодно про товар); бесіда по телефону з менеджерами - в більшості випадків при правильній розмові можна дізнатися відразу половину всієї потрібної інформації; вивчення резюме співробітників, в яких вони можуть розкрити частину інформації, щоб сподобатися новому роботодавцю; інтернет-спілкування з менеджерами компанії-конкурента; чернетки, які сотнями видаляються з офісів; спостереження за роботою конкурентів; спостереження за діяльністю та прихильностями співробітників конкуруючої компанії у соціальних мережах та інші [2].

Умови успішного впровадження програми конкурентної розвідки: правильне розуміння, що таке конкурентна розвідка; усвідомлення керівником компанії і менеджерами вищого рівня необхідності конкурентної розвідки. Підтримка програми конкурентної розвідки з боку першої особи компанії; наявність плану по просуванню концепції конкурентної розвідки всередині компанії. Співробітники повинні знати, що таке конкурентна розвідка, як вона проводиться, що робити з отриманими даними; наявність корпоративної культури, яка заохочує обмін інформацією між підрозділами, співробітниками; взаємодія між професіоналами конкурентної розвідки і менеджерами компанії; визначення реальних потреб споживачів конкурентної розвідки; максимальне залучення співробітників в роботу зі збору конкурентних відомостей; максимальне полегшення процесу передачі інформації між підрозділом конкурентної розвідки та споживачами; наявність грошових коштів на поточні витрати, щоб підтримувати роботу програми конкурентної розвідки протягом тривалого часу [3].

Конкурентна розвідка застосовується не тільки великими і середніми компаніями. Вона з успіхом може застосовуватися і в малому бізнесі. Програму конкурентної розвідки можна розробити швидко. Це потребуватиме певного часу, протягом якого буде проходити напрацювання відповідних баз даних і знань, корисних контактів в середовищі першоджерел і експертів, які добре знають ринок і готових ділитися інформацією. Нарешті, ефективна розвідувальна система вимагає підготовлених кадрів, здатних вирішувати поставлені завдання різного ступеня складності. Терміни розгортання подібної ефективної системи комерційної розвідки можуть коливатися в проміжку від року до півтора років.

Література

1. Конкурентна розвідка : навч. посіб. / Т.Ю.Ткачук. – К.: НА СБ України, 2013. – 295 с.

2. За матеріалами Інтернет ресурсу «Конкурентная разведка и контрразведка». URL: http://www.it2b.ru

3. Ярочкин В.И., Бузанова Я. В. Корпоративная разведка . М.: «Ось-89», 2004. 422 с.

Гострик С.Р.

Національна академія Служби безпеки України

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В США

Укладання контрактів з підрядними організаціями стало невід’ємною частиною проведення спеціальних операцій та військових дій силовими структурами США. В Афганістані та Іраку приватні

фірми здійснюють керування безпілотними літальними апаратами, каналами зв'язку, наведення на ціль високоточної зброї. Недержавні підрядники управляють комп'ютерними системами, що відтворюють тактичну повітряну картину для Об'єднаного центру управління повітряними операціями, координують роботу систем зенітних керованих ракет, займаються консалтингом, навчанням та обслуговуванням, фортифікаційними роботами та тиловим забезпеченням. Деякі компанії працюють на американські спецслужби, постачаючи ІТ-обладнання, програми, та надаючи багато інших послуг.

Розвідка, рекогносцировка, спостереження та контроль виконуються багатьма корпораціями, які спеціалізуються на радіотехнічній та вимірювально-сигнатурній розвідці, інтерпретації фотознімків, аналізі, розвідці, електронних, психологічних та інформаційних війнах. Компанії, які отримали серйозні замовлення, або ті, які уклали контракт у новій для них сфері, часто укладають субдоговір з більш спеціалізованими компаніями [1].

Наведені особливості вимагають серйозного підходу до організації захисту інформації. Спеціально для цього в США розроблено тактику «Заперечення і обман». В межах цієї тактики провадиться захисна діяльність, яка спрямована на охорону державної таємниці, що насамперед циркулює в органах державної влади. Зокрема, до державної таємниці відносять наміри, плани, можливості і дії, які уряд прагне приховати від інших держав та супротивників. У свою чергу наступальна діяльність проявляється в заходах, які відволікають від правди та переключають увагу на хибні альтернативи. Тобто, у цьому випадку потрібними є програми дезінформування, які повинні ввести в оману реальних та потенційних ворогів [2].

Поряд з тим одним із основних блоків засобів, використання яких може сприяти захисту інформації, є електронні засоби. Західні експерти закликають спецслужби розширяти їх можливості в кібернетичному просторі. Як негативний досвід ігнорування цієї потреби приводяться кібернетичні напади на уряд Естонії в 2007 році, що здійснювались колективними діями російських націоналістів в міжнародному просторі з метою руйнування та нанесення шкоди інтернет-ресурсам. Ці атаки були успішними: вони надовго паралізували фінансові, урядові та оборонні установи, а на їх реалізацію потрібно було зовсім небагато складного обладнання чи спеціалізованих знань.

З метою запобігання цій шкоді, об'єктом якої в першу чергу стають органи державної влади та об'єкти критичної інфраструктури, необхідним є розроблення доктрин для ведення боротьби в кіберпросторі та підбір відповідних засобів для цього. Показовим у цьому відношенні є практика Сполучених Штатів Америки (The U.S. Force

Cyber Command Strategic Vision) [3]. Так, вважається, що електронні системи виявлення підозрілих типів активності чи аномальних подій повинні бути встановлені на відповідних найбільш вразливих об'єктах. З їх допомогою спецслужби повинні краще захищати ті зони інформації, які є настільки таємними, що можуть поширюватись лише серед осіб, які відповідають критеріям допуску.

Незважаючи на те, що ця вимога знаходиться в прямій суперечності з безперевним обміном інформацією на Заході, її дотримання є конче необхідним – чим більш доступними є таємні дані, тим більш вірогідним є їх витік чи розголошення, тим легше буде їх викрасти.

Крім того, керівникам органів державної влади рекомендується посилювати стан охорони державної таємниці за допомогою наступних режимних заходів: утруднення доступу до таємної інформації; створення системи класифікації з обмеженим доступом різних категорій співробітників, які пройшли ретельну перевірку; застосування заходів безпеки в роботі з комп'ютерами, які б позбавляли допуска незацікавлених співробітників до секретних файлів без наявності певного кода; збереження носіїв інформації у вогнетривкому сейфі вночі.

Ще одним тактичним прийомом, який сприяє ефективному контррозвідувальному забезпеченню органів влади в США, є постійне навчання працівників цих органів елементам безпеки. Так, їм рекомендується пояснювати, що заходи безпеки направлені на їх захист та здійснюються в цілях процвітання урядової структури й країни в цілому. При цьому підкреслюється необхідність допомоги у визначенні підозрілої поведінки інших працівників.

У разі порушення працівниками правил безпеки їх слід звільняти. З іншого боку, якщо співробітник, який порушив правила безпеки, звільняється, не зазнавши покарання, інші його колеги можуть наслідувати його. У цьому випадку покарання має бути обов'язковим, оскільки виконуватиме ще й профілактичну роль.

Врахування наведеного досвіду захисту інформації в США є необхідним у контексті євроатлантичної інтеграції України. З огляду на викладене до шляхів удосконалення цієї практики у нашій країні слід віднести: посилення охорони державної таємниці в органах державної влади, інформації з обмеженим доступом – на об'єктах критичної інфраструктури, відповідних режимних заходів; постійне навчання осіб, які мають доступ до цієї інформації, елементам безпеки; розширення можливостей спецслужб в кібернетичному просторі; розроблення доктрин для ведення боротьби в кіберпросторі та підбір відповідних засобів для цього.

Література

1. Clearing House for Arab Intelligence, Intelligence Online, No.

535, 24 November – 7 December 2006, p.4.
2. Donald C.F. Daniel, «Denial and Deception», in Transforming U.S. Intelligence, op. cit., pp. 134-146.
3. The U.S. Force Cyber Command Strategic Vision (Washington D.C., 4 March 2008.).

УДК 651, 658 (477)

Гоц О.В.
Національна академія Служби безпеки України
Семчишина С.В.
Національна академія Служби безпеки України

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДОКУМЕНТІВ В УМОВАХ ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В сучасних умовах ведення проти України інформаційної війни перед нами стоять вимоги значного посилення захисту інформаційної безпеки, та протидії кібератакам зі сторони ворога.

Плідне та повне використання документів стає можливим за умов чіткої організації інформації, яка зберігається в архівах, бібліотеках та інших центрах документації. Основною ланкою такої організації є системи наукової класифікації документів, які сьогодні розробляються в межах вітчизняного документознавства та суміжних із ним наук. На сьогоднішній день не існує єдиної класифікації документів, оскільки науковці здійснюють об'єднання різних систем та підсистем документації на основі усталених розроблених класифікаційних схем. Проте сучасні вимоги до захисту інформаційної безпеки вимагають встановлення єдиних правил до класифікації документів; особливо тих, що мають обмежений доступ.

Поняття "класифікація" використовується найчастіше одночасно і у значенні процесу, і у значенні результату, тобто, розуміється як угруповання і як отримана в його результаті схема. Для розмежування процесу класифікації і його результату науковцями пропонується вживати два терміни:

- класифікування документів – процес упорядкування або розподілу документів за класами з метою відбиття відносин між ними й складання класифікаційної схеми;
- класифікація документів – це система їх супідрядності, використовувана як засіб встановлення зв'язків між класами документів, а також для орієнтування в їх різноманітті [1, с. 90].

Наразі використовуються наступні класифікації документів [1; 2; 3; 4]:

1. За видами діяльності, що відбиваються у документах, вони поділяються на документи із загальних та адміністративних питань та документи за функціями управління.

2. За назвами документи класифікуються так: наукові звіти, креслення, схеми, графіки, накази, розпорядження, плани, акти, протоколи, договори, інструкції, довідки, пояснювальні записки, авторські посвідчення тощо.

3. За способом фіксації інформації документи бувають письмові, графічні.

4. За місцем складання документи підрозділяються на документи, використовувані для вирішення зовнішніх і внутрішніх питань. Зовнішня документація, у свою чергу, ділиться на вхідну й вихідну кореспонденцію.

5. За ступенем складності документи класифікують на прості й складні.

6. За ступенем гласності розрізняють документи відкриті (несекретні) і документи з обмеженим доступом.

7. За юридичною чинністю документи підрозділяють на справжні й підроблені. Справжні документи бувають дійсні й недійсні.

8. За строками виконання документи класифікуються на термінові й нетермінові.

9. За стадіями підготовки документи поділяються на чорновий документ й оригінал. З останнього можуть бути виготовлені копії, виписки з документу й дублікат.

10. За походженням документи класифікують на службові, підготовлені на підприємствах, в організаціях, і особисті листи громадян з викладом скарг, пропозицій, прохань.

11. За строками зберігання документи діляться на документи постійного й документи тимчасового зберігання.

12. За ступенем обов'язковості документи бувають інформаційні і директивні – обов'язкові для виконання, що носять характер юридичної або технічної норми.

13. За ступенем уніфікації розрізняють документи індивідуальні, типові, трафаретні, зразкові й уніфіковані у вигляді анкети й таблиці.

14. За характером змісту документи бувають первинні й вторинні.

Це основні класифікації, що використовуються у документознавстві. Існують іще класифікації за рівнем узагальненості інформації, за характером знакових систем фіксації інформації, за каналом сприйняття інформації, за ступенем поширеності документів, за регулярністю виходу документів у світ, за часом появи у зовнішньому середовищі, за місцем походження тощо.

Зважаючи на швидку та широкомасштабну інформатизацію су-

спільства, можна стверджувати, що будуть з'являтися нові класифікації документів, які вже створюватимуться у віртуальному середовищі і матимуть нові ознаки для класифікації. Враховуючи сучасні реалії пов'язаних із рухом України у всіх сферах розвитку до європейських умов життя, необхідно досконало вивчати загальноєвропейські стандарти інформаційної безпеки з подальшим використанням їх у розробці нових правил класифікації документів.

Література

1. Бездрабко В.В. Документознавство в Україні: інституціоналізація та сучасний розвиток : монографія / В.В. Бездрабко ; Київ. нац. ун-т ім. Тараса Шевченка. – К. : Четверта хвиля, 2009. – С. 88-96
2. Документознавство: курс лекцій / Уклад. : О. Ю. Малюк, Н. М. Лєсовець, Г. Ю. Есаулова; ЛНУ ім. Тараса Шевченка. – Луганськ, 2013. – 166 с.
3. Палеха Ю.І. Організація загального діловодства: навч. посіб. для студ. ВНЗ / Ю.І. Палеха, Н.О. Леміш. – К. : Ліра-К, 2009. – 458 с.
4. Швецова-Водка Г.М. Документознавство: навч. посіб. / Г.М. Швецова-Водка. – К. : Знання, 2007. – 398 с.

УДК 001.18

Давидюк А.В.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СКЛАДОВА КІБЕРНЕТИЧНОЇ АТАКИ

З метою усунення невизначеностей в подальшому розкритті даної тематики наведемо визначення соціальної інженерії та кібернетичної атаки. Отже під *соціальною інженерією* будемо розуміти метод несанкціонованого доступу до захищених інформаційних ресурсів, який базується на способах впливу на людську психологію [1]. *Кібернетична атака* – цільова атака, процес здійснення якої контролюється вручну в реальному часі людиною, що є центром атаки. Метою даної атаки є розкрадання захищеної інформації з інформаційної системи конкретної компанії, організації або державної служби [2].

Одним з прикладів використання соціальної інженерії є електронний лист, зміст якого буде спонукати користувача запустити прикріплений до листа файл і таким чином активується троянська програма або інше шкідливе програмне забезпечення. Проте, найефективнішим вважається симбіоз фішигу та електронного листа з використанням соціальної інженерії. В свою чергу *фішинг* – це вид інтернет

шахрайства з використанням соціальної інженерії для отримання доступу до конфіденційної інформації користувачів [3]. Одним з яскравих прикладів використання такого симбіозу є складна кібератака з використанням BlackEnergy. Дане повідомлення включало в себе адресу електронної пошти з доменом gov.ua, призначеного для органів державної влади, як елемент фішингу і документ Office в якості приманки. Приклад такого листа наведений на рисунку 1.

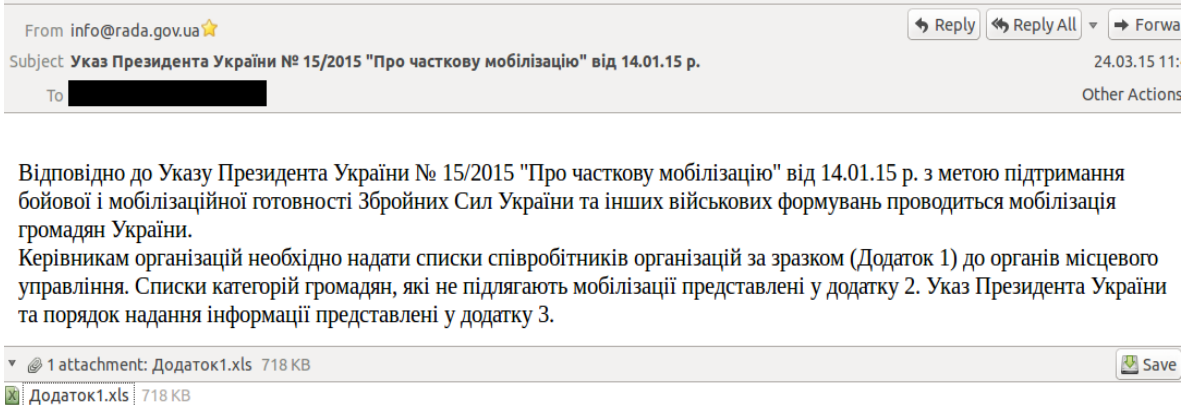

Рисунок 1. Зміст листа [4].

Це звичайна практика цілеспрямованих атак. Користувач отримує від зловмисника електронною поштою повідомлення, з вкладеним шкідливим файлом, якщо цільовий вузол має вразливості в області безпеки, то на ньому буде автоматично запускатися код макросу або користувач побачить наступне повідомлення, що має на меті спонукати його запустити макроси. Зловмисник в свою чергу попереджає жертву українською мовою: "Зверніть увагу, що! Цей документ підтримується тільки більш новою версією Office, щоб відобразити вміст документа, необхідно включити макроси. " Приклад такого попередження наведений на рисунку 2.

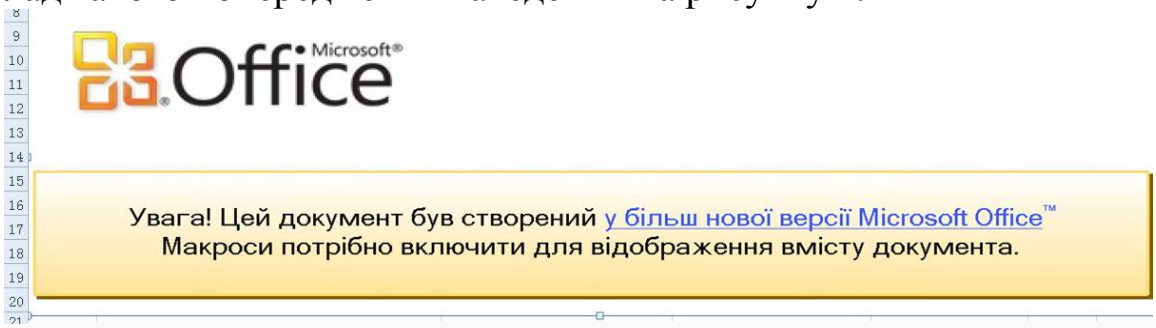

Рисунок 2. Приклад попередження, зробленого зловмисником [4].

Зауважимо, що на перший погляд звичайний лист може нести в собі значиму загрозу діяльності та репутації організації, а у випадку якщо така діяльність пов’язана з об’єктами критичної інфраструктури – то і життю людини. Використання таких листів базується на емоційній реакції – на потужній короткій емоції. Відповідно до вище вказаного доцільним є сформувати перелік рекомендацій щодо захисту від наведених вище підступних методів зловмисників.

1) Витримайте паузу 10 секунд і подумайте: У чому сенс повідомлення ?

2) Зверніть увагу на адресу відправника - хто надіслав вам це повідомлення - наскільки часто ви спілкуєтесь? У разі обмеженого кола адресатів листування обмежте за допомогую налаштувань поштового сервісу перелік адрес, від яких можете отримувати листи.

3) Якщо зміст чи адреса відправника викликали підозру або просто бажаєте перестрахувати себе зв'яжіться з відправником телефоном та переконайтесь у достовірності вмісту повідомлення.

Намагання зловити користувача на емоційній реакції дуже легко нівелюється простою зупинкою і думкою про те, що не варто поспішати і просто подумати, що це і для чого.

Отже з посиленням існуючих заходів та розробкою нових методів захисту зловмисники стають все більш винахідливими. Тому варто постійно бути вкрай обережними та уважними, щоб не стати їх жертвою. Виконання вище наведених рекомендацій допоможе вам мінімізувати та усунути ризики кібернетичної безпеки.

Література

1.Митник К.Д. Мистецтво обману/ К. Д. Митник, В. Л. Саймон. – М.: Компанія АйТі, 2004. – 360 с.

2.Targeted threat hunting [Електронний ресурс] – Режим доступу до ресурсу: https://www.secureworks.com/capabilities/incident-response/incident-management/targeted-threat-hunting..

3.Фишинговая атака [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://it-web-log.ru/2012/02/fishingovaya-ataka/.

4.Comprehensive Analysis Report on Ukraine Power System Attacks [Електронний ресурс] // Antiy Labs. – 2016. – Режим доступу до ресурсу: http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/.

УДК 347.734

Дячук П.Р.
Національна академія Служби безпеки України
Іванов Ю.А.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

ПРАВОВІ АСПЕКТИ ОХОРОНИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ В БАНКІВСЬКИХ ПРАВОВІДНОСИНАХ

Належна правова охорона комерційної таємниці є одним із важливих аспектів забезпечення економічної безпеки учасників господарського обороту та держави в цілому. Особливої актуальності це набуває у сфері банківських правовідносин в умовах

соціально-економічної та політичної нестабільності.

Відповідно до статті 505 Цивільного кодексу України [1] комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

У банківських правовідносинах інформацію, яка є комерційною таємницею, можна розділити на дві складові:

1. Інформація, яка є комерційною таємницею самого банку як суб’єкта господарювання.

2. Інформація, яка є комерційною таємницею клієнтів банку.

Правова охорона комерційної таємниці банку не має ніяких суттєвих особливостей порівняно із правовою охороною комерційної таємниці будь-яких інших суб’єктів господарювання.

Що ж до інформації, яка є комерційною таємницею клієнтів банку, то режим її правової охорони залежить від певних обставин.

Так, зокрема, матеріальні носії такої інформації можуть бути розміщені клієнтом в орендованому банківському сейфі (так зване закрите зберігання цінностей). В такому разі йтиметься не про збереження комерційної таємниці, а про забезпечення схоронності цінностей, довірених банку клієнтом.

Натомість при наданні інших послуг банк може безпосередньо отримувати від клієнта інформацію, яка є його комерційною таємницею. Це, зокрема, відбувається у процесі надання суб’єктам господарювання банківських кредитів. При цьому відповідно до ч.2 статті 60 Закону України «Про банки і банківську діяльність» [2] комерційна таємниця клієнтів банку набуває статусу ще й банківської таємниці з відповідним правовим режимом.

Відповідно до статті 2 Закону України «Про банки і банківську діяльність» клієнт банку – це будь-яка фізична чи юридична особа, що користується послугами банку. Отже у разі відмови банку від укладення із суб’єктом господарювання кредитного договору, останній не стає його клієнтом, а тому на надану ним банку інформацію правовий режим банківської таємниці не поширюється. Приєднуємось до думки тих науковців, які вважають, що правовий режим банківської таємниці слід поширити й на інформацію, отриману від суб’єктів, котрі зверталися до банку, але його клієнтами не стали. Водночас до внесення відповідних змін до законодавства, правова охорона такої інформації може здійснюватися відповідно до норм щодо комерційної таємниці. Однак при цьому слід враховувати, що, суб’єкт господарювання має повідомити банк про те, що певна інформація визначена ним як комерційна таємниця, оскільки

перелік такої інформації, на відміну від банківської таємниці, нормативно не визначено.

За звичайних умов банк забезпечує збереження отриманої від клієнтів інформації відповідно до вимог законодавства та нормативно-правових актів НБУ. Окремо слід звернути увагу на проблеми збереження такої інформації у разі виникнення нештатного режиму, що унеможливлює роботу банківської системи у звичайному порядку. Організацію роботи банківської системи за таких умов регламентовано інструкцією, затвердженою постановою Правління НБУ від 22 липня 2014 року № 435 [3]. Однак ця інструкція, на жаль, не містить спеціальних норм спрямованих на забезпечення схоронності банківської документації, яка може містити комерційну інформацію клієнтів та їх комерційну таємницю. Таким чином, у разі захоплення приміщення банківської установи, поряд із готівкою та іншими цінностями, можуть бути втрачені й відповідні документи.

Отже вітчизняне законодавство що правової охорони комерційної таємниці у сфері банківських правовідносин потребує вдосконалення.

Література

1. Цивільний кодекс України: Закон України від 16.01.2003р. №435-IV. URL: http://zakon.rada/gov/ua.

2. Про банки і банківську діяльність: Закон України від 7.12.2000р. № 2121-III. URL: http://zakon.rada/gov/ua

3. Про затвердження Інструкції щодо організації роботи банківської системи в надзвичайному режимі: постанова Правління НБУ від 22.07.2014р. № 435. URL: http://zakon.rada/gov/ua

УДК 347.734

Єргакова С.А.
Національна академія Служби безпеки України
Іванов Ю.А.
кандидат юридичних наук, доцент
Національна академія Служби безпеки України

ПРАВОВІ АСПЕКТИ ЗБЕРЕЖЕННЯ БАНКІВСЬКОЇ ТАЄМНИЦІ ЗА НАДЗВИЧАЙНИХ УМОВ ФУНКЦІОНУВАННЯ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

Відповідно до статті 7 Закону України «Про Національний банк України» [1] однією з функцій НБУ є визначення особливостей функціонування банківської системи України в разі введення воєнного стану чи особливого періоду, здійснення мобілізаційної підготовки системи Національного банку. На виконання цієї функції був створений певний нормативний масив щодо забезпечення мобілізаційної готовності центрального банку і банківської системи держави, однак можливість

його застосування розглядалася як мало ймовірна, а відтак – недостатньо уваги приділялося детальній регламентації правовідносин.

В умовах фактичного виникнення надзвичайних умов функціонування держави у цілому та її банківської системи зокрема, гостро постала проблема приведення банківського законодавства у відповідність до потреб практики. Тому протягом 2014 року Національним банком України було прийнято низку нормативно-правових актів, спрямованих на забезпечення функціонування банківської системи в надзвичайних умовах. Так, зокрема, постановою Правління НБУ від 22 липня 2014 року № 435 затверджено Інструкцію щодо організації роботи банківської системи в надзвичайному режимі (далі – Інструкція) [2]. В преамбулі зазначеної постанови вказано, що вона прийнята з метою забезпечення функціонування банківської системи України та безперебійного фінансування потреб держави та життєдіяльності населення в умовах надзвичайного режиму роботи. При цьому поняття «надзвичайний режим роботи» в Інструкції чітко не визначено. Водночас з контексту п. 2 цього нормативно-правового акта випливає, що йдеться про порядок роботи банківської системи у разі виникнення нештатного режиму, що унеможливлює роботу банківської системи у звичайному порядку. Зокрема, відповідно до п. 12 Інструкції її вимоги можуть використовуватися в діяльності Національного банку та банків в особливий період. Надзвичайний режим роботи банківської системи України запроваджується постановою Правління НБУ.

Аналіз змісту Інструкції засвідчує, що нею врегульовано загалом п’ять блоків питань, пов’язаних з функціонуванням банківської системи в нештатному режимі:

1. Управління НБУ грошово-кредитним та валютним ринком.
2. Особливості функціонування системи електронних платежів (СЕП).
3. Порядок організації роботи з готівкою в банківській системі.
4. Особливості роботи інформаційних систем НБУ.
5. Організація та ведення бухгалтерського обліку.

Основну увагу НБУ зосередив на безпеці безготівкових розрахунків та схоронності готівки. Детально регламентовано порядок дій банківських працівників при виникненні загрози захоплення приміщення банківської установи озброєними особами. Зокрема регламентовано процедуру знищення або пошкодження готівки у разі неможливості її вивезення у безпечне місце.

Не заперечуючи важливості заходів, спрямованих на збереження цінностей та недопущення протиправного заволодіння ними в надзвичайних умовах, зазначимо, що НБУ залишив поза увагою

можливість втрати документації, яка містить банківську таємницю.

Відповідно до статті 61 Закону України «Про банки і банківську діяльність» [3] банки зобов'язані забезпечити збереження банківської таємниці. Постановою Правління НБУ від 14 липня 2006 року № 267 затверджено Правила зберігання, захисту, використання та розкриття банківської таємниці [4]. Однак при цьому вимоги щодо захисту інформації, яка містить банківську таємницю, в надзвичайних умовах функціонування банківської системи не визначено.

Отже, на наш погляд, доцільно доповнити Інструкцію окремим розділом, в якому будуть визначені заходи, спрямовані на недопущення втрати документів, які містять банківську таємницю.

В умовах надзвичайного режиму роботи, поряд із заходами, передбаченими Інструкцією і розрахованими на застосування виключно в межах цього режиму, особливого значення набувають і інші заходи, які передбачені законодавством для забезпечення стабільності банківської системи. Так, зокрема, надзвичайні події в державі, як правило, супроводжуються збільшенням кількості банків, які набувають ознак проблемних, а згодом, – неплатоспроможних. При цьому, відповідно до ч. 3 статті 75 Закону України «Про банки і банківську діяльність» рішення Національного банку України про віднесення банку до категорії проблемного є банківською таємницею. Така позиція законодавця цілком виправдана, адже проблемний банк може протягом встановленого строку відновити свою нормальну діяльність. Натомість вільне поширення інформації про віднесення банку до категорії проблемних здатне спричинити ефект паніки серед його вкладників, що неминуче призведе до неплатоспроможності банку з наступним виведенням його з ринку. Водночас положення ч. 3 статті 75 не узгоджується зі змістом ч. 1 статті 60 Закону України «Про банки і банківську діяльність», що змушує ставити питання про необхідність вдосконалення законодавчого визначення банківської таємниці.

Література

1. Про Національний банк України: Закон України від 20.05.1999р. № 679-XIV. URL: http://zakon.rada/gov/ua

2. Про затвердження Інструкції щодо організації роботи банківської системи в надзвичайному режимі: постанова Правління НБУ від 22.07.2014р. № 435. URL: http://zakon.rada/gov/ua

3. Про банки і банківську діяльність: Закон України від 7.12.2000р. № 2121-III. URL: http://zakon.rada/gov/ua

4. Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: постанова Правління НБУ від 14.07.2006р. № 267. URL: http://zakon.rada/gov/ua

УДК 65.012.8:004.056.5:330.42

Жуйкова К.В.
Національна академія Служби безпеки України
Гулак Г.М.
кандидат технічних наук, доцент
Національна академія Служби безпеки України

РАЦІОНАЛЬНЕ УПРАВЛІННЯ РЕСУРСАМИ ДЛЯ ОНОВЛЕННЯ АПАРАТНОЇ ТА ПРОГРАМНОЇ ПЛАТФОРМ ЗАХИЩЕНИХ АСУ ТВ

Швидке моральне старіння апаратної і програмної платформ (АПП) у сучасних автоматизованих системах управління технологіями виробництва (АСУ ТВ), відбувається набагато швидше їх фізичного зносу, що обумовлено об'єктивним трендом сучасності: необхідністю обробляти більше інформації за менший проміжок часу в умовах обмежень на ресурси та зростання кількості та сили кібератак. Отже, перед підприємствами багатьох сфер суспільного виробництва, включаючи паливно-енергетичний комплекс, виникає проблема визначення раціонального шляху оновлення (апгрейда) АПП в захищених АСУ ТВ, як процесу прийняття рішення у виборі конкретних продуктів (засобів, модулів, комплектуючих), які відповідають встановленим функціональним вимогам та критеріям з безпеки, в умовах фінансовим обмежень. Наведене обумовлює актуальність розв'язку поставленої задачі.

Розглянемо задачу забезпечення припустимого рівню запобігання атакам (L) (%) залежно від виду експлуатованої АПП в АСУ ТП і вибору конкретних засобів у множині запропонованих в умовах раціонального використання фінансових ресурсів, що виділяються на придбання та оновлення АПП.

Кошти (Q) (грн.), що потрібні для придбання АПП та/або їх оновлення залежать не тільки від їх ціни, а й архітектури системи та від встановленої величини/відсотка запобігання атак $(L_э)$.

Використовуючи метод апроксимації функцій та принцип мінімаксних значень у роботі знайдено рішення поставленої задачі.

Для визначення оптимальної величини коштів Q_{opt1}, при якому придбання та/або оновлення АПП виявиться найбільш ефективним [1, 2] і для спрощення розрахунків, функцію зростання кількості реалізованих атак $L_{p1} = f_1(Q)$ подано у вигляді лінійної:

$$L_{p1}(Q) = L_{p1_0} + Q / K_1, \qquad (1)$$

а криву $L_{э1} = f_1(Q)$ у вигляді спадної функції:

$$L_{э1}(Q) = L_{э1_0} + 1/K_2 Q, \quad (2)$$

де

$L_{э1_0}$ і L_{p1_0} – величини, що визначають певний початковий рівень успішних атак, що залежать від створеної системи захисту,

K_1 – коефіцієнт, що враховує успішні атаки в залежності від технічних характеристик АПП, що пропонується до застосування та/або оновлення,

K_2 – коефіцієнт, що враховує успішні атаки від виду застосовуваної АПП.

У точці оптимуму витрати $L_{э1_{opt}} = f_1(Q_{opt1})$ і $L_{p1_{opt}} = f_1(Q_{opt1})$ рівні: $L_{э1_{opt}} = L_{p1_{opt}}$.

Якщо постійні успішні атаки однакові і не залежать від технічних характеристик техніки, то:

$$(K_2 / K_1) * Q^2 - 1 = 0, \quad (3)$$

звідки точка оптимальних витрат буде визначатися виразом:

$$Q = \sqrt{K_1 / K_2}. \quad (4)$$

Таким чином, співвідношення коефіцієнтів і збільшення цього співвідношення повинно узгоджуватися з купівельною спроможністю підприємства. В цьому випадку оновлення є найбільш ефективним, ніж придбання нового устаткування або ПЗ

Література

1. Жуйкова К.В. Оценка влияния качественных параметров техники на оптимальный объем средств лизинга // Економіка розвитку. Харківський державний економічний університет. – 2002 р. - № 1. – с.24-26

2. Підготовка та проведення лізингових операцій в сфері екології Практичні рекомендації. Сосюрко Ю.В. та ін. Київ: Аверс, 2000. 215 с.

Коломайко А.Є.

Національна академія Служби безпеки України

ПЕРСОНАЛ ЯК ДЖЕРЕЛО ВИТОКУ ІНФОРМАЦІЇ

Людина була завжди найуразливішим об’єктом для загроз витоку та втрати інформації. Можна встановити найсучасніші системи технічного захисту, видати мільйони нормативних актів, які регулюють захист інформації, але доки буде ігноруватися людський фактор (тобто фактор людського впливу на інформацію, загрози, які йдуть від людей та причини цих загроз), доти юридичні, організаційні та технічні засоби будуть мало ефективними. Персонал органі-

зації частіше всього стає причиною витоку інформації [1].

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги до персоналу.

На сьогоднішній день існує все більше і більше можливостей отримання інформації, в тому числі й інформації з обмеженим доступом (тобто такої інформації, витік якої може завдати шкоди її власнику). З'являється все більше загроз витоку даних. А з розвитком новітніх технологій способи їх отримання постійно вдосконалюються.

Отже, існує і багато засобів, що повинні забезпечувати захист інформації з обмеженим доступом. Крім технічних засобів захисту є безліч інструкцій, правил, які регламентують поводження із такою інформацією, а також є ціла низка нормативних актів, з яких ці інструкції випливають.

Для кращого розуміння можливостей витоку інформації та визначення способів його попередження необхідно розглянути класифікацію загроз, пов'язаних з персоналом.

Такі загрози поділяються на зовнішні і внутрішні загрози підприємства, які пов'язані з персоналом. Зовнішньою загрозою є така загроза, що знаходиться за межами підприємства, але саме через існування якої потрібно захищати інформацію і через яку існують загрози внутрішні. Адже, як би не було зацікавлених осіб в отриманні інформації підприємства, її не потрібно було б захищати. До зовнішніх загроз можна віднести протиправну діяльність кримінальних структур, конкурентів, фірм або приватних осіб, що займаються промисловим шпигунством та соціальною інженерією.

До внутрішніх загроз відносяться дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними та потенційними партнерами (аж до втрати цінних контрактів) тощо.

До зовнішніх відносяться:

а) промислове шпигунство. Західні теоретики розуміють під «промисловим шпигунством» добування законним і незаконним шляхом у конкуруючих фірм (монополій, політичних партій, фізичних та юридичних осіб, правоохоронних органів тощо) відомостей або інформації у сфері наукових досліджень, виробництва продукції за найбільш перспективними технологіями тощо, а також персональних даних з метою їх використання у конкурентній боротьбі або у

корисливих цілях [3];

б) соціальна інженерія – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним. Зловмисник отримує інформацію, наприклад, шляхом збору персональних даних про службовців об'єкту атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця.

2) Внутрішні:

а) Необережність персоналу. Дуже часто співробітники, хоч й не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього.

Тож необережність можна поділити на дві категорії:
- дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації;

-дії чи бездіяльність співробітників у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки.

В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії.

б) Умисні дії працівників по розголошенню інформації та мотиви цих дій.

На відміну від необережності, умисел передбачає, що метою дій співробітників було саме розголошення інформації, що є конфіденційною.

Для того щоб виявити або попередити такі дії, потрібно визначитися, чому ж саме працівники пішли на них. Кожна людина є індивідуальною, в кожного своє життя та свої проблеми, через які він приймає ті чи інші рішення. Тож кожна ситуація має свої нюанси, але є декілька розповсюджених причин для розголошення інформації співробітниками. До них відносяться: помста; матеріальна або інша вигода; самореалізація.

Тож загроза цілісності інформації йде від людини. Можна встановити найсучасніші системи технічного захисту, видати мільйони нормативних актів, які регулюють сферу захисту інформації, впровадити інші засоби та заходи захисту на підприємстві але без належної ефективної роботи з персоналом, який працює на підприємстві неможливо забезпечити його інформаційну безпеку.

Література

1. Нечаюк, Л. І. Готельно-ресторанний бізнес: менеджмент [Електронний ресурс]. – Режим доступу: http://tourlib.net/books_ukr/

2. Тарас Ткачук «Шляхи запобігання та протидії промисловому шпигунству» Бизнес и безопасность №3/2007 – 7с.

Кролевецька І.А.
Національна академія Служби безпеки України

ПРОМИСЛОВЕ ШПИГУНСТВО: МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ

Промислове шпигунство є невід'ємною частиною бізнесу, так як конкурент поривається досягти більш високого становища на ринку, яке займає лідируюча фірма. Конкурент часом вдається до заволодіння конфіденційною або комерційною інформацією лідируючої фірми, для того що б наздогнати або обігнати її в економічному зростанні. При цьому рівень впливу промислового шпигунства зростає з року в рік і вдосконалюється, виходячи з росту інформаційних технологій і засобів їх застосування.

Промислове (комерційне) шпигунство – один з видів недобросовісної конкуренції, який є досить поширеним у сучасному світі. Промислове шпигунство є діяльністю із незаконного добування відомостей, що становлять комерційну цінність.

Відповідно до ст. 16 Закону України «Про захист від недобросовісної конкуренції» неправомірним збиранням комерційної інформації вважається збирання протиправним способом відомостей, що становлять відповідно до законодавства України комерційну таємницю, якщо це завдало чи могло завдати шкоди суб’єкту господарювання [1].

Для суб’єктів, які мають намір отримати доступ до конфіденційної або комерційної інформації характерні ознаки оперативної роботи, зокрема: незаконне проникнення на територію конкурента, знаття інформації з каналів зв’язку, стеження, підкуп, шантаж, викрадення інформації тощо.

Сукупність методів, притаманних промисловому шпигунству, можна об’єднати в дві групи:

- Агентурні методи (вивідування потрібної інформації у фахівців конкурентів; переманювання фахівців для отримання від них інформації; підкуп співробітників з закритих підрозділів конкурента; засилання агентів на фірму або в оточення провідних фахівців; викрадення креслень, документів і зразків виробів; негласний контроль за діловою кореспонденцією);
- Технічні методи (апарати звукового контролю (радіозакладки); техніку, призначену для зняття інформації з вікон спеціально звукозаписною апаратурою та використанням мікрофонів різного призначення і дії; прилади для зняття інформації з телефонних ліній зв'язку; спеціальне обладнання для спостереження і передачі відеозображень; спеціальні фотоапарати, прилади, призначені для спо-

стереження в денний час і прилади нічного бачення, телевізійні системи далекого спостереження; використання комп'ютерних програм, вірусів та несанкціонований доступ до АС і мереж компанії та електронної пошти співробітників) [2].

Захиститися від промислового шпигунства досить складно, особливо в нашій країні, оскільки українські компанії часто не готові витрачати значні кошти на технічні системи захисту інформації. Однак без попередження випадків промислового шпигунства не обійтися, мабуть, жодному підприємству, у користуванні якого є відомості, які можуть являти собою комерційну таємницю або конфіденційну інформацію, розголошення якої може завдати істотних економічних збитків.

Кожне підприємство повинно не допускати негативних наслідків промислового шпигунства в своєму бізнесі і для цього йому необхідно розробляти способи захисту від промислового шпигунства. Підприємство створює власну службу безпеки, яка розробляє політику безпеки підприємства, положення про комерційну таємницю, що вбачають методи щодо захисту від промислового шпигунства з урахуванням особливостей діяльності та розташування підприємства [3].

Правильно розроблена стратегія щодо захисту підприємства службою безпеки, завжди застереже його від зовнішніх загроз конкурентів. Крім технічного забезпечення безпеки підприємства, потрібно надавати довіру співробітникам, забезпечуючи їм комфортні умови праці і стимулюючи їх працю. Під створенням комфортних умов розуміється не тільки технічне оснащення приміщення, а й людський фактор, тобто створення позитивного мікроклімату в колективі - дружелюбність, згуртованість, підтримка, взаємодопомога, прагнення виконувати завдання спільно. Під стимулюванням співробітників мається на увазі стабільність в роботі та достойна заробітна плата, підвищення кваліфікації, можливість самореалізації, просування по кар'єрних сходах, грошові винагороди (надбавка до заробітної плати, премії за вдало виконані роботи) і т.д. [4].

Поєднавши разом технічні та людські фактори, підприємство може забезпечити високу ступінь безпеки, ефективність роботи і процвітання подальшого бізнесу.

Література

1. Закон України «Про захист від недобросовісної конкуренції» 236/96-вр від 03.03.2016. URL: http://zakon2.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80 (дата звернення: 16.04.2017).

2. Ярочкин В.И., Бузанова Я.В. Системы защиты предпринимательства: защиты от недобросовестной конкуренции. М.: Фонд «Мир». 2005. 254 с.

3. Промислове шпигунство: профілактика, оперативне правове реагування, от 30.09.2016/Ілляшев та партнери. URL: http://attorneys.ua/uk/publications/industrial-epionage-prevention-rapid-legal-response/ (дата звернення: 16.04.2017).

4. Захист від промислового шпигунства / Premier Alliance security & investigation agency. URL: https://premier-alliance.biz/uk/spetsializatsiyi/informatsiyniy-zahist/zahist-promislovogo-shpigunstva/ (дата звернення: 20.04.2017).

УДК 316.422

Мосьпан А.О.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»
Скоропад С.І.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»

АНАЛІЗ ПОНЯТІЙНОГО АПАРАТУ В ОБЛАСТІ ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Соціальна інженерія як метод несанкціонованого доступу до захищених інформаційних ресурсів, базується на способах впливу на людську психологію.

Людину, яка використовує у своїй діяльності методи соціальної інженерії, можна назвати соціальним інженером.

Соціальний інженер – фахівець широкого профілю, який зазвичай є порушником інформаційної безпеки, вміє впливати на людину, навчений збирати необхідну інформацію будь-якими способами. Вже сьогодні, можна виділити ряд галузей, в яких використовується соціальна інженерія.

Особистісне проектування (створення життєвої стратегії, профорієнтація, супровід особистісних криз і перепрограмування, соціалізація та вирішення конфліктів в колективі). Особистісне проектування ставить завданням побудову і супровід особистої життєвої стратегії, що якнайкраще відповідає вимогам і ходу мислення особистості, її зазвичай прихованим амбіціям, архетипам і сенсообразам.

Психотерапія міжособистісних і корпоративних відносин – досить розвинена галузь.

Організаційне проектування (створення і трансформація організацій – інституційних і корпоративних структур). Це діяльність, яка сьогодні формується як окрема галузь.

Консалтинг як галузь включає експертну аналітику, стратегічне

планування, оптимізацію інституційних і корпоративних оргструктур в умовах реальної діяльності, інжиніринг корпоративного та інституційного управління, корекцію стандартної оргструктури для забезпечення просування через неї специфічних проектів, тощо.

Відкрите лобіювання законів і виконавчих рішень – це типова сфера діяльності політичних партій, проте потребує послуг гуманітарних технологів.

Проектний менеджмент – створення проектів під певні соціальні цілі і завдання, відкрите обговорення і просування цих проектів в інститутах масової комунікації, запуск проекту у виконання і поточне управління в рамках існуючого проекту. Розрізняють корпоративний і інституційний менеджмент, стратегічний і поточний менеджмент.

Іміджмейкінг – інженерія ЗМІ, шоу-бізнесу, публічної політики; виробництво сенсообразів і сенс-лінгвістичне конструювання цілих іміджевих компаній, робота з інститутами масової комунікації: проектування компаній для іміджмейкінгу і просування через них заданих образів, розробка рекламних кампаній в контексті створення та просування певного образу або стилю життя, створення і просування нових стилів.

Виробництво і організація комунікації – інженерія інститутів масової комунікації, включаючи комп'ютеризацію та інтернетизацію, соціологічні дослідження, збір та обробку інформації, виробництво новинної і аналітичної публічної інформації (журналістика).

Освіта – вже існуюча галузь індустрії, в якій відбувається комерціалізація (створення приватних структур освіти і надання комерційних послуг в структурах некомерційного освіти). Одним з головних напрямків є виробництво умов і технологій самоосвіти.

Сучасні технічні засоби захисту інформації досягли рівня, коли на злом витрачається багато часу, або ціна захищеної інформації на багато менша витрат на її добування. Вся соціальна інженерія ґрунтується на:

- слабкій безпеці (candysecurity) – термін, введений Белловін і Чесвіком з BellLabs для опису сценарію безпеки, де зовнішня межа, така як брандмауер, міцна, але інфраструктура, розташована за ним, слабка;
- згідно з вітчизняними і зарубіжними джерелами близько 70% (а за деякими джерелами ця цифра ще вище) всіх порушень, пов'язаних з безпекою інформації, відбуваються саме співробітниками підприємства

Проаналізувавши діаграму, мимоволі виникає питання: «Чому співробітник є найбільшим джерелом загроз?» Можна виділити 5 причин цього факту:

- при порушеннях, викликаних безвідповідальністю, співробітник цілеспрямовано або випадково виробляє будь-які дії щодо компрометації інформації, пов'язані зі злим умислом;
- буває, що співробітник підприємства заради самоствердження (для себе або колег) затіває свого роду гру «користувач – проти системи». І хоча наміри можуть бути нешкідливими, буде порушена сама практика безпеки. Такий вид порушень називається зондуванням системи;
- порушення може бути викликано і корисливим інтересом. У цьому випадку співробітник буде намагатися цілеспрямовано подолати систему захисту для доступу до інформації, що зберігається, переробляється і оброблюється на підприємстві;
- відома практика переманювання фахівців, так як це дозволяє послабити конкурента і додатково отримати інформацію про підприємство. Тобто плинність кадрів – четверта причина;
- фахівець, який працює з конфіденційною інформацією, відчуває негативне психічний вплив, обумовлений специфікою цієї діяльності. Виконуючи вимоги режиму секретності, співробітник змушений діяти в рамках обмеження своєї свободи, що може привести до стресів і психологічних зривів.

Література

1. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. / [О.М.Богданов, В.М.Петрик, Д.В.Пахольченко] / за заг. ред. В.М.Петрика. – К.: Вид-во ІСЗЗІ КПІ, 2017. – 60

УДК 336.71

Олійник Ю.С.
Національна академія Служби безпеки України

СУЧАСНЕ РОЗУМІННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

На сьогоднішній час існують вже традиційні поняття із захисту інформації. Безпека інформації за суттю - є стан інформації, інформаційних ресурсів, інформаційних та телекомунікаційних систем (конфіденційність, цілісність та доступність). А вже захист інформації означає сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Тобто, це діяльність, що спрямована на забезпечення безпеки інформації. Тож переходячи до поняття, такого як інформаційна безпека, стисло можна сказати що це поєднання, гібрид, двох по-

нять, а саме: безпеки інформації та захисту інформації. Та якщо ми порівняємо це визначення з визначенням з міжнародних стандартів, то побачимо, що там не виокремлюються цих два поняття. Перше: інформаційна безпека - стан захищеності життєве важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1]. Друге визначення, яке дає нам міжнародний стандарт більш стисле: інформаційна безпека - збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність [2].

Як же ми розуміємо поняття кібербезпека? Багато фахівців та науковців, що досліджують дане питання приходять до зовсім протилежно різних визначеь. Детальніше пояснимо декілька з них.

Перше - нічого нового. Численні фахівці з комп'ютерної безпеки вважають, що кібербезпека (або кіберзахист) – це лише новий термін, який означає саме те, чим вони займались протягом останніх десятиліть. А також існує думка, що нові слова допомагають збільшити фінансування.

Друге - кібербезпека - безпека кібернетичних систем. Суттєва мета кібернетики - це розуміння і визначення функцій та процесів систем, які мають мету і які беруть участь у циклічних ланцюгах, що переходять від дії до сприйняття, далі до порівняння з кінцевою метою, і знову до дії. Кібернетика охоплює багато різних дисциплін, деякі з яких дійсно є можливими цілями для кібератак. Наприклад: штучний інтелект, робототехніка, системи керування, системи підтримки прийняття рішеньта соціальні системи.

Третє - кібербезпека включає наступальні дії, котре ще має на увазі також зниження кіберризиків.

Та четверте - кібербезпека - безпека інформації у кіберпросторі.

Але все ж таки існує найбільш загально прийняте поняття, котре виражене у наступному вигляді. Під кібербезпекою розуміють властивість захищеності активів від загроз конфіденційності, цілісності, доступності у кіберпросторі [3].

Кіберпростір – це комплексне віртуальне середовище, що не має фізичного втілення, сформоване в результаті діяльності людей, програм і сервісів в мережі Інтернет шляхом мережних і комунікаційних технологій [3].

В Україні теж є своє визначення даного терміну, яке знаходить-

ся в проекті Закону України. Кібербезпека - стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі [4].

Так як ми розглядаємо кібербезпеку в контексті захисту, слід розглянути ще таке поняття як кіберзагроза, яке теж наявне в цьому проекті. Кіберзагроза - наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці [4].

Аналізуючу світову практику з даної теми, можна зробити висновок, що розрізняють такі види кіберзагроз: таргетовані атаки (Advanced Persistent Threat), кібертероризм (вплив на системи керування), кібервійни, хактивізм, зловживання у соціальних мережах (вплив на суспільство), атаки на банківські системи (викрадення грошей), атаки на електронний уряд, апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання.

І як приклад, можна навести одну з найцікавіших та небезпечних реалізованих кіберзагроз. У 2010 році було виявлено шкідливе програмне забезпечення Stuxnet, яке продемонструвало реальність загроз, які до того вважали лише уявними. Деякі її характеристики: програма була здатна атакувати локальні мережі, не підключені до Інтернету; програма була призначена для атаки на промислове обладнання ядерного об’єкта; програма була розроблена великою і добре скоординованою групою розробників.

Пізніше виявили зразки програмного забезпечення, яке мало розвідувальні функції, і було розроблене такими ж великими і професійними группами. Приклади таких програмних засобів – DuQu, Flamer, Red October.

Як з’ясувалось, деякі з масштабних розвідувальних операцій у кіберпросторі проводились протягом майже десяти років.

Таким чином, кіберпростір вже став територією активного протистояння і будь-які сучасні комп’ютерні системи є вразливими. Атаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп’ютерних систем. Виявлення таких атак ускладнюється тим, що вони здійснюються на обмежену кількість спеціально визначених цілей, не викликають збоїв і відмов комп’ютерів, і тому тривалий час не потрапляють у поле зору дослідників з антивірусних лабораторій. Сьогодення показує, що методи захисту не завжди ефективні і вимагають розвитку та постійного оновлення (адаптації).

Література

1. Закон України від 09.01.2007 № 537-V «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

2. ДСТУ СУІБ 1.0/ISO/IEC 27001:2010, Інформаційні технології - методи захисту - система управління інформаційною безпекою, офіційний переклад.

3. ISO/IEC 27032:2012, Information technology - Security techniques - Guidelines for cybersecurity.

4. Проект Закону України від 20.09.2016 № 1524-VIII «Про Основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.

Омельчук І.В.

Національна академія Служби безпеки України

ВПЛИВ ЗМІ НА СУСПІЛЬНУ ДУМКУ ЯК ІНФОРМАЦІЙНА ЗАГРОЗА

Сучасне суспільство важко уявити без щоденного «підкріплення» порцією свіжих новин. Це дає змогу бути в курсі останніх регіональних і світових подій та тенденцій, а також в певній мірі формує світогляд. Чи замислювалися ми чому виникає певний контраст подачі у різних ЗМІ однієї і тієї ж події чи факту?

Часто можна помітити, що різні ЗМІ диктують нам своє бачення подій, що впливає на погляди не лише окремої людини, а й цілих спільнот і суспільства. Так, певний підбір слів та спосіб (формат) подачі новин може створювати однобоке «бачення» світу, навіть у тому випадку, коли інформація достовірна. Це відповідним чином впливає на людей і може сформувати необ’єктивне ставлення до того, що відбувається, чим створюється одна із наймасштабніших сучасних загроз інформаційній безпеці.

У сучасному суспільстві ЗМІ виконують низку важливих функцій, зокрема комунікативну, інформаційну. Завдяки цьому здійснюється вплив на всі сфери життєдіяльності суспільства, на соціально-психологічний і духовно-культурний розвиток кожного члена суспільства, тому що кожна нова інформація, що надходить по каналах ЗМІ, відповідним чином стереотипізована й несе в собі багаторазово повторювані ціннісні орієнтації й установки, що закріплюються у свідомості людей [3].

Зазвичай, ЗМІ використовують фрагментарний або послідовний способи донесення політичної інформації. Якщо послідовний спосіб притаманний переважно для друкованих публікацій, то фрагментарний прийом розповсюджений на телебаченні, що зумовлено об’єктивною потребою в поділі інформації для різностороннього й оперативного її подання. Фрагментарний метод часто перешкоджає

більшості громадян виробити цілісну картину політичних факторів та подій і, врешті-решт, дезорієнтує глядачів, викликає в них політичну байдужість та апатію, змушуючи вірити оцінкам політичних коментаторів. Все це створює сприятливі умови для маніпулювання свідомістю, досить поширеного в діяльності сучасних мас-медіа в Україні.

Як основний елемент управління громадською думкою ЗМІ найчастіше використовують відволікання уваги людей від вагомих проблем і рішень, прийнятих політичними та економічними правлячими колами за допомогою постійного насичення інформаційного простору незначущими повідомленнями. Вони самі створюють проблему, якусь ситуацію, розраховану на те, щоб спровокувати певну реакцію серед населення. Аби воно само забажало вжиття заходів, які потрібні правлячим колам або іншими конкретним суб'єктам.

При донесенні до громадськості будь-якого матеріалу про конкретну подію сьогодні часто спостерігається як ЗМІ висвітлюють лише негатив, умисно зосереджуються на «роздмухуванні» скандалу, забуваючи про те, що дотримуючись принципу об'єктивності у поданні інформації необхідно повідомляти суспільство про позитивні зміни та події [4].

Аналізу способів та форм психологічного впливу мас-медіа на суспільство сьогодні присвячується багато робіт вітчизняних і зарубіжних учених.

Зокрема одним із найнебезпечніших проявів такого впливу є використання ЗМІ в процесі терористичної діяльності. Адже важливим фактором природи тероризму є те, що теракт передбачає емоційний вплив на суспільну думку. Він породжує жах, панічний настрій, веде до втрати довіри до влади, що викликає політичну нестабільність. ЗМІ найбільш ефективні для здійснення впливу на великі маси людей, що дає привід розглядати їх як частину стратегічного потенціалу тероризму. Результативність інформаційного впливу, який здійснюється за допомогою мас-медіа, пояснюється сильними психологічними ефектом причетності до подій, коли людина поринає в них «тут і зараз» (ефект CNN) [1].

Постає головне питання, а чи можемо ми захистити свої інформаційні інтереси на правовому рівні від негативного впливу ЗМІ?

Так, прийнята нещодавно Доктрина інформаційної безпеки визначає деякі положення щодо ЗМІ, пункт 6 якої окреслює роль відповідних уповноважених державних органів у сфері контролю за ЗМІ та захисту українського інформаційного простору.

Але як це все має працювати? Щодо Служби безпеки України, то зі слів заступника міністра інформполітики Д. Золотухіна: «Схема дуже проста: Служба безпеки України виключно в рамках своїх

повноважень виявляє в текстах веб-сайтів інформацію, яка містить заклики до повалення конституційного ладу або до порушення територіальної цілісності України, фіксує їх в рамках внутрішньовідомчих документів, створює відповідну документацію до них і реалізує цю документацію, пишучи листи, наприклад, на адресу Інтернет асоціації України, яка є внутрішнім регулятором цієї спільноти и виступає як провідник саморегулювання галузі. Інтернет асоціація України, отримуючи ці листи, готує своїм учасникам – провайдерам, відповідні месиджі, і далі вже учасники спільноти в рамках знову ж таки законодавства і в рамках своїх прав можуть реагувати або не реагувати на ці листи, оскільки вони не обов'язкові до виконання. І є патріотчно налаштовані провайдери, які реагують на ці листи, і, використовуючи свої технічні можливості» [2].

Тобто можна зробити висновок, що перші кроки у побудові правового захисту суспільства від інформаційних потоків засобів масової інформації вже починають розроблятися і втілюватися в життя. Про їх ефективність наразі важко оцінити, адже вплив ЗМІ виявляється не тільки у Інтернеті, але й на телебаченні та у пресі, при цьому досконалих правових механізмів захисту населення від деструктивного впливу на свідомість людини немає.

Таким чином ЗМІ сьогодні – це певний своєрідний інформаційний світ, який встановлює свої правила та може різними способами ефективно впливати на формування суспільної думки, що само по собі вже накладає на журналістів високий моральний обов’язок щодо подання повної, достовірної, своєчасної, різнобічної інформації, яка забезпечуватиме об’єктивне ставлення людей до важливих для суспільства подій.

Література

1. Власенко О.В. Фактори негативних інформаційних впливів на громадян України. [Електроний ресурс]. – Режим доступу : http://www.academy.gov.ua/ej/ej8/doc_pdf/vlasenko.pdf

2. Золотухін Д.Ю. Воювати з Росією “баблом” – марна справа. Потрібно боротися мізками. [Електроний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-society/2192348-dmitro-zolotuhin-zastupnik-ministra-informacijnoi-politiki-ukraini.html

3. Карлова В.В. Вплив засобів масової інформації на формування української національної свідомості. [Електроний ресурс]. – Режим доступу : http://www.academy.gov.ua/ej/ej6/txts/07kvvunc.htm

4. Кравчук В.М. Вплив ЗМІ на формування громадянської свідомості / В.М. Кравчук, О.А. Дмитрусь // Юридичний науковий журнал. – 2015. – №6. – С.17.

УДК 681.3.06

Пахольченко Д.В.
Інститут спеціального зв'язку та захисту інформації
НТУУ «КПІ ім. Ігоря Сікорського»

ЗАСТОСУВАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ НА ПРИКЛАДІ ГРИ «СИНІЙ КИТ»

У даній доповіді я намагатимусь викласти позицію авторів стосовно гри «Синій кит», яка набуває все більш широке поширення в нашій країні, з точки зору застосування соціальної інженерії.

Вже багато місяців поспіль у Мережі обговорюють підліткову гру «Синій кіт», або ж «Тихий дім», «Море китів», «Розбуди мене о 4:20». У смертельної «гри» багато назв, але результат завжди однаковий – смерть підлітків і зламані горем батьки, які не розуміють, що ж змусило їхню дитину звести рахунки з життям.

Потрапити в «гру» було дуже просто. Дітей вербували в різних групах соціальної мережі «ВКонтакте», або ж дитина могла сама «призвати» так званих кураторів «гри», написавши на своїй особистій сторінці повідомлення з певним хештегом: #синийкит #яждуинструкций #тихийдом та іншими варіаціями. Далі з дітьми просто починали листування, переконували їх у власній унікальності та самотності, потім пропонували зіграти в «гру».

Одним з перших завдань «гри» було надіслати свою геолокацію. Далі вишкрябати лезом кита на руці, прокинутись о 4.20, піднятися на дах. Як докази дитина повинна була робити фотозвіт виконаних завдань. Якщо дитина відмовлялась виконувати будь-яке із завдань і зіскакувала з гачка, куратор «гри» починав погрожувати розкрити листування, опублікувати інтимні фото, які також були у списках «завдань» та особисто розправитися з підлітком, або завдати шкоди його сім'ї. За даними кіберполіції кількість подібних завдань варіюється від 13 до 50.

На думку авторів організатори таких груп переслідують одну мету – збагачення, а дана «гра» є яскравим прикладом застосування соціальної інженерії. Одним із завдань для підлітків є надання куратору «гри» даних платіжної картки їхніх батьків, що є персональною інформацією кожного користувача будь якого банку, відповідно до Закону України «Про захист персональних даних».

Кураторів даною «гри» можна сміло назвати соціальними інженерами. Для здійснення своїх цілей, вони використовують мережу Інтернет та телефонний зв'язок як інтерактивні вектори нападу для спілкування та підтримання контакту з гравцями, а також особисті

підходи, адже потрібно застосовувати індивідуальний підхід до кожного гравця, враховуючи його стать, вік та вподобання. Також куратори «гри» використовують прямі види атак, такі як введення в оману та шантаж, адже гра засновується на тотальній брехні та погрозах на адресу рідних [1].

Майже всі сім'ї, які пережили суїцид дитини, стверджували, що взаємини у сім'ї були «гарні» і що вони не бачили нічого незвичайного. Однак згідно статистики, учасниками так званих «груп смерті» ставали діти, які не отримували достатньо уваги з боку батьків.

Тому саме для батьків учнів старших класів ліцею № 142, що знаходиться у місті Київ та особливо для батьків «у віці», а також інших не байдужих, був проведений відкритий урок на тему «Запобігання участі ваших дітей, в так званих групах смерті». І одним із питань, яке виносилось на розгляд, були саме рекомендації щодо захисту їхніх платіжних банківських карток. Адже, окрім того що існує можлива загроза життю їхніх дітей, вони на початковому етапі можуть втратити значну суму свої заощаджень.

Висновки: сьогодні «Синій кит», а завтра вже може бути «Білий дельфін», або ще якась назва. Концепція даних ігор приблизно однакова, але сенс механізмів протидії їм повинен базуватися на тому, що у багатьох підлітків можуть траплятися проблеми у житті, які здаються їм нерозв'язними. Тоді вони найбільше потребують підтримки і любові своїх близьких людей – не показової і оптимістичної, а небайдужої і кваліфікованої допомоги в розумінні себе і світу.

Література

1. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. / [О.М.Богданов, В.М.Петрик, Д.В.Пахольченко] / за заг. ред. В.М.Петрика. – К.: Вид-во ІСЗЗІ КПІ, 2017. – 60 с.

УДК 327.84: 351.88

Пістрюга Т.В.
Воєнно-дипломатична академія
імені Євгенія Березняка

ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЗАРУБІЖНИХ КРАЇН ДЛЯ ВИРІШЕННЯ ЗАДАЧ РОЗБУДОВИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ УКРАЇНИ

Доктриною інформаційної безпеки України визначено одним з пріоритетів державної інформаційної політики побудову дієвої та ефективної системи стратегічних комунікацій та недопущення вико-

ристання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні [1]. Інтеграція національного інформаційного простору у європейський і світовий простір з розвитком системи стратегічних комунікацій України актуалізує необхідність об'єктивного оцінювання українськими спеціальними службами стану інформаційного простору (ІП) зарубіжних країн. Не зважаючи на чисельність робіт, які характеризують інформаційну політику різних держав та розвиток технологій контент-аналізу, єдиного методичного підходу до оцінювання стану ІП країни, який задовольняє потреби спеціальних служб не існує. Проте його вироблення бачиться принципово необхідним для виявлення ризиків та загроз національним інтересам України в інформаційній сфері, які породжуються у ІП зарубіжних країн. Також вироблення програм інформаційної інтеграції неможливе без комплексного оцінювання стану ІП країни-партнера.

Дослідження існуючих підходів до оцінювання інформаційних процесів в зарубіжних країнах вказує на ефективність методик, які ґрунтуються на визначенні рівня свободи функціонування ЗМІ у певній країні. Вважається, що такий показник безпосередньо впливає на світові інтеграційні процеси та стратегічні комунікації в інформаційній сфері. Найчастіше використовуються рейтинги міжнародних неурядових організацій "Reporters sans frontières" (штаб квартира – м. Париж) та "Freedom House" (штаб квартира – м. Вашингтон).

Спробуємо проаналізувати, наскільки запропоновані ними методики є придатними для використання спеціальними службами у вирішенні вище окреслених задач, а також можливості їхньої адаптації.

"Reporters sans frontières" (RSF), починаючи з 2002 року розробляє "Всесвітній індекс свободи преси" ("The World Press Freedom Index"), який використовується ЗМІ, дипломатами і міжнародними організаціями. Методика передбачає аналіз свободи ЗМІ на основі оцінки плюралізму, їх незалежності, якості законодавчої бази і безпеки журналістів у 180-ти країнах світу. Індекс формується шляхом інтегральної оцінки відповідей експертів на запитання анкети по кожній країні з урахуванням даних щодо порушень і актів насильств по відношенню до журналістів. Шкала оцінювання передбачає п'ять категорій щодо стану свободи ЗМІ: добрий (good), досить добрий (fairly good), проблематичний (problematic), поганий (bad), дуже поганий (very bad) [2].

Freedom House надає експертно-аналітичне дослідження "Свобода преси" ("Freedom of the Press"). Індекс свободи преси розподіляється за трьома категоріями: "вільні" ("free"), "частково вільні" ("partly free") та "невільні" ("not free") за трьома критеріями: право-

ве (найнижчий бал 30), політичне (40) та економічне (30) середовище [3]. Сьогодні Freedom House також окремо розглядає ситуацію на тимчасово окупованій території АР Крим. Так, згідно з дослідженням "Свобода преси" ситуація на Кримському півострові оцінена як "невільна" з індексом свободи 94, що відповідає мінімальним балам. Окремо звертає на себе увагу той факт, що індекс окупованого Кримського півострова на 11 пунктів нижче, ніж індекс самої держави-агресора [4].

Спеціальні служби України в оцінках режимів у зарубіжних країнах частіше застосовують таку градацію: "помірний", "ускладнений", "жорсткий". Вадою цього підходу є відсутність системи вимірюваних показників. З метою її подолання спробуємо інтегрально встановити відповідності між запропонованими методиками оцінювання стану ІП та прийнятою шкалою. Для аналізу використаємо дані по країнах, які розподілимо за трьома категоріями по відношенню до України: держава-агресор (РФ), суміжні країни (Білорусь, Польща, Словаччина, Угорщина, Румунія, Молдова, Туреччина та Грузія), країни, що впливають на воєнно-політичну обстановку у світі (США та КНР).

Для унаочнення дані двох досліджень за 2016 рік зведемо у таблицю, де країни розташовано в ієрархічному порядку від найвищого до найнижчого індексу. Умовно зазначимо діапазон індексів у відповідності до назв характеристик: від 0 до 50 – "помірний"; від 51 до 100 – "ускладнений"; від 101 до 140 – "жорсткий". Таким чином зведена таблиця оцінки стану ІП іноземних країн у ієрархічному порядку виглядатиме так:

Таблиця 1.

№	**Reporters sans frontiures**	**Freedom House**	**Середні показники**	
1.	Словаччина (12)	США (21)	Словаччина (13)	"помірний"
2.	США (41)	Словаччина (24)	США (31)	
3.	Польща (47)	Польща (28)	Польща (37,5)	
4.	Румунія (49)	Румунія (38)	Румунія (43,5)	
5.	Грузія (64)	Угорщина (40)	Угорщина (53,5)	"ускладнений"
6.	Угорщина (67)	Грузія (49)	Грузія (56,5)	
7.	Молдова (76)	Молдова (56)	Молдова (66)	
8.	РФ (148)	Туреччина (71)	Туреччина (111)	"жорсткий"
9.	Туреччина (151)	РФ (83)	РФ (115,5)	
10.	Білорусь (157)	КНР (87)	Білорусь (124)	
11.	КНР (176)	Білорусь (91)	КНР (131,5)	

*в дужках зазначені індекси країн згідно результатів дослідження вказаних організацій.

Отже у висновку слід зазначити, що спеціальні служби України для вирішення задач в рамках розвитку стратегічних комунікацій держави, повинні проводити об'єктивну оцінку інформаційного режиму в іноземних країнах та мають розробити адаптовану методику оцінювання ІП іноземних країн. Використовуючи дані та методичні підходи RSF та Freedom House спеціальні служби матимуть більш об'єктивний підхід до оцінювання стану ІП іноземних країн.

Література

1. Доктрина інформаційної безпеки України затверджена Указом Президента України від 25.02.2017 року № 47/2017 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua

2. Reporters sans frontières. The World Press Freedom Index. URL: https://rsf.org/en/world-press-freedom-index

3. Freedom House. Freedom of the Press. URL: https://freedomhouse.org/report/freedom-press/freedom-press-2016

4. Freedom House. Freedom of the Press. Crimea. URL: https://freedomhouse.org/report/freedom-press/2016/crimea

УДК 004.023

Прищепа С.В.
Інститут проблем реєстрації
інформації НАН України
Ланде Д.В.
доктор технічних наук, професор
Інститут проблем реєстрації
інформації НАН України

ЕКСТРАГУВАННЯ БЕЗПЕКОВИХ ПОДІЙ З TWITTER

У мережі Інтернет міститься величезна кількість інформації, за допомогою обробки якої можна якісно підвищити швидкість реагування на найрізноманітніші безпекові завдання – перетинання кордону ворожими військами, DOS атаки, теракти та інше. Найбільш швидкими та динамічними у розповсюдженні важливих безпекових подій є соц. мережі Twitter та Facebook.

Інструменти для виявлення подій:

Прикладів якісного виявлення подій не так багато, але вони є. Приклади охоплюють як підходи на основі правил, так і статистичні роботи.

Система EVITA – це інструмент для розпізнавання подій. [1, с. 700–707] Система має добрі показники F1, як для 2005 року, коли вона була вперше презентована. В EVITA використовується попе-

редня лінгвістична обробка та поверхова синтаксична інформація для машинного навчання. Це вимагає створення корпусу з лексем, речень, автоматичну морфологічну розмітку тексту (POS tagging).

TIPSem. Тут використовується семантичне маркування ролей для ідентифікації тимчасово використовуваної мови, а далі використовується підхід структурованого навчання для виявлення подій. [2, с. 725-733]

Система екстрагування подій ATT1 досягла найкращих результатів на TempEval-3 в 2013-му році. Ця система трохи відрізняється від TIPSem. Виявлення подій в цій системі базується, як на семантиці текстів, так і на синтаксичному його розборі. Важливо відзначити, що ATT1 більше спирається на лексичні, ніж на семантичні особливості в тексті. Вона працює на підході послідовного позначення (sequence labeling). [3, с. 20–24]

Наш підхід:

Ми використовуємо спеціальні шаблони і словники, так як, більшість подій мають контекстно-залежне відношення і більшість з них згадується лише в декількох документах, написаних навколо якогось тимчасового інтервалу. Причому, для кожної категорії бажано створювати свій шаблон поведінки і словники під час добування подій певної категорії. Присвоєння певної категорії документу здійснюється методом опорних векторів. Далі відбувається розбиття текстів на ключові слова та фрази. Кожному ключовому слову присвоюємо вагу для даної предметної області по TF-IDF методу.

Для виявлення подій, їх суб'єктів і об'єктів ми створюємо спеціальні шаблони правил розбору речень з певної тематики і словники індикаторів подій з певної теми, які заповнюються з експертом з урахуванням різних лінгвістичних ознак теми (категорії). Індикатори тематичної події представлені словниками. Використовується не один словник індикаторів подій з певної теми, а два. Виділення індикаторів події відбувається за допомогою пошуку індикаторів в реченнях документа з одного з словників присвоєної документу категорії. Використання подвійних словників дозволяє привласнити індикатору події спеціальний аргумент приналежності до одного зі словників, а це дозволяє будувати більш складні шаблони умов і вивести показники точності екстрагування подій на більш високий рівень.

Ми підходимо до питання екстрагування подій, як до виявлення індикаторів (тригерів) події заданих типів і виявлення їх аргументів та зв'язку з фігурантами в реченні, а потім відібрана інформація про ці події розпізнається і об'єднується в єдиному поданні для кожної виявленої події.

Визначимо подію *e*, як кортеж (сутність та дата) + згадка про *e,*

m_e – може бути будь-який твіт, що містить посилання до сутності і написаний в специфічну дату. Особливості події екстрагуються з згадок про подію

$x_e = f(\{m_{e'} | e' = e\})$, які можуть бути використані для оцінки ймовірності що подія відноситься до категорії E, відповідно до деяких заданих параметрамів для категорії, θE.

$$p_{\theta E}(y_e = 1 | x_e) = \frac{1}{1 + e^{-\theta_E \cdot x_e}}$$

Якщо в реченні знайдений індикатор події і хоча-б один фігурант - йде подальший розбір речення - нумерація порядку всіх слів у реченні і присвоєння кожному слову свого порядкового номера. Коли всім сутностям присвоєні типи, аргументи і порядковий номер в реченні - йде підбір якому типу шаблонів відповідає дане речення. Варіанти шаблонів - індикатор тематичної події одного зі словників і варіанти розташування інших перемінних в реченні документу певної категорії. Шаблони для словника №1 і №2 можуть відрізнятися.

Ми розраховуємо на якість виявлення подій на рівні 0,79-0,84 по F1-мірі для текстів українською / російською мовою.

Література

1. Saur´ı, R., Knippen, R., Verhagen, M., and Pustejovsky, J. (2005). Evita: a robust event recognizer for QA systems. с. 700–707.
2. Llorens, H., Saquete, E., and Navarro-Colorado, B. (2010). TimeML events recognition and classification: learning CRF models with semantic roles с. 725–733.
3. Jung, H. and Stent, A. (2013). ATT1: Temporal annotation using big windows and rich syntactic and semantic features. с. 20–24.

УДК 35.078.3

Рагнєв А.О.

Національна академія Служби безпеки України

ПРОБЛЕМАТИКА УКРАЇНСЬКОГО КОНТЕНТУ В НАЦІОНАЛЬНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

Сьогодні людство стрімко вступило в інформаційну еру, тому на передові щаблі виходить інформація. У зв’язку з цим, з’являється необхідність чіткого усвідомлення понять "інформація", "право на інформацію", "інформаційні відносини" та чіткого врегулювання правових аспектів взаємодії цих понять. Особливої актуальності набуває питання захисту українського інформаційного наповнення в національному просторі.

Для початку варто з’ясувати, що таке інформаційна сфера. Під нею розуміють сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, а також системи регулювання відповідних суспільних відносин та відносин, що виникають при: формуванні і використанні інформаційних ресурсів, створенні і використанні інформаційних технологій та засобів їх забезпечення; захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації[1]. Тобто, будь-які відносини, матеріальні і нематеріальні предмети, які хоч якось торкаються інформації, - є складовими інформаційної сфери. Інформаційний ж простір, на думку автора, є більш вузьким поняттям, адже, по-перше, він є територіально визначеним, хоч і не має чітких меж. По-друге, він включає в себе певні скеровані інформаційні потоки і, відповідно, суб'єкти, які цими потоками керують. За територіальною ознакою можна диференціювати інформаційні простори світового, регіональних та національних рівнів. У результаті такого поділу бачимо, що український національний простір є складовою більш масштабнішого інформаційного простору, а тому піддається впливу інших просторів, як одного з ним рівня, так і більших за нього.

Виходячи з викладеного, проблема захисту контенту національного виробництва у державному інформаційному просторі стає все більш актуальною. Як зазначає В. К. Конах: "Аналіз національного інформаційного простору України свідчить, що з часу здобуття незалежності актуальною проблемою залишається його змістовне наповнення (контент). Означена проблема пов’язана з тим, що, з одного боку, він перебуває під тиском низки чинників іноземного походження, а з іншого – характеризується невідповідністю вітчизняного інформаційного продукту світовим критеріям. [2]" Дане питання є предметом як інформаційної безпеки, так і інформаційного права, оскільки без законодавчої підтримки цю проблему вирішити неможливо. Але наріжним каменем є ст. 5 Закону України "Про інформацію", в якій вказано, що кожен має право на інформацію [3].

У зв’язку з цим, надзвичайно важко на законодавчому рівні змусити суб'єктів національного інформаційного простору використовувати і популяризувати саме вітчизняного виробника, якщо таке бажання відсутнє у самого суб’єкта. Можна виділити два чинники цього небажання:

1. Соціокультурний
2. Економічний

Перший рівень відображає в собі причину небажання - непопулярність серед населення, а наслідком цього є відсутність економіч-

ної вигоди для тих, хто б розповсюджував контент (другий рівень). Відсутність економічної вигоди призводить до відсутності бажання популяризувати контент. Відповідно до цього можна помітити замкнутість цієї проблеми. Для того ж, щоб розірвати це коло, необхідно не просто вплинути на суб'єкти розповсюдження інформаційного контенту, а й на самого виробника.

На сьогодні, найбільш доцільними здаються два напрямки впливу:

- На суб’єкти розповсюдження:
  - Економічний(або дотації з держбюджету, або приватні інвестиції)
  - Правовий (імперативні приписи)
- На виробника інформаційної продукції (підвищення національного стандарту якості такого роду продукції)

Отже, враховуючи сучасний стан нашої країни необхідно чітко усвідомити доцільність закріплення провідного місця у національному інформаційному просторі України саме вітчизняного якісного контенту. Дане питання є предметом безпосередньо інформаційної безпеки як однієї з основ здорового розвитку суспільства. У межах соціотехнічної парадигми, інформаційна безпека має три рівня: індивідуальний, загальний і захисний[4]. Відповідно, на кожному з них необхідно зробити певний акцент на усуненні причин відсутності контенту українського виробника в національному інформаційному просторі. Так, на індивідуальному рівні варто підвищувати загальну правову культуру і правосвідомість, здатність адекватно сприймати правову інформацію, а також проводити популяризацію українського контенту серед самого населення - споживача інформації. На загальному рівні - більш детально впорядкувати важливі види інформаційної діяльності, модернізувати правову базу, яка забезпечує визначеність і визнання прав і свобод людини, а також законність і правопорядок в інформаційній сфері, на предмет колізії та прогалин. Більше того, саме законодавчо необхідно закріпити певний стандарт якості, якому має відповідати інформаційна продукція вітчизняного виробника. На рівні захисту необхідно чітко встановити обов'язки суб'єктів, а також відповідальність за їх порушення; встановити контроль за дотримання якості контенту, що виробляється національним виробником, а також способи правового впливу у випадках порушення; покращення захисту певних категорій інформації та поліпшення психологічного захисту свідомості людини і суспільства. При цьому, правові заходи мають підкріплюватися і діяльністю відповідних культурно-масових організацій та рухів, які б пропагували необхідність збереження національного контенту, сприяли б підвищенню його якості.

Література

1. Інформаційні системи і технології на підприємствах : підручник / В. Л. Плескач, Т. Г. Затонацька. - К. : Знання, 2011. - 718 с.
2. Національний інформаційний простір України: проблеми формування та регулювання / В. К. Конах // Стратегічні пріоритети. - 2013. - № 2. - С. 97-103. - Режим доступу : www.nbuv.gov.ua
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII - [Електронний ресурс] - Режим доступу : www.rada.gov.ua
4. Тихомиров О.О. Інформаційна безпека: соціотехнічна парадигма/ О.О. Тихомиров // Інформаційна безпека людини, суспільства, держави. - 2014. - № 1 (14). - С. 13-20.

УДК 004.424.6:004.6](045)

Савченко Д.С.

Національна академія Служби безпеки України

ПРИНЦИПИ ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ З АНАЛІЗУ НЕСТРУКТУРОВАНИХ ТЕКСТІВ У МЕРЕЖІ ІНТЕРНЕТ

Невідповідність між темпами зростання обсягів неструктурованої текстової інформації в мережі Інтернет наявним потребам щодо якості її автоматизованої обробки, в тому числі в контексті реалізації механізмів кібернетичної безпеки, обумовлює актуальність проблеми інтелектуалізації методів роботи з неструктурованими текстами. В першу чергу на сьогодні існує потреба у більш досконалих методиках автоматизованої обробки неструктурованих текстів, що дозволяють ефективно працювати з неструктурованими даними значних обсягів. До того ж, завдання з аналізу неструктурованих текстів в мережі Інтернет мають ряд особливостей, які впливають на принципи побудови, структуру і функціональні можливості автоматизованої системи для їх вирішення.

Зокрема, з уразуванням цих особливостей автоматизована система має будуватися на основі наступних принципів: 1) відокремлення програмної логіки від наборів даних і забезпечення одночасної потокобезпечної роботи багатьох програмних модулів з одними й тими ж спільними даними; 2) відокремлення програмної логіки від інтерфейсу з користувачем; 3) можливість доступу до наборів даних як локально, так і через комп’ютерну мережу; 4) розподілене і дубльоване зберігання наборів даних на різних пристроях і в різних мережах; 5) існування окремих версій програмних модулів для основних типів операційних систем; 6) реентерабельність програмних модулів; 7) можливість розподіленого виконання складних функцій автоматизованої системи багать-

ма копіями програмного модуля як локально, так і через комп'ютерну мережу, в тому числі між різними операційними системами; 8) максимальна швидкість виконання програмного коду; 9) гнучкість конфігурування автоматизованої системи, підтримка внутрішньої мови сценаріїв, компіляція сценаріїв у швидкі для виконання внутрішні структури даних.

Відокремлення програмної логіки від наборів даних означає, що, по-перше, програмні модулі існують окремо від будь-яких наборів даних (баз даних, словників, карт, таблиць тощо) і є зв'язаними з ними лише через посилання на блок ресурсів в контексті виконання окремого запиту, і, по-друге, набори даних є окремими сутностями, що ніяк не зв'язані з програмними модулями.

Забезпечення одночасної потокобезпечної роботи багатьох програмних модулів з одними й тими ж спільними даними означає, що повинна підтримуватись можливість читання і запису даних в один ресурс з різних програмних модулів автоматизованої системи одночасно, але при цьому повинен забезпечуватись механізм синхронізації доступу на запис даних.

Відокремлення програмної логіки від інтерфейсу з користувачем означає, що програмні модулі автоматизованої системи повинні підтримувати єдиний програмний інтерфейс через стандартні мережеві протоколи, засоби спільного розподілення пам'яті і системну консоль. Графічний інтерфейс користувача повинен забезпечуватися окремим додатковим модулем (факультативним), який би керував програмними модулями через єдиний програмний інтерфейс.

Можливість доступу до наборів даних як локально, так і через комп'ютерну мережу означає, що програмні модулі сприймають посилання на блоки ресурсів у стандартному форматі, який надає можливість адресувати як локальний, так і мережевий ресурс (наприклад, URI).

Розподілене і дубльоване зберігання наборів даних на різних пристроях і в різних мережах означає, що, по-перше, будь-який ресурс може містити лише частину необхідної інформації і посилатися далі на інший ресурс, а, по-друге, ресурс також може містити посилання на свої копії.

Існування окремих версій програмних модулів автоматизованої системи для основних типів операційних систем означає, що програмна логіка і інтерфейс повинні бути спроектовані таким чином, щоб з мінімальними змінами забезпечувалась їх успішна компіляція і функціонування в різних операційних системах.

Реентерабельність програмних модулів автоматизованої системи означає можливість їх повторного виклику із різних програмних потоків, тобто, що вони не повинні зберігати проміжний стан між зверненнями в глобальних або статичних об'єктах.

Можливість розподіленого виконання складних функцій авто-

матизованої системи багатьма копіями програмного модуля як локально, так і через комп'ютерну мережу означає, що програмні модулі мають засоби для мережевої і міжпотокової взаємодії, функціонал для визначення в локальній системі або в мережі вільних програмних модулів, розбиття складних запитів на елементарні операції, передачі вільним модулям окремих елементарних операцій на виконання, і отримання від них результатів їх виконання.

Максимальна швидкість виконання програмного коду означає, що з огляду на велику кількість обчислень програмні модулі автоматизованої системи розроблені в середовищах, які генерують найшвидший програмний код для даного типу мікропроцесорів, а їх вихідний код оптимізований на максимальну швидкість виконання.

Гнучке конфігурування автоматизованої системи, підтримка внутрішньої мови сценаріїв для її конфігурування, компіляція сценаріїв у швидкі для виконання внутрішні структури даних означають, що з метою забезпечення більш ефективної адаптації системи до різних умов роботи вона містить розвинену структуру параметрів конфігурації і підтримує внутрішню мову сценаріїв для зміни зазначених параметрів у потрібний спосіб, а самі сценарії виконуються тільки після їх попередньої компіляції у швидкий псевдокод.

Відповідність автоматизованої системи зазначеним принципам дозволить організувати процес обробки неструктурованих текстів у розподіленому програмному середовищі з високим ступенем паралелізму окремих операцій.

УДК 681.5(042.3)

Семко О.В.
Інститут телекомунікацій і глобального інформаційного простору НАН України
Бурячок В. Л.
доктор технічних наук, професор
Державний університет телекомунікацій

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ФУНКЦІОНУВАННЯ ЗАХИЩЕНОЇ СИСТЕМИ ОБМІНУ ДАНИМИ В УМОВАХ КІБЕРНЕТИЧНОГО ПРОТИБОРСТВА

Метою роботи є розробка інформаційної технології функціонування захищеної системи обміну даними в умовах кібернетичного протиборства, як сенсорної мережі на базі протоколу ближнього радіозв'язку 802.15.4/ZigBee, що дозволяє створювати самоорганізуючі відмовостійкі гарантоздатні ІТС за умов оптимального управління ресурсами в умовах конфлікту та невизначеностей.

Сенсорні мережі є єдиною бездротовою технологією, за допомо-

гою якої можна вирішити завдання інформаційної взаємодії в ІТС, спостереження і контролю, за умов критичної зміни параметрів функціонування мережі, зовнішнього та внутрішнього середовища [1, 2].

Актуальність роботи обумовлена тим, що преважна більшість наземних мобільних бездротових мереж зв'язку мають фіксовану інфраструктуру, яка включає стаціонарні (Ad Hoc) та мобільні (MANET) абоненти, з'єднані між собою за допомогою каналів передачі даних і функціонують в умовах конфлікту і невизначеностей в зовнішньому і внутрішньому середовищі ІТС.

На відміну від мереж із ієрархічною структурою і централізованим управлінням, однорангові мережі без інфраструктури складаються з однотипних вузлів, де кожен вузол має комплексом програмно-апаратних засобів, що дозволяють організувати передачу даних від джерела до одержувача безпосередньо при фізичному наявності такого шляху і тим самим розподілити навантаження на мережу і підвищити сумарну пропускну здатність мережі. Передача даних від одного абонента до іншого може відбуватися, навіть у випадку якщо ці вузли знаходяться поза зоною прямої радіовидимості. У цих випадках пакети даних цих абонентів ретранслюються іншими вузлами мережі, які мають зв'язок з кореспондуючими абонентами. Мережі з багаторазової ретрансляцією називаються багатопрольотними або багатоскачковими (multihop). При розробці таких мереж основними проблемами є маршрутизація пакетів від вузла джерела до вузла одержувачу, масштабованість мереж, адресація кінцевих пристроїв, підтримання зв'язності в умовах змінної топології.

При проектуванні та експлуатації сенсорних мереж актуальним завданням є вирішення проблеми забезпечення гарантоздатності, яка в значній мірі визначається розвиненістю механізму їх управління [3]. Сучасна система управління об'єднує ресурси сенсорної мережі та програмні засоби в єдине ціле і визначає її гарантоздатність. Незважаючи на те, що постійно розробляються нові апаратні та програмні засоби для організації процесів інформаційної взаємодії елементів обчислювальних систем і сенсорних мереж, відповідні інформаційні технології ефективного управління такими системами і мережами на поточний час розвинені недостатньо.

Література

1. Levis P., Madden S., Polastre J. and dr. «TinyOS: An operating system for wireless sensor networks» // W. Weber, J.M. Rabaey, E. Aarts (Eds.) // In Ambient Intelligence. New York, NY: Springer-Verlag, 2005. 374 p.

2. Гольдштейн, Б.С. Сети связи пост-NGN / Б.С. Гольдштейн, А.Е. Кучерявый. - СПб.: BHV, 2013. - 160 с.

3. Семко В.В., Семко О.В. Дослідження властивостей рішення задачі конфлікту за методом інтегрального усікання варіантів // Проблеми інформатизації та управління. 2014. Вип. 2(46). С.60-71.

УДК 004.056

Шестак Я.В.
Київський національний університет
ім. Тараса Шевченка
Огбу Д.О.
Київський національний університет
ім. Тараса Шевченка
Оксіюк О.Г.
доктор технічних наук, професор
Київський національний університет
ім. Тараса Шевченка

МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІТС

Відома безліч робіт в предметній області моделювання вторгнень у комп'ютерні системи і обгрунтування показників захищеності. Спершу торкнемося деяких методик, які апробовані, наприклад, методики S. Kumar, E. H. Spafford які запропонували розглядати атаки як шаблон, який показує між подіями і їх змістом:

– S. Kumar, E. H. Spafford запропонували модель комп'ютерних атак на основі розфарбованих мереж Петрі. Кожна сигнатура атаки виражається як шаблон, який показує взаємозв'язок між подіями і їх змістом. Позначення початкового і кінцевого станів і зв'язок між ними визначають шаблон подій.

– K. Iglun, R. A. Kemmerer, P. A. Porras описали підхід до аналізу переходу станів при вторгненні для моделювання комп'ютерних атак. У їхній статті комп'ютерна атака представляється як послідовність дій, виконуваних атакуючим для компрометації безпеки комп'ютерної системи. Атаки описуються за допомогою діаграм переходу станів.

– У роботі F. Cohen "Моделювання комп'ютерних атак, захист і послідовність" розглянутий підхід до оцінювання мережевої безпеки як "причинно-наслідкова модель атаки і захисту інформаційної системи". Вона складається з мережі, яка відображається вузлами і їх зв'язками, причинно-наслідкового зв'язковою описової моделі і псевдо випадкового генератора чисел. Варто вказати на значне спрощення подібного уявлення при моделюванні комп'ютерних вторгнень, заснованому на причинно-наслідковому зв'язку.

Як бачимо [1] методику K. Iglun, R. A. Kemmerer, P. A. Porras, де вони представляють атаку як послідовність дій для компрометації безпеки комп'ютерної мережі. F. Cohen підійшов до розгляду оцінки мережевої безпеки як до причинно-наслідкової моделі.

Детальніше розглянемо один з методів оцінки захищеності ІТС на основі дерев атак. Всю методику можна розкласти на три етапи, підготовчий, етап експлуатації і заключний етап:

На підготовчому етапі для кожного вузла ІТС формується список можливих атакуючих дій, розбитих на групи за різними ознаками.

На етапі експлуатації визначається якісний рівень ризику для всіх загроз, також будуються дерева атак, на основі яких відбувається подальше оцінювання захищеності ІТС.

Рівень захищеності, аналізованою ІТКС на основі дерев атак визначається на заключному етапі. За отриманою інформацією про вразливості, присутніх в ІТС формуються і вибираються моделі порушників на основі знань експерта з безпеки. Наступним етапом методики є підготовка даних для формування дерев атак і виділення можливих атакуючих дій, доступних порушнику для кожного вузла ІТС.

Перша стадія проведення аналізу - це збір інформації про доступність в вузлах ІТС, за допомогою різних ПЗ, наприклад: ICMP, TCP SYN Ping, ICMP Timestamp Request. Друга стадія аналізу - пошук уразливого програмного забезпечення.

На третій стадії проведення аналізу використовуються як окремі уразливості із словника, так і шаблони. На етапі експлуатації відбувається первинна побудова дерев атак. Елемент моделі атак, що описує дерево атак, є вектором:

$$M=\langle S, S_0, G, \pi \rangle, \quad (1)$$

де

S – безліч станів мережі,

S_0 – початковий стан мережі,

G – безліч показників, що визначають відсоток досягнення порушником своїх цілей при використанні побудованого дерева атак,

$\pi = S \cdot S$ – безліч переходів між станами, яке можна визначити наявними у зловмисника атакуючими діями.

Вузли дерева атак задають можливі атакуючі дії, пов'язані між собою відповідно до того, в якому порядку їх може виконувати певний порушник. Маршрут атаки є частиною дерева атак і являє собою послідовність станів ITC(S0, S1..., Sn), причому(Si, Si 1) $\in \pi$ $\forall i \in [0,]$. В результаті отриманих дерев атак і маршрутів дій оцінюються показники захищеності. Слабкість хоста обчислюється за формулою:

$$C(s) = \sum_{i=1}^{n} \max(0, S(w_i) - 60)/n, \quad (2)$$

де

s – вузол ІТС;

$S(w_i)$ – оцінка для слабкого місця w і вузла s;

n – кількість вузлів ІТС з оцінкою S вище 60.

Дії зловмисника під час проведення дії характеризує такий показник, як поверхня атаки - усі можливі маршрути атаки, виходячи з поточного стану порушника на дереві атак і його навичок.

Ризик визначається як результат можливості (ймовірності) загрози та наслідків її реалізації для всієї ІТС. У найзагальнішому вигляді методика розрахунку показника "Рівень ризику" виглядає таким чином: рівень ризику атаки визначається як добуток ймовірності успішної реалізації атаки на шкоду, яку завдають в разі успішної реалізації атаки.

Література:

1. Абрамов Е.С. Применение графов атак для моделирования вредоносных сетевых воздействий // Известия ЮФУ. Ростов-на-Дону: Издательство Южный федеральный университет, 2012. - №1(126) «Информационная безопасность». с.165-174.

Шкуратенюк О.В.

Національна академія Служби безпеки України

ДО ПИТАННЯ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОЇ РЕГЛАМЕНТАЦІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із актуальних напрямів реформування українського адміністративного права є модернізація відповідальності за правопорушення в інформаційній сфері. Питаннями правового регулювання обігу інформації та відповідальності за правопорушення у вказаній сфері займались такі науковці, як, Арістова І.В., Благодарний А.М., Марущак А.І., Кормич Б.А., Кохановська О.В., Макаренко В.В., Романенко І.В., Тихомиров О.О. та інші. Але питання вдосконалення відповідальності за правопорушення у сфері інформаційної безпеки, на нашу думку, ще не дістали належної уваги, хоча останнім часом набувають все більшої актуальності.

Існують різні класифікації правопорушень у сфері інформаційної безпеки, але, на нашу думку, однією з найбільш вдалих є класифікація, відповідно до якої вказані правопорушення поділяються на три групи, що пов’язані: а) з посяганням на інформацію; б) з розповсюдженням інформації, що завдає шкоди; в) правопорушення, пов'язані з посяганням на право громадян та інших суб’єктів на доступ до відкритої інформації [1, с. 89]. Вважаємо за доцільне подібним

чином класифікувати адміністративні правопорушення у сфері інформаційної безпеки.

Відразу зазначимо, що ця класифікація, як і переважна більшість інших наукових класифікацій, є певною мірою умовною та дискусійною.

Проаналізувавши зміст КУпАП, до першого пункту класифікації (**правопорушення, пов'язані із посяганням на інформацію**) можна віднести правопорушення, передбачені ч. 1 ст. 92-1; ч. 2 ст. 163-5; ч. 1 ст. 195-5; п. 1 ч. 1 ст. 212-2; п. 4 ч. 1 ст. 212-2; п. 5 ч. 1 ст. 212-2; п. 6 ч. 1 ст. 212-2; п. 7 ч. 1 ст. 212-2; п. 8 ч. 1 ст. 212-2; п. 9 ч. 1 ст. 212-2; ч. 1 ст. 212-5; ч. 1 ст. 212-6; ч. 3 ст. 212-6; ч. 4 ст. 212-6; ч. 5 ст. 212-6; ч. 6 ст. 212-6 КУпАП.

До другого пункту класифікації - **розповсюдження інформації, що завдає шкоди**, можна віднести правопорушення, відповідальність за вчинення яких встановлена ч. 5 ст. 96; ч. 1 ст. 148-3; ч. 2 ст. 164-3; ч. 3 ст. 164-3; ч. 2 ст. 166-9; ч. 1 ст. 173-1; ч. 1 ст. 185-7 КУпАП.

До третього пункту класифікації – **правопорушення, пов'язані з посяганням на право громадян та інших суб'єктів на доступ до відкритої інформації, або на право оприлюднення відкритої інформації**, можна віднести правопорушення, передбачені ч. 1 ст. 53-2; ч. 1 ст. 82-3; п. 3 ч. 1 ст. 83-1; ч. 1 ст. 91-3; ч. 1 ст. 91-4; ч. 1 ст. 92-1; ч. 1 ст. 163-5; ч. 1 ст. 166-4; ч. 5 ст. 166-6; ч. 1 ст. 166-9; ч. 1 ст. 186-3; п. 2 ч. 1 ст. 212-2; п. 3 ч. 1 ст. 212-2; ч. 2 ст. 212-3; п. 2 ч. 1 ст. 212-4; ч. 1 ст. 212-11 КУпАП [2].

На нашу думку, законодавцю слід об'єднати всі вказані правопорушення у одному розділі, подібно до того, як це зроблено у КУпАП відносно інших правопорушень, наприклад, правопорушень, що посягають на власність (глава 6 КУпАП).

Окремого розгляду потребує питання адміністративної відповідальності юридичних осіб за вчинення правопорушень в інформаційній сфері. Останнім часом у законодавстві з'явилось чимало норм, які передбачають накладення стягнень на юридичних осіб, зокрема за правопорушення в інформаційній сфері. Так, наприклад, згідно з ч. 6 ст. 20 Закону України «Про державну таємницю» дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасовано Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання органом державної влади, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених статтею 20 Закону України «Про державну таємницю» [3].

Законодавство про адміністративну відповідальність юридичних осіб в Україні на сьогодні недостатньо розроблене, в деяких випадках юридичні особи несуть відповідальність нарівні з фізичними особами [4, с. 175]. За вчинення адміністративного правопорушення

у сфері інформаційної безпеки на фізичних осіб найчастіше накладається штраф. На нашу думку, цей вид адміністративного стягнення також варто застосовувати і до юридичних осіб – порушників законодавства про інформацію.

Враховуючи викладене, для створення логічно завершеного, ефективного правового регламентування адміністративної відповідальності за правопорушення в інформаційній сфері, насамперед, необхідно передбачити у чинному КУпАП розділ, який би містив правопорушення у сфері обігу інформації, а також закріпити у чинному КУпАП (або у новому Кодексі України про адміністративні проступки) норму, яка б передбачала адміністративну відповідальності юридичних осіб за вчинення правопорушень в інформаційній сфері.

Література:

1. Інформаційна безпека держави: підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. – Т. 2. / за заг. ред. В.В. Остроухова – К.: ДНУ "Книжкова палата України", 2016. – 328 с.
2. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР України. – 1984. – додаток до № 51. – Ст. 1122.
3. Про державну таємницю: Закон України від 21 січня 1994 року № 3855–12 // Відомості Верховної Ради України. – 1994. – № 16. – Ст.93.
4. Адміністративне право України: Підручник / Ю.П. Битяк, В.М. Паращук, О.В. Дьяченко та ін. / За ред. Ю.П. Битяка. – К.: Юрінком Інтер, 2005. – 544 с.

Шпак В.Г.

Національна академія Служби безпеки України

Талалай Д.В.

доктор юридичних наук

Національна академія Служби безпеки України

ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ: СУТНІСТЬ ТА ЗМІСТ

На сьогоднішній день питання дотримання та захисту інформаційних прав людини і громадянина стоїть дуже гостро. Шлях України до повноправного членства у Європейському співтоваристві визначає переоцінку пріоритетів розвитку, зміну ролі держави в управлінні інформаційною сферою, чому значною мірою має сприяти проведення комплексного оновлення інформаційного законодавства України. Індивідуальну увагу необхідно приділити удосконаленню правового за-

хисту, запобігання, попередження, припинення правопорушень у процесах створення, зберігання, поширення, обігу інформації.

Становлення та розвиток інформаційних засад суспільства припускає наявність сукупності передумов, що забезпечують його оновлення і розвиток. Базовою умовою такого процесу є юридично оформлений захист інформаційних прав і свобод людини і громадянина [5, с. 46].

З огляду на це, дослідження питань правового механізму захисту інформаційних прав і свобод людини і громадянина в Україні стає досить актуальним.

Проблемі захисту інформаційних прав присвятили ряд вчених, праці яких взяті за основу дослідження: М.П. Рагозін, В.М. Брижко, В.Я. Настюк, О.А. Баранов, О.Г. Огородник, В.В. Бєлєвцева, В.С Цимбалюк, М.С. Малеїн.

Неодноразово в юридичній літературі ми зустрічаємо поняття «механізм» для характеристики правових явищ. Наприклад, механізм захисту прав людини, проте абсолютного визначення та тлумачення цього поняття немає.

Так, Мотьвилавка Е.Я. розкриває поняття механізму як системи певних правових засобів, які спрямовані на захист людини [1, с. 54].

Український конституціоналіст Погорілко В.Ф., погоджуючись з Мотьвилавком Е.Я., тлумачив механізм як систему правових засобів. Ці засоби необхідні для захисту прав. Крім того, Погорілко В.Ф., як і Рогозін М.П. зазначав, що механізм захисту прав людини є системою влади держави, основною функцією якої є захист прав людини та громадянина.

Рогозін М.П. визначає, що юридичний механізм захисту прав людини – це можливості здійснення громадянами певних вчинків щодо захисту власних прав і свобод, а також система органів, які захищають і забезпечують ці права та свободи [2, с. 180].

З такою думкою Рогозіна М.П. погоджується й Огородник О.Г., проте він до механізму захисту прав відносить ще й громадські організації, правові та нормативні акти, які покликані захищати права людини [3, с. 15].

З огляду на вищевказане можна зробити висновок, що механізм захисту інформаційних прав людини – це система заходів, що застосовують уповноважені особи, спрямовану на усунення порушень інформаційних прав людини.

Настюк В.Я. виділяє два шляхи виникнення інформаційних прав і свобод людини і громадянина у правовій системі української держави. Перший шлях – ухвалення нових нормативно-правових актів внутрішньо державного характеру, що закріплюють нові інфо-

рмаційні права людини і громадянина. Другим шляхом – ратифікація міжнародних угод, що містять нові інформаційні права людини і громадянина [4, с. 31].

Бєлєвцева В.В. поділяє правовий механізм захисту інформаційних прав і свобод людини і громадянина на два види: нормативно-правовий та організаційно-правовий.

Нормативно-правова форма виражається в ухваленні нормативно-правових актів або у внесенні до існуючих нормативно-правових актів таких змін, які можуть сприяти здійсненню захисту інформаційних прав людини і громадянина. В даному механізмі Бєлєвцева В.В. виділяє його наступні елементи: нормативне закріплення здійснення правового захисту інформаційних прав людини і громадянина; юридичний факт, який дозволяє почати процес правового захисту інформаційних прав людини і громадянина; правовідносини, в яких є права та відповідні ним обов'язки; суб'єкти правового механізму захисту інформаційних прав людини і громадянина; об'єкти правового механізму захисту інформаційних прав людини і громадянина [5, с. 46].

Організаційно-правову форму Бєлєвцева В.В. вбачає в діяльності державних органів, що беруть участь у процесі захисту прав людини в інформаційній сфері. Основна роль у ньому належить Президентові України, Верховній Раді України, органам виконавчої влади. Роль Президента України обумовлена тим, що він є гарантом прав і свобод людини в українській державі. Роль органів виконавчої влади визначається в організації виконання норм Конституції України і законів. [5, с. 46].

Слід зазначити, що особливе місце в організаційно-правовому механізмі захисту інформаційних прав людини відводиться правоохоронним органам, які виконують одну з найактивніших ролей у захисті інформаційних прав і свобод людини і громадянина.

Сутність механізму захисту полягає в досягненні справедливості у суспільних відносинах при порушенні інформаційних прав людини. Головний задум таких механізмів полягає, на сам перед, в захисті інформаційних прав, повна реалізація людиною свого права на такий захист. Очевидно, що механізм захисту інформаційних прав та механізм реалізації людиною свого конституційного права на захист повинні бути універсальні. Для підвищення ефективності механізму захисту інформаційних прав, вважаю за необхідним ухвалити закон, що регулюватиме умови і порядок реалізації права на інформацію, що, у свою чергу, дозволить скоротити обсяг підзаконного правового регулювання. У проекті закону слід закріпити основні етапи застосування механізму захисту прав людини і громадянина,

що дозволить зробити їх універсальними. Теоретичне осмислення дії правового механізму захисту інформаційних прав і свобод людини і громадянина необхідне тому, що в цьому питанні не можна обійтися лише аналізом чинного законодавства в інформаційній сфері. Необхідне системне теоретично-правове обґрунтування і дослідження цієї суттєвої правової проблеми.

Література

1. Мотьвилавка Е.Я. Теория регулятивного и охранительного права. – Воронеж, 1990. – С. 54.
2. Рагозін М. П. Вчимося демократії Уроки громадянської освіти. - Донецьк, Видавництво «Донбас», 2004. - С.180.
3. Огородник О.Г. Механізм забезпечення прав і свобод людини та принцип законності в Україні //Право України. 2008. №6. С.15.
4. Настюк В.Я. Формування системи інформаційного законодавства в Україні. – 2011. – С. 31.
5. Бєлєвцева В.В. Правовий режим інформаційних ресурсів. – 2011. – С. 46.

РЕКОМЕНДАЦІЇ
науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави»

24 травня 2017 року Національною академією СБ України спільно з Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Інститутом модернізації змісту освіти МОН України проведено VIII Науково-практичну конференцію *«Актуальні проблеми управління інформаційною безпекою держави»*.

У роботі конференції взяли участь представники Апарату Ради національної безпеки і оборони України, Міністерства освіти і науки України, Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної прикордонної служби України, Державної служби спеціального зв'язку та захисту інформації України, Державного агентства з питань електронного урядування України, а також провідних наукових установ і вищих навчальних закладів України.

Під час конференції розглянуто комплекс актуальних проблем управління інформаційною безпекою держави в сучасних умовах, за результатами якого учасники конференції

КОНСТАТУВАЛИ:

1. Застосування країною-агресором щодо України технологій гібридної війни, насамперед в інформаційній сфері, сформувало нові виклики і загрози інформаційній безпеці держави. Саме проти України та інших європейських країн Російська Федерація використовує найновіші технології інформаційно-психологічного впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності.

2. Комплексний характер викликів і загроз національній безпеці в інформаційній сфері потребує ефективної державної інформаційної політики та політики забезпечення інформаційної безпеки, узгодженої стратегії розвитку інформаційної галузі, консолідованих дій та спільного бачення засобів реагування на сучасні виклики і загрози, визначення інноваційних підходів до формування загальнодержавної системи захисту інформації з обмеженим доступом, забезпечення інформаційної та кібербезпеки України в умовах гібридної війни.

3. В Україні прийнято низку нормативно-правових актів стратегічного рівня з питань захисту національних інтересів в інформаційній сфері. Водночас актуальним залишається питання визначення шляхів їх реалізації в сучасних умовах.

УЧАСНИКИ КОНФЕРЕНЦІЇ РЕКОМЕНДУЮТЬ:

– розробити дієві механізми виявлення, фіксації, блокування та видалення з національного інформаційного простору, зокрема з українського сегмента мережі Інтернет, інформації та ресурсів, які створюють загрози життю і здоров'ю громадян України, пропагують війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– спрямувати зусилля державних і недержавних суб'єктів сектору безпеки на розвиток системи забезпечення інформаційного суверенітету, управління ризиками і новими можливостями в інформаційній сфері, розбудову інформаційно-комунікаційної інфраструктури, формування національного інформаційного простору, оптимізації взаємодії та комунікаційного процесу між державними органами й органами місцевого самоврядування та споживачами інформаційної продукції і послуг;

– продовжити заходи щодо впровадження стратегічних комунікацій як скоординованого і належного використання комунікативних можливостей сил безпеки та оборони держави, спрямованих на реалізацію цілей України;

– удосконалити комплекс заходів із протидії негативним інформаційним впливам, зокрема, шляхом формування позитивного іміджу України у світі, донесення оперативної, достовірної й об'єктивної інформації про події в Україні до міжнародної спільноти та громадян України, розробки та впровадження програм медіаосвіти населення;

– забезпечити наповнення інформаційного простору України національним продуктом, здатним конкурувати із зарубіжними аналогами; сприяти розробці та впровадженню вітчизняних засобів обробки й передачі інформації та програмного забезпечення;

– вжити необхідних заходів щодо захисту інформації з обмеженим доступом, насамперед державної таємниці та персональних даних, що обробляються в єдиних державних реєстрах та інших інформаційних системах і базах даних;

– продовжити розбудову системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямів з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці;

– забезпечити активне залучення наукового експертного середовища до розробки та опрацювання проектів нормативно-правових актів в інформаційній сфері;

– розгорнути комплексну систему підготовки та перепідготовки фахівців з інформаційної та кібернетичної безпеки для сектору безпеки та оборони України з урахуванням досвіду проведення АТО та кращих практик зарубіжних країн;

– запровадити програми, спрямовані на стимулювання участі молодих учених, курсантів та студентів у наукових дослідженнях із проблем управління інформаційною безпекою держави;

– сприяти розвитку та активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності.

ЗМІСТ

Вступне слово 3

ДЕРЖАВНО-ПРАВОВІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Авдошин І.В. Проблеми правового регулювання інформаційних відносин в Україні 5

Архипов О.Є., Бровко В. Д. Кібербезпека – виникнення, формування, розуміння 7

Баранов О.А. Нова парадигма безпеки в умовах інтернету речей (IOT) 10

Благодарний А.М. Проблеми удосконалення адміністративно-юрисдикційної діяльності органів Служби безпеки України на стадії порушення справ про адміністративні проступки у сфері інформаційної безпеки 12

Бондаренко І.Д. Напрямки уніфікації «комп'ютерної» термінології в статтях розділу XVI КК України 14

Волошин О.В. Превентивні антитерористичні заходи як механізм протидії терористичним загрозам в інформаційній сфері 17

Воскобойніков С.О. Модернізація процесу формування професійної компетентності фахівців кібернетичної та інформаційної безпеки в Україні 19

Гавловський В.Д. До питання використання соціальних мереж у деструктивних цілях 21

Гордієнко С.Б., Богуш В.М., Настрадін В.П. Проблеми підготовки суспільства до викликів кібертероризму 23

Грищук Р.В. Гібридна загроза в кіберпросторі: інформаційна та кібернетична складові 26

Гуцалюк М.В. Заходи боротьби з контрафакцією і піратством у мережі Інтернет 29

Даник Ю.Г. Формування системи забезпечення

кібербезпеки України 31

Довгань О.Д. Правове забезпечення кібербезпеки: проблема державного рівня 33

Заєць П.М., Іванова О.С., Скубак О.М. Поняття інформаційної безпеки в кіберпросторі України 36

Іванов О.Ю. Російсько-українське інформаційне протиборство з «кримського питання»: генезис та сучасний стан 38

Касперський І.П. Вітчизняне та європейське регулювання стратегічних підходів у гарантуванні кібербезпеки 41

Климчук О.О., Ткачук Н.А. Формування державної кібербезпекової політики 43

Ковбан А.В. Інформаційна безпека як елемент глобальних прав 47

Ковтун Ю.В. Загрози інформаційному простору держави в умовах агресії Російської Федерації 50

Комісаров О.Г. Теоретико-правова модель вітчизняного законодавства, що регулює інформаційно-аналітичну діяльність правоохоронних органів 52

Кудінов В.А. До проблеми щодо створення надійних паролів користувачів інтегрованої інформаційно-пошукової системи МВС України 54

Карпенко О.В. Сучасні безпекові імперативи реалізації державної інформаційної політики України 57

Куроєд В.В. Засоби маніпуляцій в інформаційній війні 59

Ланде Д.В., Бойченко А.В. Побудова моделі розвитку ситуації на основі аналізу інформаційного простору 61

Левченко О.В. Визначення структури методики виявлення, аналізу та оцінювання інформаційних загроз державі у воєнній сфері 63

Мамченко С.М. Проблеми підготовки фахівців із забезпечення інформаційної безпеки на сучасному етапі реформування системи вищої освіти України 66

Марутян Р.Р. Біо-інформаційні технології в контексті безпеки людини: державно-правовий вимір 69

Меленті Є.О., Білецький С.В. Рекомендації зі зміцнення інформаційної безпеки держави 72

Небава М.І., Міронова Ю.В. Інтегральний підхід до оцінювання рівня захисту інформаційного простору 73

Николаєнко Г.В. Правові засади регулювання професійної конфіденційності в державній статистичній діяльності 76

Остроухов В.В., Величко М.В., Салагор І.М. Природний та штучний інтелекти: цивілізаційні блага та проблеми 78

Павлючук С.О., Скіцько О.І. Інформаційне законодавство України, проблеми та напрямки розвитку 84

Овсянніков В.В., Паламарчук Н.А., Паламарчук С.А., Пеньков В.І. Деякі питання щодо підготовки фахівців у сфері інформаційної та кібернетичної безпеки України 87

Пальчик М.Л. Державно-приватне партнерство у кібер-захисті критичної інфраструктури 89

Петрик В.М. Порівняльна характеристика понять «радикалізм», «екстремізм», «терор», «тероризм», «терористичний акт», «інформаційний тероризм», «диверсія» 91

Платоненко А.В., Лазаренко С.В. Актуальні загрози інформаційної безпеки серед українських користувачів мобільних пристроїв 93

Погребняк В.П., Дашковська О.В., Солоденко А.К. Інтернаціоналізація вітчизняної вищої освіти 95

Половніков В.В. До проблеми визначення поняття кримінального аналізу та його застосування 97

Присяжнюк М.М. Міжнародний інформаційний тероризм як загроза національній безпеці України 100

Процюк Ю.О., Островський С.М., Штонда Р.М. Шляхи розвитку стратегічних комунікацій у військовій сфері 102

Пучков О.О., Конюшок С.М. Підготовка фахівців з інформаційної та кібернетичної безпеки держави: досвід

ІСЗЗІ КПІ ім. Ігоря Сікорського 104

Романов М.С. Участь науково-навчальних установ Російської Федерації у спеціальних інформаційних операціях 106

Ромащенко І.В. Іноземна мова як комунікативна складова здійснення науково-дослідної діяльності майбутніми фахівцями з інформаційної безпеки держави 108

Савич О.С. Інформаційна безпека під час електронного документообігу у торгівельному мореплавстві 110

Савінова Н.А., Осадчук Д.Д. Тренд «морська безпека» як стратегічна складова інформаційної безпеки України..... 114

Сервецький І.В. Деякі проблеми забезпечення інформаційної безпеки в Україні..... 119

Слухай Н.В. Лінгвістичні маркери замаскованої світоглядної позиції суб'єкта мас-медійної інтеракції..... 122

Столбовий В.М., Черновський М.А. Адміністративно-правові заходи захисту інформації в інформаційних (автоматизованих) системах 124

Стрельбицька Л.М., Стрельбицький М.П. Антологія та інспірування інформаційного тероризму..... 126

Тиква В.Л. Використання мережі Інтернет для впливу на суспільну свідомість 130

Тіщенко В.М. Інформаційне забезпечення фільтраційно-перевірочної діяльності Державної прикордонної служби України 133

Ткаченко В.В. Стандарти вищої освіти у сфері кібербезпеки – важливий інструмент модернізації освітнього процесу та запорука національної безпеки України 135

Ткачук Л.М., Волчаста К.В. Інформаційна безпека України 138

Ткачук Н.А. Загрози національній системі кібербезпеки держави в сучасних умовах..... 140

Ткачук Т.Ю. Кібербезпека: підходи до визначення в окремих країнах..... 142

Тронц В.М., Колонюк В.В. Інформаційна війна як засіб ведення конфлікту 144

Тугарова О.К. До проблеми юридичної відповідальності викривачів інформації 147

Хорошко В.О., Блавацька Н.М., Хохлачова Ю.Є., Тимченко М.П. Класифікація вхідної оперативної інформації в системах захисту 149

Чередниченко А.О., Чередниченко О.Ю. Інформаційно-аналітичне забезпечення системи управління економічною безпекою підприємств будівельної галузі 151

Чередниченко О.Ю. Актуальність та проблемні питання практичного втілення поняття «персонального онлайн-кабінету»в кримінальному процесі України 153

Шевченко А.С. Концепція побудови технічної складової системи кібернетичної безпеки Збройних Сил України 155

Шевченко М.О. «Правовий статус біженців у контексті боротьби з тероризмом» 157

СТРАТЕГІЧНІ КОМУНІКАЦІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ЗОВНІШНІЙ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Андрійчук О.В., Ланде Д.В. Застосування інструментарію підтримки прийняття рішень при виявленні інформаційних операцій 161

Браіловський М.М. Використання віртуалізації для створення мереж майбутнього під час надзвичайного стану 163

Горовий В.М. Еволюційні причини інформаційного протистояння 165

Гринь А.К., Гамаліна К.А. Особливості проведення спеціальних інформаційних операцій в умовах антитерористичної операції 168

Дубов Д.В., Дубова С.В. Публічна дипломатія в умовах воєнно-політичних криз: кампанія США проти Гренади 170

Князєв С.О. Інформаційна війна: причини виникнення та сучасні тенденції 172

Козюра В.Д., Степаненко В.І., Хорошко В.О. Таргетовані кібератаки – реальна загроза об'єктам критичної інфраструктури України 175

Кудирко В.М., Горшков Г.М. Щодо особливостей використання астротерфінгу в інформаційній агресії РФ на шкоду інтересам України 177

Лахно В.А. Кібербезпека інформаційно-комунікаційних систем транспорту як складова національної безпеки 179

Марущак А.І. Суспільно необхідна інформація і приватність особи 181

Мошко М.С., Прозоров А.Ю. Стратегічні комунікації як інструмент протидії зовнішній інформаційній агресії 182

Наконечний В.С., Курченко О.А., Рабчун Д.І. Метод ресурсної оптимізації комплексу програмних засобів захисту інформації в умовах динамічного інформаційного протистояння 185

Панченко В.М. Поняття інформаційного тероризму у науковому дискурсі 187

Петров В.В. До аспектів розбудови системи стратегічних комунікацій 191

Пучков О.О., Уваркіна О.В. Стратегічні комунікації як чинник інформаційної безпеки держави 194

Рогов П.Д. До питань управління системою стратегічних комунікацій держави у воєнній сфері 196

Рогов П.Д., Ткаченко В.А. Щодо питань протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) 199

Рудніцький І.А., Хміль В.В. Розвиток спроможностей цивільно-військового співробітництва Збройних Сил України у сфері стратегічних комунікацій: організаційно-правовий аспект 201

Селіна М.Б. Ефективність проведення власних спеціальних інформаційних операцій у контексті досвіду козацтва 204

Сиволапенко Т.Л. Інформаційна зброя в сучасних

інформаційних протиборствах 207

Скачек Л.М. Боротьба з комп'ютерними злочинами 211

Сніцаренко П.М. Термінологічний нігілізм в інформаційній сфері та його наслідки для інформаційної безпеки України 212

Сніцаренко П.М., Саричев Ю.О., Хоменко Л.В. Методологічний підхід до створення підсистеми виявлення та оцінки негативного інформаційного впливу на особовий склад військ (сил) як складової системи протидії такому впливу 214

Сєкунов С.В. Категоріальний аналіз контррозвідувального захисту державних інтересів у сфері інформаційної безпеки 217

Тищук В.В. До проблеми протидії зовнішній інформаційній агресії 220

Ткаченко О.П. Щодо поточного стану реалізації СБ України трастового фонду Україна-НАТО з питань кібербезпеки 222

Толюпа С.В., Пархоменко І.І. Засоби виявлення кібернетичних атак 225

Хатян О.А. Модель виявлення PR-впливу як провідника інформаційної загрози через електронні ЗМІ 227

Циганок В.В. Підтримка прийняття рішень при побудові стратегії протидії інформаційним операціям 230

Черниш Ю.О., Штонда Р.М., Мальцева І.Р. Стратегічні комунікації – механізм протидії інформаційним війнам 232

Чеховська М.М., Лісовська О.Л., Крапівіна Н.В. Кризові комунікації як елемент управління кризовими ситуаціями 234

Шиповський В.В. Кібератака як вид застосування у секторі безпеки та оборони: DDOS-АТАКИ 236

УДОСКОНАЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ УКРАЇНИ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

Блавацька Н.М., Юрх Н.Г. Перспективи розвитку систем розпізнавання мовлення 240

Видрич Н.М., Жарук Д.М. Медіавіруси в Інтернеті як загроза національній безпеці..... 242

Гуз А.М., Гоц О. В. Охорона державної таємниці у Стародавньому Єгипті 244

Доронін І.М. Правові проблеми використання сучасних технологій розподіленої обробки даних для державних реєстрів..... 246

Жевелєва І.С. Охорона державної таємниці у Китайській Народній Республіці 249

Козій О.М. Моделі оцінки показників ефективності інформаційної діяльності підрозділу в умовах протидії витоку інформації..... 251

Корж І.Ф. Правові проблеми системи охорони державної таємниці 254

Михайлов А.А. Перспективи реформування системи охорони державної таємниці та службової інформації..... 256

Олійник В.І. Кримінально-правовий захист державної таємниці у Франції 259

Павлюк І.С. Проблематика забезпечення охорони державної таємниці в особливих умовах..... 261

Романенко І.В. Допуск до державної таємниці як правовий інститут 263

Семенюк О.Г. Щодо необхідності змін у підходах до кримінально-правової охорони державної таємниці..... 265

Сидоренко С.М. Організаційно-правові засади системи охорони державної таємниці Латвійської Республіки 269

Скіцько О.І. Деякі аспекти системи управління інформаційною безпекою мобільних пристроїв у мережі..... 271

Шепета О.В. Аналіз міжнародних угод України про взаємну охорону інформації з обмеженим доступом.....274

ПОГЛЯД НА ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ МОЛОДИХ УЧЕНИХ І СТУДЕНТІВ

Аміров М.Г., Тимофєєв Д.С. Проблематика нормативно-правового забезпечення процесу аудиту інформаційної безпеки на підприємствах України 278

Андріяшик І.В. Неправомірне використання фотографій у соціальних мережах 280

Бачинський О.В. Захист комерційної таємниці – важливий елемент системи захисту інформації в Україні.....282

Голубєв О.В. Інструмент протидії інформаційній війні – стратегічні комунікації 285

Гончаренко Д.Б. Конкурентна розвідка - необхідність сучасного бізнесу 287

Гострик С.Р. Особливості захисту інформації в США.....289

Гоц О.В., Семчишина С.В. Загальна характеристика документів в умовах посилення інформаційної безпеки.....292

Давидюк А.В. Соціальна інженерія як складова кібернетичної атаки 294

Дячук П.Р., Іванов Ю.А. Правові аспекти охорони комерційної таємниці в банківських правовідносинах.....296

Єргакова С.А., Іванов Ю.А. Правові аспекти збереження банківської таємниці за надзвичайних умов функціонування банківської системи України 298

Жуйкова К.В., Гулак Г.М. Раціональне управління ресурсами для оновлення апаратної та програмної платформ захищених АСУ ТВ..... 301

Коломайко А.Є. Персонал як джерело витоку інформації 302

Кролевецька І.А. Промислове шпигунство: методи

та засоби протидії 305

Мосьпан А.О., Скоропад С.І. Аналіз понятійного апарату в області використання соціальної інженерії 307

Олійник Ю.С. Сучасне розуміння кібернетичної безпеки 309

Омельчук І.В. Вплив ЗМІ на суспільну думку як інформаційна загроза 312

Пахольченко Д.В. Застосування соціальної інженерії в соціальних мережах на прикладі гри «Синій кит» 312

Пістрюга Т.В. Оцінювання стану інформаційного простору зарубіжних країн для вирішення задач розбудови стратегічних комунікацій України 316

Прищепа С.В., Ланде Д.В. Екстрагування безпекових подій з TWITTER 319

Рагнєв А.О. Проблема українського контенту в національному інформаційному просторі 321

Савченко Д.С. Принципи побудови автоматизованих систем з аналізу неструктурованих текстів у мережі Інтернет 324

Семко О.В. Інформаційна технологія функціонування захищеної системи обміну даними в умовах кібернетичного протиборства 326

Шестак Я.В., Огбу Д.О., Оксіюк О.Г. Методика оцінювання захищеності ІТС 328

Шкуратенюк О.В. До питання вдосконалення адміністративно-правової регламентації забезпечення нформаційної безпеки 330

Шпак В.Г., Талалай Д.В. Правовий механізм захисту інформаційних прав людини: сутність та зміст 332

Рекомендації 336

Електронна версія наукового видання

АКТУАЛЬНІ ПРОБЛЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ

VIII науково-практична конференція

Збірник матеріалів
(Київ, 24 травня 2017 року)

Авторська редакція

Технічне редагування, макетування: *Гострик С.Р., Матяш О.І.*

Об’єм даних 2,27 Мб.

Видавець і виготовлювач
Національна академія Служби безпеки України,
вул. М. Максимовича, 22, Київ, 03022
факс: (044) 257-30-35
E-mail: academy@ssu.gov.ua
Свідоцтво суб’єкта видавничої справи ДК № 99 від 23.06.2000