

МАТЕРІАЛИ  
науково-практичної конференції  
“ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ  
І ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА: НОВІ ВИКЛИКИ,  
НОВІ ЗАВДАННЯ”  
(ІТСТК-2020)

(заочна форма проведення, онлайн-режим)

18–19 листопада 2020 року

Київ – 2020

**Матеріали науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. – 294 с.**

У матеріалах науково-практичної конференції “Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання” опубліковано тези доповідей, в яких досліджуються питання аналізу і узагальнення нових теоретичних і практичних результатів у сферах криптографічного та технічного захисту інформації, кібербезпеки та кіберзахисту, телекомунікацій, комп’ютерних наук та інформаційних технологій, технічної експлуатації систем і засобів спеціального зв’язку, управління інформаційною безпекою, а також досліджуються питання підготовки фахівців з відповідних спеціальностей у закладах вищої освіти.

(заочна форма проведення, онлайн-режим)

#### РЕЦЕНЗЕНТИ:

Пучков О.О.	к.філос.н., професор
Конюшок С.М.	к.т.н., доцент
Рома О.М.	д.т.н., с.н.с.
Криховецький Г.Я.	к.т.н., с.н.с.
Єрохін В.Ф.	д.т.н., професор
Романенко В.П.	к.т.н., доцент
Субач І.Ю.	д.т.н., доцент
Іванченко С.О.	д.т.н., професор

*Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 3 від 11.11.2020).*

РОМАНЕНКО В.П., ЖЕЛНОВ А.І. Підхід до моделювання оцінки ефективності функціонування спеціальних систем зв'язку	210
КРАСОВСЬКИЙ О.І., ГАНГАЛ А.В. Інформаційний вплив РФ на населення України в аспекті гібридної війни.	212

#### **Секція № 5 “Перспективні комп’ютерні технології в сфері кібербезпеки та кіберзахисту”**

КАРПЕНКО О.В., ФЕДІЄНКО О.П. Кіберзагрози в умовах поширення гострої респіраторної хвороби COVID-19, спричиненої коронавірусною інфекцією SARS-CoV-2	214
ГОРНИЙЧУК І.В., СВЕЦЬКИЙ В.Л. Аналіз діагностичних ознак біометричних векторів для оцінки ефективності використання рукописного підпису в системах аутентифікації	216
ПОКРОВСЬКА В.В., ЦУРКАН В.В. Форми підвищення обізнаності зі забезпечення кібербезпеки	218
СУБАЧ І.Ю., ЄВДОЧЕНКО Л.О., ЧАУЗОВ О.М. Створення ситуаційних центрів з кібербезпеки для розбудови ефективної системи колективного реагування на кіберінциденти	219
ЮДІН О.К., КРИХОВЕЦЬКИЙ Г.Я., СИДОРЕНКО С.М., ТИКВА В.Л., КУЗЬМЕНКО В.В. Аналіз методів та моделей соціальної інженерії в задачах захисту державних інформаційних ресурсів	221
СОБОЛЄВ А.М. Дослідження мережевих ЗМІ в Інтернеті	223
АНДРЕЙЧУК О.В., БРАІЛОВСЬКИЙ М.М. Атаки RANSOMWARE та методи їх запобігання	225
БЛОХІНА Д.М., БРАІЛОВСЬКИЙ М.М. розвиток систем з ортогональним частотним розподіленням каналів і мультиплексуванням: OFDM	227
L.O. KUPRIŃA, M.M. BRAILOVSKYI Deepfake technology as a threat to information security	229
КАЧМАЛА О.В., БРАІЛОВСЬКИЙ М.М. Сучасні технології оцінювання стану захищеності інформаційних ресурсів на основі досліджень джерел загроз інформаційній безпеці	232
ТОЛЮПА С.В., КОТОВ М.С., КУЛЬКО А.А., САВЧЕНКО К.С. Побудова інтелектуальних систем виявлення атак	234
ТОЛЮПА С.В., ПАРХОМЕНКО І.В., ХИЖНЯК А.О., ДМИТРИЄВА І.С. Побудова систем управління інформаційною безпекою на основі програмного продукту SPLUNK	236
ДАНИЛЬЦО А.С., БІЛАН С.М. Мультимодальні біометричні технології в системах захисту інформації	238
БЕЗУХ Б.Ю., СВЕЦЬКИЙ В.Л. Система захисту комп’ютерних даних з використанням динамічних біометричних характеристик користувача	239

ШАБУНІН В.В., ЄВЕЦЬКИЙ В.Л. Покращення характеристик псевдовипадкових послідовностей	241
ВРУБЛЕВСЬКИЙ В.С., ЖИЛІН А.В. Аналіз платформи обміну інформацією про кіберінциденти MISF	242
МАКСИМЕЦЬ А.В., ЖИЛІН А.В., ВОЛОШИН Г.В. Методи виявлення та аналізу безфайлових атак	243
КРЕХОВЕЦЬКИЙ А.Ю., ЖИЛІН А.В. Автоматизація системи управління центру оперативного виявлення та реагування на кіберінциденти	244
ЖИЛІН А.В., ШАПОВАЛ О.М., ПРИВЕРТ Д.В. Модель та реалізація інтегрованої платформи кібернавчачь тактичного рівня	245
КОРОТАЄВ С.О., КУЛКОВ В.М., ОПЕРЧУК О.С. Програмний модуль візуалізації результатів контролю трафіку поштового серверу	246
РОМАНИШИН Д.М., КУЛКОВ В.М. Метод фокусованого пошуку в завданнях технічної діагностики	247
РИБАК О.О., ЛАНДЕ Д.В. Система «кіберагрегатор» – міграція в напрямку Big Data	249
РИБАК О.О., ЛАНДЕ Д.В., СОБКО А.В. Інтегрований підхід до виявлення джерел деструктивного впливу в соціальних мережах	250
МІТІН С.В., ГОРИНІН О.С., КОПІЙКА О.В. Система захисту серверу веб застосувань від TCP SYN flooding атак	251
МІЩЕНКО Р.М., МІТІН С.В., КОПІЙКА О.В. Система моніторингу та аналізу успішності студентів з модулем прогнозування напрямів діяльності випускників	252
ЗАВАЛЬНА Р.С., РЯБЦЕВ В.В. Підсистема контролю знань інформаційної системи підтримки професійного навчання	253
ЗЮЗІН І.О., РЯБЦЕВ В.В. Аналіз вимог щодо безпечного використання інформації з обмеженим доступом для захищеної LMS	255
ЛЕЙКО С.Г., РЯБЦЕВ В.В. Адаптивний рейтинговий модуль інформаційної системи ВНЗ	257
РЕЗНІК С.Є., РЯБЦЕВ В.В. Право на мобільність персональних даних за вимогами GDPR, як функція програмного модулю «Викладачі» ІС ВНЗ	258
ОЛЕКСІЄВЕЦЬ Я.В., СОКОЛОВ В.В. Методика аналізу використання зовнішніх ресурсів під час дослідження шкідливого програмного коду методами реверс-інжинірингу	259
ПАТЕНКО В.О., СОКОЛОВ В.В. Методика аналізу використання вразливих функцій під час дослідження програмного коду методами реверс-інжинірингу	260
САВОЙСЬКИЙ Г.С., СОКОЛОВ В.В. Модель обчислень на основі трансформації сполук об'єктів	261
КУБРАК В.О., СУБАЧ І.Ю., МАРТИНОВ В.Д. Підсистема інформування команди реагування на інциденти безпеки системи управління інформаційною безпекою SPLUNK	262

МИКИТЮК А.В., СУБАЧ І.Ю., ГРЕТ С.В. Алгоритм моніторингу інформаційних потоків для запобігання витоку даних з інформаційно-телекомунікаційних мереж	263
КЕЛИМ М.А., УСПЕНСЬКИЙ О.А. Застосування прихованого моніторингу в технічній комп'ютерній розвідці	264
БЛЮВИЦЬКА І.А., ПЦУК М.О., ЦУРКАН В.В. Моделі програмного компоненту аналізування шкідливого програмного забезпечення	265
КОВАЛЬЧУК Д.І., ЦУРКАН В.В. Моделі програмного засобу візуалізування несанкціонованих підключень USB флеш накопичувачів	266
ПОПРУЖНА К.П., ЦУРКАН В.В. Моделі програмного модулю оркестрування засобів забезпечення кібербезпеки	267
ЦУРКАН В.В., ЧЕРНАТА С.О. Моделі програмного компоненту автоматизування мережевих налаштувань	268
ЦУРКАН В.В., ЮДІНА Д.О., НАГОРНИЙ Р.М. Моделі програмного компоненту оцінювання ризику кібербезпеки критичної інформаційної інфраструктури	269
ВЕРБЦЬКИЙ Б.В., ШАРАДКІН Д.М. Використання нейронних мереж для пошуку аномалій в роботі комп'ютерних мереж	270
ГРУДІЛОВА О.В., ШАРАДКІН Д.М. Проблеми пошуку та огляд методів виявлення аномалій в потоках даних за допомогою статистичного аналізу часових рядів	272
ТУРЧИНА К.В., ШАРАДКІН Д.М. Потокова кластеризація та її використання для виявлення загроз в інформаційно-комп'ютерних мережах	274
МУЖЕСЬКИЙ К.К., ШАРАДКІН Д.М., ХАРЕНКО В.Р. Програмний модуль он-лайн моніторингу та виявлення аномалій поведінки в комп'ютерних мережах за допомогою методів машинного навчання	276
ГОРОНДЕЙ Є.В., ЯКОВІВ І.Б. Методика протидії каналам дистанційного управління АРТ-атаками	278
ОВЧАРЕНКО Д.І., ЯКОВІВ І.Б. Автоматизація процедур розвідки кіберзагроз на основі технології SCAP	279
ЯРЕМЧУК Ю.Є., САЛІЄВА О.В. Оцінювання рівня захищеності об'єкта критичної інфраструктури	280
ПОТОЦЬКИЙ В.М., КОРОСТЕЛКІН М.В., БІЛАН С.М. Дослідження генератора псевдовипадкових чисел на основі клітинних автоматів з активними клітинами	282
ЦУРКАН В.В., ВОЛОШИН Д.В. Забезпечення кібербезпеки методами машинного навчання	283
ЦУРКАН В.В., ГРИЦУНЬ К.Б. Візуалізування стану забезпечення кібербезпеки за технологією CyGraph	284
ГАВРИЛЯК В.Б., ПАРШУКОВ С.С. Щодо застосування поняття “забезпечення кібербезпеки” в галузі публічного управління в Україні	286

науково-практична конференція  
**«ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ  
СИСТЕМИ І ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА:  
НОВІ ВИКЛИКИ, НОВІ ЗАВДАННЯ»**  
(ІТСТК-2020)

(заочна форма проведення, онлайн-режим)

Збірник матеріалів науково-практичної конференції  
18-19 листопада 2020 року

Підписано до друку 10.11.2020 Формат 60x84/16. Папір офсетний.  
Гарнітура «TimesNewRoman» Друк – цифровий.  
Ум. друк. арк. 17,09. Обл. вид. арк. 18,38.