

Міністерство освіти і науки України
Державна наукова установа “Інститут модернізації змісту освіти”
Центральноукраїнський національний технічний університет

Комп’ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали Всеукраїнської науково-практичної
конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27–29 листопада 2018 р.)

Кропивницький ЦНТУ 2018

УДК 004
ББК 32.97
К63

К63 Комп'ютерна інженерія і кібербезпека: досягнення та інновації: матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) / М-во освіти і науки України, Держ. наук. установа “Інститут модернізації змісту освіти”, Центральнуокр. нац. техн. ун-т. — Кропивницький: ЦНТУ, 2018. — 448 с.

Збірник містить тези доповідей учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених “Комп'ютерна інженерія і кібербезпека: досягнення та інновації” (м. Кропивницький, 27–29 листопада 2018 року). Праці присвячені актуальним питанням інформаційних систем і технологій, технологій проектування комп'ютерних систем та мереж, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних ІТ, комп'ютерної електроніки, логіки, схемотехніки, графіки, нормативно-правових засад забезпечення кібернетичної безпеки, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для аспірантів, докторантів, науковців, викладачів і студентів технічних спеціальностей закладів вищої освіти та всіх, хто цікавиться питаннями комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 11 від 29 листопада 2018 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

*Тексти матеріалів конференції друкуються у авторській редакції, мовою оригіналу.
За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації
відповідальність несуть автори.*

Адреса організаційного комітету конференції

Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

© Автори матеріалів, 2018
© Центральноукраїнський
національний технічний
університет, 2018

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

<i>Huskova V. H., Bidyuk P. I. A Combined Approach to Modeling Heteroscedastic Processes and Financial Risk Estimation</i>	14
<i>Litvinov A. A., Viniichuk Y. V., Dubovyi M. V., Bezotosnyi D. O. On Specific of Field Level Database Optimistic Locking for Increasing Information System Performance</i>	17
<i>Артеменко-Діденко А. І., Маковецько Д. О. Моделювання пропускнуої здатності мережі E-UTRA для адаптивних режимів MCS</i>	18
<i>Береговий С. М. Побудова інформаційних систем керування виробничими конвеєрними лініями засобами SCADA Wonderware System Platform</i>	21
<i>Бураков Р. А., Левицька Т. О. Автоматизована обробка класичних творів для фортепіано з використанням сіамської нейронної мережі</i>	22
<i>Вакуленко Д. О. Актуальні питання впровадження інфокомунікаційних технологій в агропромисловому комплексі України</i>	24
<i>Гвозденко В. О., Дем'янчик С. О., Давиденко Є. О. Технологія прийняття оптимального стратегічного рішення в військово-цивільній сфері</i>	26
<i>Голобородько Р. В. Дослідження захищеності мереж UMTS/LTE із використанням двостороннього підсилювача у комплексі зі спрямованою антеною</i>	28
<i>Гончар О. М., Дреєва Г. М. Використання спеціалізованих мов програмування для операторів програмованого обладнання</i>	30
<i>Гринюк С. В., Кирилюк Л. М. Scratch як об'єктно-орієнтоване середовище візуального програмування</i>	32
<i>Грінченко Є. М., Колмик О. О. Методи управління інформаційними ризиками</i>	35
<i>Гура І. О., Александров Р. І. Важливість впровадження та розвитку кіберфізичних систем в Україні</i>	37
<i>Дмитрієва О. А., Клімаш О. В. Алгоритмічні методи кластеризації в рекомендаційних системах з колаборативною фільтрацією</i>	39
<i>Дмитрієва О. А., Гуськова Н. Г. Зведення чисельної реалізації рівнянь в частинних похідних до методу прямих на коллокаційних блокових різницевих схемах</i>	41
<i>Дмитрієва О. А., Александров М. О. Підвищення ефективності методу контентної фільтрації з урахуванням розрідженості даних</i>	43
<i>Желєзняк Б. Ю. Переваги квантових комп'ютерів</i>	45
<i>Желєзняк Б. Ю. Огляд найбільш використовуваних на практиці алгоритмів</i>	47
<i>Желєзняк Б. Ю. Огляд історії розвитку квантової криптографії</i>	49
<i>Жолнер І. Д., Вялкова В. І. Використання теорії живих систем у СКЗІ</i>	51
<i>Заволодько Г. Е., Павлова Д. Б., Колеснікова Я. С. Інформаційна мережа систем спостереження як основа інформаційного забезпечення користувачів системи контролю повітряного простору</i>	52

<i>Ізотов Є. О.</i> Аналіз сервісу управління персоналом як частина кіберфізичної системи університету	55
<i>Ісмаїлов К. Ю., Балтовський О. А.</i> Концепція побудови динамічної інформаційної системи управління складної соціально-організованою структури	56
<i>Казарінова М. В.</i> Дослідження класифікаційних моделей для організації інформації в електронних бібліотечних системах	58
<i>Коба О. В.</i> Використання системи геСАРТСНА як засобу оцифровки друкованих носіїв	60
<i>Коваленко О. В., Коваленко А. С.</i> Аналіз основних підходів математичного моделювання та методологій для забезпечення максимальних показників безпеки програмного забезпечення	63
<i>Ковальова К. М.</i> Розробка методики діагностування цифрових систем	66
<i>Кузнецов О. О., Агєєва М. М.</i> Біометрична автентифікація на основі динамічної обробки зображень облич із використанням методу Eigenface	67
<i>Кузнецов О. О., Власенко О. В.</i> Біометрична автентифікація на основі відбитків пальців	69
<i>Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С.</i> Питання підвищення рівня захищеності в інформаційно-телекомунікаційних системах	71
<i>Кячев О. А.</i> Аналіз механізмів захищеності систем Інтернету речей	73
<i>Лозовий А. М.</i> Використання віртуальних машин для завантаження криміналістичних образів жорстких дисків	74
<i>Лудан Д. В.</i> Розробка інформаційної технології для організації інтерактивних квестів	76
<i>Можарівський В. В.</i> Автоматизована торгівля на біржах криптовалют	78
<i>Нетепенко В. В.</i> Ідентифікації диктора за голосом	79
<i>Окунь Є. В., Романько Д. В.</i> Інтернет речей та проблеми його захисту	81
<i>Остапенко А. О.</i> Застосування кінетичного підходу до моделювання гідродинаміки	83
<i>Підгорний П. Є., Сидорова М. Г.</i> Розробка програмно-математичного забезпечення для аналізу траєкторій пересування об'єктів у просторі та часі	86
<i>Пісарєв Д. С., Петрова О. О.</i> Візуалізація «backtracking algorithm»	88
<i>Пономаренко А. С.</i> Місце генетичних алгоритмів у сучасному світі	89
<i>Пономаренко А. С.</i> Класифікація атак на інформаційні системи	91
<i>Проніна О. І.</i> Формалізація організації заказу в умовах індивідуальних потреб клієнта	93
<i>Пронюк М. Я., Кропивницька В. Б.</i> Порівняльний аналіз баз даних SQL та NoSQL	96
<i>Рідозуб О. В.</i> Розробка базових підходів до створення програмного забезпечення для роботи з напівпровідниковими детекторами CdTe, CdZnTe	97
<i>Рудакова Є. О.</i> Інформаційна система ідентифікації рослин	99

<i>Савчук Т. О., Приймак Н. В.</i> Інформаційна технологія пошуку асоціативних правил при розробці програмного забезпечення	100
<i>Семенченко О. А.</i> Аналіз розвитку інформаційних систем у світі	103
<i>Середін О. Д., Шматок О. С.</i> Порівняння потужності критерія Крамера - фон Мізеса і критерія хі-квадрат для малих тестових вибірок біометричних даних	106
<i>Єлізаров А. Б., Симониченко Я. А., Симониченко А. А.</i> Дослідження сучасних програмних стеганографічних засобів приховування інформації.....	108
<i>Смірнова Т. В., Смірнов О. А., Дреєв О. М., Смірнов С. А.</i> Використання хмарних експертних систем в сфері інформаційного забезпечення обробки поверхні деталей	111
<i>Стовманенко В. О., Григор'єв Д. О., Давиденко Є. О.</i> Використання алгоритмів системного аналізу для роботи із медіа	114
<i>Столяренко Є. Ю., Неласа Г. В.</i> Розробка веб-сервісу для виконання операцій з елементами скінченних полів.....	116
<i>Ткачук Р. О.</i> Переваги операційної системи Linux	117
<i>Фесечко Д. В.</i> Порівняльний аналіз формату MP3.....	119
<i>Фесечко Д. В., Коноплицька-Слободенюк О. К.</i> Методології розробки програмного забезпечення	121
<i>Четверик А. І.</i> Визначення коефіцієнтів розподілу грошових коштів за заходами.....	122
<i>Шевченко М. М.</i> Хмарний сервіс зберігання даних.....	123
<i>Шуліка Я. П.</i> Сучасне on-page SEO	125
<i>Шуліка Я. П.</i> Біле та чорне SEO	126
<i>Шуліка Я. П.</i> Сучасне off-page SEO	127
<i>Щербак В. К.</i> Використання сенсору Kinect в системах діагностування рухомих об'єктів	129
<i>Щербак Б. В.</i> Розробка модулю автоматизовані системи для подачі матеріалу студентам за допомогою технологій доповненої реальності.....	131
ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ	
<i>Берладін В. К., Коноплицька-Слободенюк О. К.</i> Квантові технології сьогодення та перспективи їх розвитку	132
<i>Горбань А. С., Цололо С. О.</i> Декомпозиція першого технологічного циклу синтезу оксидних нанопорошків	134
<i>Жесан Р. В., Голик О. П.</i> Коротке узагальнення основних причин вразливості сучасних комп'ютеризованих систем	137
<i>Колосов А. А.</i> Моделювання компонентів керування MEMC зі зворотними зв'язками з використанням Matlab / Simulink.....	140

<i>Колосов Є. А.</i> Моделювання мікроелектромеханічних актюаторів з використанням Matlab/Simulink	141
<i>Кумченко Ю. О., Нагін Р. Ю.</i> Платформа віртуалізації Proxmox VE для керування кластерами високої доступності	142
<i>Кумченко Ю. О., Шевченко О. В.</i> Комплексна система захисту серверного приміщення	144
<i>Маркова О. М., Дяченко Д. О.</i> Інформаційна система для контролю безпеки підйомних судів у залізничних шахтах	146
<i>Минайленко Р. М., Дреєв О. М., Собінов О. Г., Денисенко О. О.</i> Програмна компенсація дрейфу нуля в системі вимірювання вологості зерна в потоці	148
<i>Незамай В. О.</i> Використання методу автоматного програмування при побудові систем комунікації «Smart House»	150
<i>Пасічко Є. В.</i> Верифікація кінцевого автомата з допомогою UVM	151
<i>Покотило О. А.</i> Аналіз протоколу динамічної маршрутизації BGP та його вразливостей	152
<i>Сіленко М. О.</i> Вибір системи числення для побудови комп'ютерних систем	154

ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

<i>Liubchenko O. S.</i> Research Generation Register Model Components Methods for Verification Environment	155
<i>Бабич Є. Ю.</i> Кооперативна багатозадачність в RTOS	157
<i>Банченко В. О.</i> Дослідження та програмна реалізація стиснення звукової інформації за допомогою вейвлетних методів	158
<i>Башиїнська О. О.</i> Особливості розшифровки телеметричних логів безпілотних авіаційних комплексів в умовах неповноти інформації про перелік типів повідомлень	160
<i>Бобилєва О. С., Дмитрієва О. А.</i> Дослідження методу стрільби при розв'язанні крайових задач	163
<i>Газдюк К. П., Жихаревич В. В., Остапов С. Е., Чижевський В. В.</i> Розробка системи для комп'ютерного моделювання біологічних процесів	166
<i>Ганістрат Д. О., Карабут Н. О.</i> Методи інтеграції програмного забезпечення	167
<i>Згара К. Г.</i> Компоненти та архітектура корпоративної соціальної мережі	168
<i>Золотухін Б. Є.</i> Актуальні питання стандартизації та регламентації процесів реалізації програмних засобів	169
<i>Іванова О. Т., Сидорова М. Г.</i> Опанування проблеми управління часом за допомогою інформаційних технологій	170
<i>Константинова А. А., Константинова Л. В.</i> Дослідження засобів для підвищення транзакційної продуктивності MySQL	171

<i>Косолап М. В., Михальчук Г. Й.</i> Програмне забезпечення для розв’язання задачі маршрутизації з різнорідним вантажем	172
<i>Майданик О. О.</i> Особливості генетичних алгоритмів	173
<i>Майданик О. О.</i> Важливість оптимізації коду	175
<i>Манченко Я. В.</i> Спеціалізовані програмні засоби діагностики стану користувача глобальної мережі	177
<i>Мишевський Г. А., Кузнєцов Д. І.</i> Методи та засоби оптимізації пошуку медіа файлів у хмарних сховищах на основі використання Android додатку	178
<i>Пархоменко Д. О.</i> Концептуальні засади забезпечення якості програмних продуктів	180
<i>Патиковський Ю. В.</i> Структурно-функціональні особливості оцінки якості програмних засобів критичного призначення	181
<i>Петренко А. Б., Колпаков М. О.</i> Інтеграція хмарних сховищ Amazon S3 у веб-додатки розроблені засобами мови програмування Java	182
<i>Петренко Д. О.</i> Аналіз методів та розробка прототипу програмної системи для моніторингу технічного стану автомобіля	185
<i>Половинка О. Л.</i> Використання паралельної реалізації для пошуку асоціацій	186
<i>Ткаченко О. С.</i> Аналітична оцінка трудомісткості процесів реалізації програмних засобів	187
<i>Фесечко Д. В.</i> Принципи роботи з великими даними	188
<i>Фролова М. С., Снівак Р. В.</i> Застосування технології доповненої реальності та 3d-моделювання для попередження надзвичайних ситуацій	190
<i>Черніков Д. Д., Коноплицька-Слободенюк О. К.</i> Проблема 2038 - 32bit systems	192
КОМП’ЮТЕРНІ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ	
<i>Бабич Є. Ю.</i> Небезпека штучного інтелекту	193
<i>Берладін В. К., Гермак В. С.</i> Штучний інтелект у сучасному світі	194
<i>Боярський Д. О.</i> Генерація дизайну сайтів на основі використання згорткових генеративних змагальних мереж глибокого навчання	196
<i>Власюк І. В., Сухомлин А. А.</i> Нейронні мережі з розподіленою обробкою даних	197
<i>Гіцеларь Д. В.</i> Штучний інтелект та його залежність від відеоігор	198
<i>Гіцеларь Д. В.</i> Методи утворення штучного інтелекту комп’ютерно-керованим персонажем. Обґрунтування вибору саме нейронної мережі	200
<i>Гриб О. О., Коноплицька-Слободенюк О. К.</i> Штучні нейронні мережі	202
<i>Калюжний Р. І.</i> Симбіоз штучного інтелекту і хмарних технологій	204
<i>Котов І. А.</i> Модель маркування сигнального графа мережі метаправил в онтологіях інтелектуальних систем	205

<i>Логінова С. М.</i> Дослідження методу лейтнера з нейромережею для мобільного додатку вивчення іноземної мови	208
<i>Маценко Р. В.</i> Використання нейромережевої комп'ютерної системи для анімаційних об'єктів	210
<i>Мельник Р. А., Шпортко В. О., Тушиницький Р. Б.</i> Програмне забезпечення для екстракції, збереження та опрацювання зображень супутникових карт хмарності	211
<i>Разно В. С.</i> Штучна нейронна мережа. Нейронні мережі проти звичайних комп'ютерів.....	213
<i>Сидоренко С. В.</i> Прогнозування тенденцій рівня цукру у крові за допомогою нейронної мережі	215
<i>Сінєгіна А. Д.</i> Передача стилю за допомогою нейронної мережі	216
<i>Сінєгіна Ю. Д.</i> Колоризація зображень за допомогою згорткової нейронної мережі	218
<i>Холоша М. С., Сидорова М. Г.</i> Побудова ансамблю нейронних мереж для тегування зображень	220
<i>Шуліка Я. П.</i> Сучасні можливості штучного інтелекту	221

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

<i>Безрук Є. А., Брусеньский В. Р., Козіна Г. Л.</i> Впровадження технології блокчейн в торгівлю цінними паперами	223
<i>Демидов З. Г.</i> Big data: застосування та можливості.....	225
<i>Дреєва Г. М.</i> Імітаційне генерування фрактального трафіку за допомогою GERT моделі	226
<i>Коваленко Д. О.</i> Розробка програмного забезпечення для веб-ресурсу “Планувальник навантаження викладачів ХНЕУ імені Семена Кузнеця”	230
<i>Коваль В. О.</i> Переваги та недоліки клієнт-серверної архітектури	231
<i>Коваль В. О., Коноплицька-Слободенюк О. К.</i> Переваги та недоліки мережевих топологій	232
<i>Константинова Л. В., Константинова А. А.</i> Дослідження засобів для кросплатформеної розробки мобільних додатків	234
<i>Константинова Л. В., Константинова А. А.</i> Огляд існуючих засобів для повнотекстового пошуку в веб-проектах.....	236
<i>Корованенко В. В.</i> Оптимізація процесу вибору постачальника безкоштовного хостингу.....	238
<i>Кулік І. С.</i> Система підтримки прийняття рішення при оцінюванні якості трафіку в NGN.....	241
<i>Кучерявий М. В.</i> Аналіз алгоритмів взаємодії елементів інтернету речей	244
<i>Мамонтов О. О.</i> Застосування методів сплайнапроксимації для синтезу характеристик нелінійних пристроїв засобів телекомунікації	247
<i>Матвєєнко Ю. В.</i> Сучасні WEB-дизайн і інтернет-технології	248

<i>Оксіюк О. Г., Кротов В. Д.</i> Управління потоками даних в Ad Hoc мережах спеціального призначення	250
<i>Ткаченко Е. В.</i> Огляд сучасних технологій розробки баз даних їх властивостей та функцій.....	253
<i>Цюпко В. В.</i> Хмарні сервіси SaaS, PaaS, IaaS і їх тренди розвитку	255
<i>Шуліка Я. П.</i> Розробка сайту з урахуванням SEO	257

КОМП'ЮТЕРНА ЕЛЕКТРОНІКА, ЛОГІКА Й СХЕМОТЕХНІКА

<i>Аносов О. В.</i> Аналіз застосування методу АЕР для формальної верифікації HDL-опису дизайнів цифрових систем.....	259
<i>Антонюк М. А., Неласа Г. В.</i> Дослідження арифметики точок еліптичної кривої на пристроях з обмеженим об'ємом пам'яті	261
<i>Кучеренко І. О.</i> Використання темпоральних графів при розробці шаблону опису алгоритмів функціонування скінченних автоматів	262
<i>Майданик О. О.</i> Мови опису апаратури для ПЛІС та їх використання в сучасній обчислювальній техніці	264
<i>Попко С. О.</i> Розробка інтелектуального зарядного пристрою на основі мікроконтролера	266
<i>Семеніхін Д. О.</i> Моделювання MEMS сенсорів з використанням Matlab/Simulink.....	267
<i>Сенько А. О., Андрющенко Д. Ю.</i> Дослідження структури статичного ОЗП	269

КОМП'ЮТЕРНА ГРАФІКА

<i>Абель Т. В., Дреєва Г. М.</i> Дослідження та програмна реалізація системи генерування зображення за допомогою рекурентних повторень.....	271
<i>Гіцеларь Д. В.</i> Огляд та практичне застосування L-систем.....	273
<i>Долженко І. О.</i> Дослідження методів сегментації для розпізнавання харчових об'єктів ...	275
<i>Карпов Є. О.</i> Особливості комп'ютерної графіки в контексті Net-Art	277
<i>Ладигіна О. А.</i> Аналіз моделей освітлення для досягнення фотореалізму у віртуальній реальності	279
<i>Сахарова А. В.</i> Цифрове оточення людини	281
<i>Ткаченко А. М.</i> Роль комп'ютерної графіки у підготовці майбутнього фахівця в сучасних умовах працевлаштування	283
<i>Шевченко В. О.</i> Вибір засобів комп'ютерної графіки для вирішення прикладних задач	285

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

<i>Obach V.</i> Current Issues of Cyber Defense in Ukrainian Billing and Payment Systems	286
<i>Гайтота Є. В., Чуницька В. В., Нікуліщев Г. І.</i> Про врахування досвіду Німеччини в Стратегії кібербезпеки України	288

<i>Жогов В. С., Форос Г. В.</i> Особливості нормативно-правового регулювання кібербезпеки в Україні та в законодавстві інших країн	291
<i>Колодяжний І. О.</i> Вдосконалений підхід до протидії пропаганді сепаратизму та антиукраїнській ідеології в соціальних мережах.....	293
<i>Копиця Н. С., Ликов Ю. В.</i> Аналіз документа “Політика конфіденційності” на базі регламенту GDPR в популярних інтернет-ресурсах	295
<i>Обач В. А., Гермак В. С.</i> Аналіз впливу темних патернів на свідомість людини	297
<i>Прокопов В. В., Гермак В. С.</i> Огляд основних вразливостей SCADA-система та засобів їх усунення	298
<i>Романовська М. С.</i> Компаративний аналіз визначення сутності поняття „кібербезпека”	300
<i>Семеній Д. М.</i> Нормативно-правові засади забезпечення кібербезпеки України	303
<i>Толмачов Ю. П.</i> Актуальні питання забезпечення інформаційної безпеки у медіасфері України	306
<i>Хомяк О. О., Шматок О. С.</i> Методологія формування систем захисту інформації сучасних АС	307

ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОГО СЕГМЕНТА КІБЕРПРОСТОРУ

<i>Артюх С. Г., Шевченко А. С.</i> Аналіз методик забезпечення інформаційної безпеки організацій та інформаційних систем	308
<i>Безрук Є. А., Брусеньский В. Р., Нікуліцев Г. І.</i> Використання технології uXTD та методу Timing-атак для деанонізації користувачів Тог.....	309
<i>Бойко О. С.</i> Протидія несанкціонованому запису мовної інформації	312
<i>Колодяжний І. О.</i> Дослідження алгоритмів аналізу віртуальних соціальних мереж	315
<i>Леонтьєв В. С., Неласа Г. В.</i> Аналіз методів спарювання точок еліптичних кривих	317
<i>Майборода О. П.</i> Демаскуючі ознаки GSM і CDMA радіоакустичних закладних пристроїв.....	318
<i>Недільський Д. С.</i> Інформаційні війни в соціальних мережах	320
<i>Петров М. В.</i> Дослідження технології блокчейн, криптографії та крипто валют.....	321
<i>Прокопов В. В.</i> Нормативно-правові засади протидії маніпуляціям суспільною свідомістю і поширенню спотвореної інформації в Україні.....	322
<i>Савченко О.О.</i> Специфічні властивості скручених кривих Едвардса для криптографічних додатків	324
<i>Трухачов А. В., Козіна Г. Л.</i> Аналіз захищеності ідентифікації клієнта у системі Біткоін.....	326
<i>Шуліка Я. П.</i> Сучасна пропаганда як продукт інформаційного простору	327
<i>Щирова Ю. А.</i> Аналіз впливу атак на традиційні системи автентифікації користувачів.....	329

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

<i>Білоконь Д. С., Форос Г. В.</i> Окремі аспекти протидії кіберзлочинності.....	331
<i>Вакулинська А. Є.</i> Методи біометричної автентифікації.....	334
<i>Глазунов Д. М.</i> Важливість забезпечення захисту інформації від загроз соціальної інженерії.....	336
<i>Донченко П. О., Жума В. М., Савельєва Т. В.</i> Механізм реагування на потенційно небезпечні дії користувача в Linux.....	339
<i>Кривенко С. С., Шматок О. С.</i> Методи виявлення закладних пристроїв	341
<i>Кульчицький О. С.</i> Вимоги протидії кіберзлочинності в умовах громадської локалізації.....	344
<i>Макеєв А. В.</i> Огляд особливостей кіберзлочинів в Україні	345
<i>Пашинських В. В.</i> Огляд дистрибутивів GNU/Linux для тестування безпеки	346
<i>Пашинських В. В., Коноплицька-Слободенюк О. К.</i> Двофакторна автентифікація: огляд та недоліки.....	348
<i>Пашинських В. В.</i> Огляд інструментів для пентестинга.....	350
<i>Поліщук О. В., Карабут Н. О.</i> Кібертероризм як глобальна проблема	352
<i>Стрілець А. М.</i> Основні технології проти кіберзлочинності	354
<i>Хлистун В. В.</i> Кіберзлочинність як загроза для кожного: види, причини розвитку, поради до протидії загрозам	357
<i>Шостак В. І.</i> Захист інформаційних ресурсів та засобів обробки інформації	359

ЗАХИСТ ПРОГРАМ ТА ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

<i>Sokolov V. Y., Korzhenko O. Y.</i> Analysis of Recent Attacks Based on Social Engineering Techniques.....	361
<i>Аяз Р. Х.</i> Використання конволюції/деконволюції для стегоаналізу зображень в рамках підходу Хармсена и Перл мана	364
<i>Бабюк Є. М.</i> Інновації у сфері кібербезпеки: хмарні ресурси та машинне навчання	366
<i>Байлюк Є. М.</i> Розвідувальна організація з питань загроз Cisco Talos Intelligence Group ...	368
<i>Байлюк Є. М.</i> Покращений протокол безпеки безпроводних мереж Wi-Fi Protected Access 3 (WPA3)	370
<i>Безносюк І. В.</i> Сучасні методи аутентифікації	372
<i>Безрук Є. А., Брусеньский В. Р., Неласая Г. В.</i> Використання технології ubeacons для тергетингу та методи боротьби з нею	374
<i>Вервейко В. В.</i> Аналіз методів захисту від комп'ютерних вірусів	377
<i>Власов Б. Ф.</i> Модернізація алгоритму гешування MD5	378
<i>Ганечко О. О., Даніленко В. М., Сагун А. В.</i> Підсистема інтелектуальної фільтрації електронних повідомлень на базі алгоритму машинного навчання	380

<i>Гонтарь І. А.</i> Методика виявлення вразливостей мереж стандарту IEEE 802.11 з використанням пакету KALI LINUX.....	383
<i>Грек О. М., Марчук А. В.</i> Розробка технологій захисту від мережних атак із використанням апарату штучних нейронних мереж	385
<i>Гриб О. О.</i> Особливості роботи брандмауерів	386
<i>Григоров А. Г.</i> Актуальність протидії XSS-атакам та засоби захисту від них	388
<i>Гурєєва А. О., Карабут Н. О.</i> Методи і технології захисту комп'ютерних мереж (фізичний та каналний рівні).....	390
<i>Дмитрієва О. А., Горбенко В. Ю.</i> Створення відмовостійких розподілених інформаційних систем	392
<i>Добринін К. І.</i> Засоби забезпечення захисту аккаунтів користувачів при використанні публічних мереж стандарту 802.11	393
<i>Журова П. В.</i> Блочне шифрування з властивостями виправлення помилок	395
<i>Ільєнко А. В., Яковенко О. Л., Данилюк Ю. Р.</i> Аналіз сучасних методів автентифікації з використанням криптографічних перетворень.....	396
<i>Коваль В. О.</i> Захист персональних даних в Інтернеті.....	398
<i>Колмик О. О., Грінченко Є. М.</i> Майнінг на чужих ресурсах.....	399
<i>Кохан Є. Р.</i> Соціальна інженерія як загроза інформаційній безпеці.....	401
<i>Крапівін В. В.</i> Система виявлення мережових атак на основі алгоритмів нечіткого виведення.....	402
<i>Краштанук К. К.</i> Чи потребує Інтернет Речей інтеграції блокчейну?	405
<i>Кузнєцов О. О., Попова М. В., Шаповал О. В., Чернов К. А., Єрьомин Е. С.</i> Аналіз і дослідження автоматизованих технологій пошуку вразливостей програмного забезпечення	406
<i>Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С.</i> Аспекти експрес аналізу захищеності комп'ютерних даних.....	409
<i>Лісова В. П.</i> Аналіз методів пошуку прихованих мереж в корпоративній мережі з розгорнутими ролями Active Directory	411
<i>Мартиненко О. О., Телющенко В. А.</i> Оцінка надійності програмних засобів захисту	413
<i>Марченко А. Ю.</i> Мінімізація факторів суб'єктивності в тестуванні на проникнення.....	414
<i>Маисталер Д. О.</i> Динамічне використання групи ключів в асиметричному Шифруванні	415
<i>Михайловський Р. Л., Шматок О. С.</i> Система стеганоаналізу на основі розпізнавання образів	416
<i>Недільський Д. С., Коноплицька-Слободенюк О. К.</i> Grey Wizard – нові технології захисту веб-ресурсів.....	418

<i>Оксіюк О. Г., Руденко А. С.</i> Захист інформації у корпоративних мережах на основі моделі OSI	419
<i>Павлов І. І.</i> Методи підвищення надійності та захищеності корпоративних комп'ютерних мереж	421
<i>Покотило О. А.</i> Аналіз моделі Cyber Kill Chain та її використання для забезпечення захисту мережі	423
<i>Романько С. В., Астраханцев А. А.</i> Методи вбудовування цифрових водяних знаків у відеофайли, що стиснені за стандартами MPEG	425
<i>Сандаков О. О., Гермак В. С.</i> Огляд сучасних криптографічних алгоритмів	427
<i>Сердюк О. Ю.</i> Підхід щодо оцінки вразливостей інформаційних систем з використанням метрик стандарту NIST CVSS v3	429
<i>Трапезнікова В. П., Телющенко В. А.</i> Алгоритм вибору альтернативних засобів захисту для автоматизованої системи	432
<i>Удовиченко А. В.</i> Вибір методу аутентифікації у бездротових мережах	434
<i>Федорко М. А., Маслова Н. О.</i> Застосування вітчизняних стандартів шифрування для захисту даних великих обсягів	435
<i>Нікуліщев Г. І., Хвостенко А. І.</i> Дослідження та аналіз сучасних методів та засобів захисту хмарних обчислень	437
<i>Хемішінець Є. В., Куцак С. В.</i> Аналіз механізмів захисту даних в бездротових мережах	439
<i>Целуйко В. В., Никодюк Д. В.</i> Важливість використання SIEM в системах захисту банківської таємниці	442
<i>Чекурда О. М., Пономарьов О. А.</i> Формування моделі загроз для інформації, що циркулює в телекомунікаційних системах військового призначення	443
<i>Черняк Т. О., Глушко В. В.</i> Вдосконалення методів безпечного хешування при забезпеченні автентичності та цілісності даних у автоматизованих банківських системах	444
<i>Ярош І. В., Черняк Т. О.</i> Розробка системи виявлення вторгнень у web-додатки	446

**Вдосконалення методів безпечного хешування
при забезпеченні автентичності та цілісності даних
у автоматизованих банківських системах**

Високорентабельна економіка у процесі розвитку потребує впровадження ультрасучасної системи обігу грошей, а також експлуатації ефективних платіжних інструментів. Обсяги даних, які оброблюються у сучасних внутрішніх платіжних системах (ВПС), постійно зростають, з'являються нові електронні послуги, стрімко розвивається обчислювальна техніка – все це потребує збільшення показників безпеки даних у ВПС.

Актуальність теми зумовлена необхідністю створення теоретичної рекомендації по використанню методів ключового хешування, що забезпечують цілісність та автентичність інформації у всесвітніх платіжних системах комерційних банків. Нажаль, зараз не існує механізмів та концепцій, які б гарантували фінансову безпеку національної платіжної системи в цілому та банківської діяльності окремо, щоб при цьому ще були науково обґрунтовані.

Постійний розвиток ринкової економіки потребує належної платіжної системи, яка дозволить проводити розрахунки, що виповідатимуть світовим загальноприйнятим стандартам: де на першому знаходяться безпека, надійність та час проведення платежів. Національна платіжна система є складною та багаторівневою системою із централізованим керуванням. Саме це забезпечує надійний і важливий у стратегічному плані канал, через який фінансові транзакції проводяться.

НПС – це багаторівнева складна система управління критичного застосування або СУКЗ, де передача даних потребує постійного контролю над безпекою, при цьому це повинно здійснюватися на кожному рівні обов'язково. Підсистема криптографічної безпеки даних – це одна з найважливіших частин у складі ВПС, реалізація базується на відповідних механізмах та протоколах.

Питання безпеки ВПС та мереж зв'язку банківської й фінансово-кредитних сфер можна без перебільшення віднести до національного рівня. Методи обробки, зберігання та передачі даних, які використовувалися у інформаційних системах останні роки, самі по собі були факторами появи загроз. Вони пов'язані з ймовірністю повної втрати або спотворення чи втрати конфіденційності інформації, яка направлена чи належить кінцевому користувачеві.

Загроза інформаційної безпеки в інформаційних системах – це можливість втручання у дані, які обробляються автоматизованою системою, що може призвести до копіювання даних чи їх спотворення або знищення, блокування доступу, в тому числі втручання у дію роботу компонентів автоматичної системи.

Класифікація загроз інформаційної безпеки відбувається за наступними критеріями: компоненти інформаційних систем (ІС), на які направлені загрози (програмне забезпечення, дані, інфраструктура та підтримуюче обладнання); мета впливу; зовнішнє чи внутрішнє джерело загрози; спосіб реалізації (техногенний чи природний характер). [1]

Мета впливу загроз ділиться на три основні типи: загроза цілісності, доступності та конфіденційності.

На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних

реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Якщо проаналізувати загальну класифікація загроз інформаційної безпеки на ВПС, то можна зробити висновки, що є джерела ненавмисних загроз ІС:

- поламка складових частин обладнання;
- збій у роботі програмного забезпечення;
- неправильні дії з боку користувачів та персоналу;
- ненавмисні помилки у програмно-апаратному забезпеченні.

Звичайно, такі загрози наносять суттєвий збиток, але навмисні загрози з точки зору функціонування є більш значними, бо сама їх мета – це завдання збитків ІС або її користувачам. Такі загрози реалізуються шляхом довготривалої та масової атаки за допомогою вірусів чи несанкціонованих запитів. Атаки матимуть наступні наслідки: повна чи часткова втрата інформації, підтасовка даних, доступ до інформації отримують сторонні особи. Не важко уявити до чого можуть привести події такого роду. Тому протидія загрозам інформаційної безпеки, які вже були розглянуті вище, є пріоритетною задачею засобів захисту комп'ютерних систем та мереж. Послуги інформаційної виступають в якості засобів захисту ІС.

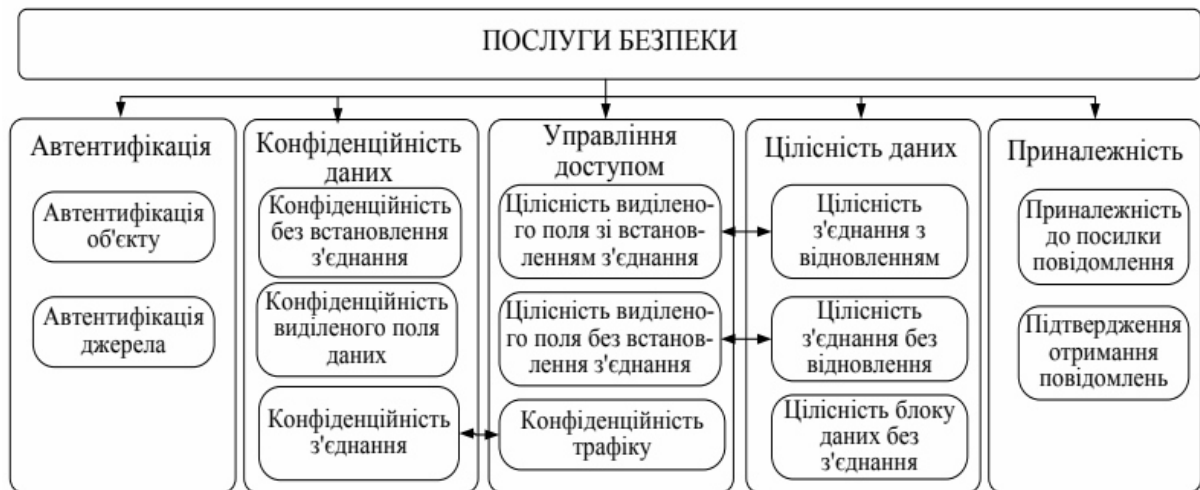


Рисунок 1 – Види послуг безпеки

За рахунок основних досягнень у сфері ІТ та комунікацій ВПС постійно розвивають да вдосконалюють свої функції. А саме послуги оплати насамперед через банкомати, термінали та віддалених користувачів; продаж товарів через онлайн-магазини тощо.

Характеристики обчислювальної техніки постійно модернізуються, а її продуктивність постійно зростає – це підтверджує закон Мура. Таким чином, інформаційні системи постійно вразливі перед різноманітними атаками та загрозами.

Висновки. На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Список використаних джерел

1. Соколов А. В. Защита от компьютерного терроризма. [Текст] / Соколов А. В., О. М. Степанюк. – БХВ-Петербург Арлит, 2002. – 496 с.
2. Конеев И. Р. Информационная безопасность предприятия [Текст] / И. Р. Конеев, А. В. Беляев. – БХВ-Петербург, 2003. – 752 с.

Наукове видання

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ І КІБЕРБЕЗПЕКА: ДОСЯГНЕННЯ ТА ІННОВАЦІЇ

Матеріали Всеукраїнської науково-практичної
конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27-29 листопада 2018 р.)

Технічний редактор *О. П. Дóренський*

Підписано до друку 29.11.2018. Формат 60x84/8. Папір офсетний.
Надруковано на ризографі. Тираж 245 прим.

© РВЛ ЦНТУ, м. Кропивницький, просп. Університетський, 8, 25006.
Тел. (0522) 559-245, www.kntu.kr.ua