**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**
**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

**ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**




# «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

**Тези доповідей**

**29 жовтня**
**2026**

**м. Київ**

**Редакційна колегія:**

Гайдур Г.І. – д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Зибін С.В. – д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Казмірчук С.В. - д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Гахов С.О. – к.військ.н., доцент, доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Марченко В.В. – д.ф., доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

*Рекомендовано до друку кафедрою Сиситем та технологій Державного університету інформаційно-комунікаційних технологійй (протокол № 4 від 02.11.2026 р.)*

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 29 жовтня 2026 року). Навчально-науковий інститут кібербезпеки та захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2026. 388 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з кібербезпеки та захисту інформації, працівників органів державної влади та місцевого самоврядування. Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції.

**ЗМІСТ**

Рибачок Геннадій Іванович
ВИБІР ПЛАНУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТ ЯК ЗАДАЧА ПОКРИТТЯ: ПОСТАНОВКА ДЛЯ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ ..... 14
Зінченко Олександра Ігорівна
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ФАКТОР ТРАНСФОРМАЦІЇ КІБЕРЗАГРОЗ ..... 16
Тишик І. Я.
ВИЯВЛЕННЯ КІБЕРЗАГРОЗ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОЇ КОРЕЛЯЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ..... 18
Лаптєв Олександр Анатолійович, Дунаев Сергій Владиславович
ПІДВИЩЕННЯ ПРИХОВАНОСТІ ТА ЗАХИЩЕНОСТІ ДАНИХ У СМАРТ-СЕРЕДОВИЩАХ МЕРЕЖ 6G НА ОСНОВІ ОПТИМІЗОВАНИХ LDPC-КОДІВ ТА ПОСТКВАНТОВОЇ КРИПТОСИСТЕМИ НІДЕРАЙТЕРА ..... 21
Гайдур Г.І. , Селіверстов М. В.
ТЕХНОЛОГІЯ ЗАХИСТУ ВІДДАЛЕНИХ КОРИСТУВАЧІВ НА ОСНОВІ КОНЦЕПЦІЇ ZTNA ..... 24
Гайдур Г.І., Проценко М.В.
ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ МОДЕЛЕЙ ДОСТУПУ НА ОСНОВІ КОНТЕКСТНОЇ АУТЕНТИФІКАЦІЇ ..... 26
Ляшенко Я.В.
УДОСКОНАЛЕННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ НА ОСНОВІ СТАНДАРТУ ISO/IEC 27001 ..... 29
Карапиш Б.О.
ТЕХНОЛОГІЯ АВТОМАТИЗАЦІЇ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-ЗАСТОСУНКІВ НА ОСНОВІ МУЛЬТИАГЕНТНИХ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ..... 31
Цебак О.А.
ПЕРСПЕКТИВИ ГІБРИДНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ..... 32
Романюк О.Н., Майданюк В.П., Романюк О.В.
ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНИХ МОДУЛІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ ..... 34
Романюк О.Н., Майданюк В.П., Нечипорук М.Л.
АПАРАТНЕ ПРИСКОРЕННЯ ШИФРУВАННЯ ЦИФРОВИХ ЗОБРАЖЕНЬ У ВБУДОВАНИХ СИСТЕМАХ ..... 37
Tsarova Sofiia Valeriivna
RANSOMWARE DETECTION WITH ENDPOINT DETECTION & RESPONSE PLATFORMS ..... 40
Степанченко Богдан Сергійович, Собчук Андрій Валентинович
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІКИ КІБЕРЗАГРОЗ НА ОСНОВІ СИСТЕМ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ З ІМПУЛЬСНОЮ ДІЄЮ ..... 42

Бражник Артем Михайлович
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ БАГАТОЕТАПНИХ КІБЕРАТАК У ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ АДАПТИВНОЇ КОРЕЛЯЦІЇ ПОДІЙ ..... 44
Магдєєв В.С., Мєшков В.І.
АНАЛІЗ ОЗНАК СОЦІОТЕХНІЧНИХ СЦЕНАРІЇВ СПОНУКАННЯ КОРИСТУВАЧА ДО ВИКОНАННЯ НЕБЕЗПЕЧНИХ ДІЙ У ВЕБСЕРЕДОВИЩІ ..... 47
Яненко О. В., Мєшков В.І.
ОСОБЛИВОСТІ ОЦІНЮВАННЯ КІБЕРРИЗИКІВ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ПІДПРИЄМСТВА НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ..... 50
Талан Анна Владиславівна
ПОРІВНЯЛЬНИЙ АНАЛІЗ РУЧНОГО ТА ЦЕНТРАЛІЗОВАНОГО КОНФІГУРУВАННЯ КОРПОРАТИВНИХ ПРИСТРОЇВ ..... 53
Єрмаков О.В., Мєшков В.І.
АНАЛІЗ УМОВ АДАПТИВНОГО КЕРУВАННЯ ДОСТУПОМ ДО ПЕРСОНАЛЬНИХ ДАНИХ У ВЕБЗАСТОСУНКАХ З УРАХУВАННЯМ ВИМОГ GDPR..... 55
Гайдур Г.І., Тонкошкур О.В.
ТЕХНОЛОГІЯ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ZERO TRUST У ХМАРНОМУ СЕРЕДОВИЩІ НА БАЗІ ІНТЕГРОВАНИХ СИСТЕМ IAM ТА КОНТЕКСТНОГО КОНТРОЛЮ ДОСТУПУ ..... 58
Гимза О.А., Кеньо Г.В.
ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ РОЗУМНОГО ПАРКУВАННЯ ..... 61
Козловський М. В., Мєшков В.І.
АНАЛІЗ УМОВ ЗАПОБІГАННЯ ВИТОКАМ ТРАФІКУ ПІД ЧАС УСТАНОВЛЕННЯ ТА ВІДНОВЛЕННЯ ЗАХИЩЕНИХ ТУНЕЛЬНИХ З’ЄДНАНЬ..... 63
Кутовий Денис Сергійович
ПРОФІЛЬ ЗАХИСТУ ДЛЯ ПРОГРАМ-АРХІВАТОРІВ ВІДПОВІДНО ДО ВИМОГ СТАНДАРТУ ISO/IEC 15408 ..... 66
Балацький Андрій Володимирович
ВПРОВАДЖЕННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА БАЗІ CISCO DUO FOR WINDOWS LOGON ..... 68
Коваленко Ю. Б.
МОДЕЛЬ ОЦІНЮВАННЯ ЗАТРИМОК І СВОЄЧАСНОСТІ ПЕРЕДАВАННЯ ДАНИХ У МЕРЕЖАХ AFDX ТА TSN..... 71
Хохлачова Ю. Є.
ПРОГНОЗУВАННЯ МІЖСЕКТОРНИХ КАСКАДІВ У ЦИФРОВОМУ ДВІЙНИКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ..... 74

Поремський Я.С.
ТЕХНОЛОГІЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОДІЙ КІБЕРБЕЗПЕКИ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ У ПРОЦЕСАХ THREAT HUNTING ..... 77
Прокопович-Ткаченко Д. І.
МІСІЙНО ОРІЄНТОВАНА МЕТРИКА КІБЕРСТІЙКОСТІ МЕРЕЖІ З УРАХУВАННЯМ НЕБЕЗПЕЧНОЇ ДЕГРАДАЦІЇ СЕРВІСІВ ..... 80
Чайківський В.В.
АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА УСУНЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КІНЦЕВИХ ПРИСТРОЇВ КОРПОРАТИВНОЇ МЕРЕЖІ ЗАСОБАМИ CHECK POINT ENDPOINT SECURITY ..... 83
Таран В. Д.
ОСОБЛИВОСТІ ПОБУДОВИ SECURITY OPERATIONS CENTER ДЛЯ ПІДПРИЄМСТВ ІЗ ТЕРИТОРІАЛЬНО РОЗПОДІЛЕНОЮ ІНФРАСТРУКТУРОЮ ..... 86
Лукінов Я.В., Нечитайло Ю.А.
ВИКОРИСТАННЯ СТОХАСТИЧНИХ МОДЕЛЕЙ ТА СТАТИСТИЧНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ Й ПРОТИДІЇ КІБЕРАТАКАМ У КІБЕРФІЗИЧНИХ СИСТЕМАХ ..... 89
Лаврук Анна Віталіївна
ЗАХИСТ АГЕНТІВ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ВІД НЕПРЯМОЇ ІН’ЄКЦІЇ ЗАПИТІВ У КОРПОРАТИВНИХ СИСТЕМАХ ..... 93
Сердобінцев І.А., Мєшков В.І.
АНАЛІЗ СПОСОБІВ КОМПРОМЕТАЦІЇ IoT-ПРИСТРОЇВ ТА МЕТОДІВ ПРОТИДІЇ БОТНЕТАМ ..... 96
Косяченко С.Р., Мєшков В.І.
АНАЛІЗ УМОВ КЕРУВАННЯ ЖИТТЄВИМ ЦИКЛОМ ДОСТУПУ ДО КОРПОРАТИВНИХ СЕКРЕТІВ В ІТ-КОМПАНІЇ ..... 99
Корж А.Ю.
ТЕХНОЛОГІЯ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ НА ОСНОВІ ПЛАТФОРМИ UAM SYTECA ..... 102
Дасюк Юрій Євгенійович
ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ IBM MAAS360 ..... 105
Севертока О.А.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ПОРУШЕННЯМ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ UAM TERAMIND ..... 108
Резніченко С.А.
ПРОБЛЕМИ ДОСТОВІРНОСТІ OSINT-АНАЛІЗУ ІЗ ЗАСТОСУВАННЯМ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ ТА ПІДХОДИ ДО ЇХ МІНІМІЗАЦІЇ ..... 111

Мохонько Діана
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. НОРМАТИВНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ ..... 113
Стебловський Г.В., Земляков С.О.
ВАЖЛИВІСТЬ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ ESET INSPECT & PROTECT ..... 116
Гуленов І.В.
ПІДВИЩЕННЯ БЕЗПЕКИ VPN ЗА ДОПОМОГОЮ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ..... 120
Завгородня Євгенія Ярославівна
КІБЕРСТІЙКІСТЬ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: УРОКИ АТАКИ INDUSTROYER2 ТА ПІДХІД НА ОСНОВІ NIST CSF 2.0 .. 123
Шимчук Г. В., Яцків П.О.,
КОНТЕКСТНА МОДЕЛЬ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ ..... 126
Шимчук Г. В., Яцків П.О.
АДАПТИВНИЙ ЗАХИСТ ІОТ-МЕРЕЖ НА ОСНОВІ ОЦІНКИ ДОВІРИ ПРИСТРОЇВ ТА ДИНАМІЧНОЇ МІКРОСЕГМЕНТАЦІЇ ..... 129
Онопрієнко М.Ю
МЕТОДИ І ТЕХНОЛОГІЇ КІБЕРАТАК, ОРГАНІЗОВАНИХ ЗА ПІДТРИМКИ НАЦІОНАЛЬНИХ ДЕРЖАВ ТА ЗАСОБИ ПРОТИДІЇ ЇМ ..... 132
Ланде Дмитро Володимирович, Кузьмінський Віктор Сергійович
ВИЛУЧЕННЯ ТРИПЛЕТІВ ПРО КІБЕРЗАГРОЗИ З ТЕКСТОВИХ ПОВІДОМЛЕНЬ ІЗ ГАРАНТОВАНОЮ МЕЖЕЮ ЧАСТКИ ПОМИЛОК ..... 135
Четвертуха Н.Р., Отенко В.І.
ВИБІР ІНСТРУМЕНТУ ДИНАМІЧНОГО АНАЛІЗУ ДЛЯ ШКІДЛИВИХ ПРОГРАМ, ЯКІ ПРИХОВУЮТЬ СВОЮ ПОВЕДІНКУ ..... 138
Опірський І.Р., Стефанків А.В.
МЕХАНІЗМИ ВІДБОРУ ОЗНАК СИГНАЛІВ У СИСТЕМАХ РАДІОЧАСТОТНОГО ФІНГЕРПРИНТИНГУ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ ..... 141
Афонін М.В.
АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНСТРУМЕНТІВ ВІДДАЛЕНОГО ДОСТУПУ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ..... 144
Гончаренко М.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ АТАК У ПРОМИСЛОВИХ МЕРЕЖАХ MODBUS TCP НА ОСНОВІ АЛГОРИТМУ XGBOOST ..... 147
Ступченко А.О
ПОБУДОВА ЦЕНТРУ ОПЕРАЦІЙНОЇ БЕЗПЕКИ (SOC) ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЇ ..... 150

Шапко Олег Олександрович
ПРОАКТИВНЕ ВИЯВЛЕННЯ ЗАГРОЗ НА КІНЦЕВИХ ТОЧКАХ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ ПОВЕДІНКОВИХ МОДЕЛЕЙ У СЕРЕДОВИЩІ WAZUH ..... 152
Харькевич Дмитро Олегович
АВТОМАТИЗОВАНИЙ КОНТРОЛЬ КОДУ В DEVSECOPS ІЗ ВИКОРИСТАННЯМ SONARQUBE QUALITY GATE ..... 156
Курінний О.С.
ОЦІНЮВАННЯ ТА ЗНИЖЕННЯ РИЗИКІВ ЛЮДСЬКОГО ФАКТОРА ПІД ЧАС ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ ..... 160
Литвинюк Владислав Вадимович
ТЕХНОЛОГІЯ СЕГМЕНТАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ ДЛЯ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ZERO TRUST НА ОБЛАДНАННІ CISCO ..... 163
Виноградов К.В.
ТЕХНОЛОГІЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В SENTINELONE ..... 165
Довгошея Д. О.
ТЕХНОЛОГІЯ МОНІТОРИНГУ СТАНУ ДЖЕРЕЛ ДАНИХ ТА СПОВІЩЕННЯ АДМІНІСТРАТОРА У SPLUNK ENTERPRISE SECURITY ..... 168
Чуєва С.О.
ЗАСТОСУВАННЯ ЛОКАЛЬНИХ МАЛИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ПОЯСНЮВАЛЬНОГО АНАЛІЗУ КІБЕРЗАГРОЗ В ІЗОЛЬОВАНИХ МЕРЕЖЕВИХ СЕРЕДОВИЩАХ ..... 170
Середін Андрій Валерійович
ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ KEYCLOAK ..... 172
Стожок М.Р.
ТЕХНОЛОГІЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТА РИЗИК-ОРІЄНТОВАНОЇ ПРІОРИТИЗАЦІЇ ВРАЗЛИВОСТЕЙ МЕРЕЖЕВИХ СЕРВІСІВ КОРПОРАТИВНОЇ МЕРЕЖІ ..... 175
Архипенко Дмитро Євгенович
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ ІЗ ЗАСТОСУВАННЯМ МАШИННОГО НАВЧАННЯ НА БАЗІ ZEEK ..... 177
Гавриленко Д.П.
МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОПТИМІЗАЦІЇ ПРОЦЕСІВ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ В СУЧАСНОМУ SOC ..... 179
Душник Володимир Володимирович
ТЕХНОЛОГІЯ ЗАСТОСУВАННЯ SPLUNK ДЛЯ МОНІТОРИНГУ ТА ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ У ДІЯЛЬНОСТІ SOC ..... 181

Фесенко Д.С.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТЕХНІК ОБХОДУ ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ MICROSOFT DEFENDER XDR ..... 183
Піскунов Костянтин Валерійович
ТЕХНОЛОГІЯ ЗАПОБІГАННЯ ФІШИНГОВИМ АТАКАМ, СПРЯМОВАНИМ НА ВИКРАДЕННЯ ОБЛІКОВИХ ДАНИХ КОРИСТУВАЧІВ ..... 186
Гриньов Тимофій Олександрович
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ РОЗПОДІЛЕНИХ МЕРЕЖЕВИХ АТАК У КОРПОРАТИВНІЙ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ CROWDSEC ..... 190
Шавшин Є.О
КОМПЛЕКСНИЙ ПІДХІД ДЛЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ..... 193
Твердохліб Я.М.
ЗАСТОСУВАННЯ СТАТИЧНОГО АНАЛІЗУ КОДУ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ВЕБ-ЗАСТОСУНКІВ ОРГАНІЗАЦІЇ ..... 197
Мурзін І. А., студент групи ІКБм-51
ВИЯВЛЕННЯ ПОВТОРНИХ АТАК І ДОВГОТРИВАЛОГО ДОСТУПУ ЗЛОВМИСНИКІВ ЗАСОБАМИ XDR ..... 200
Тамбієва В.Г.
ПРОГРАМНА СИСТЕМА КОМПЛЕКСНОГО ЗАХИСТУ БАЗ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ..... 203
Мазур Олександра
СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ПРОАКТИВНОГО АНАЛІЗУ ..... 207
Сокульський О. Є., Топольськов Є.О., Москаленко Н. В.
ГОМОМОРФНЕ ШИФРУВАННЯ ТА ХМАРНІ ТЕХНОЛОГІЇ ..... 211
Головненко Н.Р.
РОЗРОБЛЕННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ КІБЕРАТАК НА ОСНОВІ КОРЕЛЯЦІЇ ПОДІЙ SPLUNK ENTERPRISE SECURITY ТА ТЕЛЕМЕТРІЇ SENTINELONE ..... 213
Журавель Олександр Олегович
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ АТАК ТИПУ BRUTE FORCE ІЗ ЗАСТОСУВАННЯМ МЕТОДУ МАШИННОГО НАВЧАННЯ RANDOM FOREST ..... 217
Хорольський Костянтин Андрійович
ЗАСТОСУВАННЯ ГРАДІЄНТНОГО БУСТИНГУ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВИХ ДОКУМЕНТНИХ ВКЛАДЕНЬ ФІШИНГОВИХ ЕЛЕКТРОННИХ ЛИСТІВ ..... 220
Савченко В.В.
ТЕХНОЛОГІЯ ТЕСТУВАННЯ ЗАХИЩЕНОСТІ API ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ АВТЕНТИФІКАЦІЇ ..... 224

Караєв Владислав Русланович,
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБРОБКИ ДАНИХ У ВЕБ-СИСТЕМАХ АВТОМАТИЗОВАНОГО ПІДБОРУ КОМПЛЕКТУЮЧИХ ПК ..... 227
Габорець О. А., Хоменко О. М.
ДЕСТРУКТИВНИЙ ІНФОРМАЦІЙНИЙ ВПЛИВ НА ДИТИНУ В ЦИФРОВОМУ СЕРЕДОВИЩІ: ПОНЯТТЯ, ОЗНАКИ ТА СУЧАСНІ ФОРМИ ..... 231
Дубик Артур Русланович
АРХІТЕКТУРНА МОДЕЛЬ ЗАХИЩЕНОЇ ІНТЕГРАЦІЇ AI-АГЕНТІВ У КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ НА ЗАСАДАХ ZERO TRUST ..... 235
Михайленко Юлія Іванівна
ПІДХІД ДО ВИЯВЛЕННЯ DDOS SYN FLOOD-АТАК У МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АЛГОРИТМУ XGBOOST ..... 239
Хоменко Микита Сергійович
ТЕХНОЛОГІЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ НА БАЗІ ПРОТОКОЛУ SSL/TLS ..... 242
Власюк Ігор Дмитрович
КРИТЕРІЇ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЖУРНАЛІЗАЦІЇ КІБЕРІНЦИДЕНТІВ ..... 244
Яковенко Я.І.
ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST ІЗ ВИКОРИСТАННЯМ MICROSOFT ENTRA ID ТА MICROSOFT INTUNE ..... 248
Хідзик Я.Ю.
АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ ..... 250
Попелюк Софія
АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. АТАКИ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ..... 252
Науменко Д.М.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ ..... 255
Скидан Данило Романович, Щебланін Юрій Миколайович
ЗАХИСТ КОРПОРАТИВНИХ WI-FI МЕРЕЖ МЕТОДАМИ КОМБІНОВАНОГО ШИФРУВАННЯ ТА КОНТРОЛЮ СЕСІЙ ..... 257
Азіз АБІБУЛАЄВ, Андріан ПІСКОЗУБ
ХИБНОПОЗИТИВНІ СПРАЦЮВАННЯ ДЕТЕКТОРІВ ВЕБ-АТАК У РЕАЛЬНОМУ ТРАФІКУ ..... 261
Пашенько С. П.,
РЕКОНСТРУКЦІЯ КІБЕРІНЦИДЕНТІВ ШЛЯХОМ КОРЕЛЯЦІЇ ЦИФРОВИХ СЛІДІВ ..... 265

Levterov G.A., Levterov A. A.
ANALYSIS CYBER INCIDENT PREVENTION IN THE MOBILE SECTOR OF THE UKRAINIAN ENERGY AND DEFENSE COMPLEXES UNDER CONDITIONS POWER SUPPLY DEGRADATION ..... 267
Ахмедов А.Ф.
ФОРМУВАННЯ КРИТЕРІЇВ ДЕТЕРМІНОВАНОГО БІОМЕТРИЧНОГО ПРОТОКОЛУ В IoT-ІНФРАСТРУКТУРІ ..... 271
Мельник В.І.
ТЕХНОЛОГІЯ АВТОМАТИЗОВАНОГО РЕАГУВАННЯ НА ФІШИНГОВІ АТАКИ З ВИКОРИСТАННЯМ SOAR ..... 274
Кіх М. В.,
ВИКОРИСТАННЯ АУДІОЕНТРОПІЇ ДЛЯ ФОРМУВАННЯ ПОЧАТКОВОГО СТАНУ ГІБРИДНОГО ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ..... 276
Молнар Віталій Васильович
ПОРІВНЯННЯ СПОСОБІВ АВТОМАТИЗОВАНОГО РЕАГУВАННЯ НА НЕБЕЗПЕЧНІ ЗМІНИ КОНФІГУРАЦІЇ AWS ..... 279
Костенко Яків Олександрович
СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ МЕРЕЖАХ НА ОСНОВІ SYSTECA UAM ..... 283
Ялбуган Ф. Д.
ГІБРИДНЕ ОЦІНЮВАННЯ КІБЕРРИЗИКІВ ОРГАНІЗАЦІЙ-КОНТРАГЕНТІВ ЗА OSINT-ДАНИМИ З ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ..... 285
Алексанян Андрій Ельдарович
ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ МЕТОДАМИ МАШИННОГО НАВЧАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ СИСТЕМ ..... 289
Москаленко Н. В., Сокульський О. Є., Топольськов Є.О.
ШТУЧНИЙ ІНТЕЛЕКТ ЯК СКЛАДОВА ЯКОСТІ ПЗ ..... 291
Круть Ростислав Андрійович
ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ VPN ..... 292
Власенко Г. В.
КРИТЕРІЇ ФОРМУВАННЯ ОБМЕЖЕНОГО НАБОРУ СЦЕНАРІЇВ ВАЛІДАЦІЇ МЕХАНІЗМІВ КІБЕРЗАХИСТУ НА ОСНОВІ MITRE ATT&CK ..... 294
Коршиков О.В., Мужанова Т.М.
ЕВОЛЮЦІЯ ВИМОГ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ..... 297
Миловидов В. Ю.
ОЦІНЮВАННЯ ВНЕСКУ КОНТЕКСТНИХ ОЗНАК У НЕЙРОМЕРЕЖЕВЕ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБРЕСУРСІВ ..... 300

Нижник А.О.
МЕТОД ВИЯВЛЕННЯ АНОМАЛЬНИХ ПОСЛІДОВНОСТЕЙ КОМАНД MAVLINK У СИСТЕМАХ КЕРУВАННЯ БПЛА ..... 303
Чалий О.В., Толюпа С.В.
ГРАФ ЗНАНЬ ДЛЯ ВИЯВЛЕННЯ НЕВІДПОВІДНОСТЕЙ В АУДИТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ..... 307
Козяр Михайло Олександрович
ІНТЕГРАЦІЯ DEVSECOPS-ПРАКТИК У GITOPS-КОНВЕЄР ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ ..... 310
Колесникова А. Я.
ОЦІНЮВАННЯ КІБЕРЗАХИЩЕНОСТІ ХМАРНИХ СЕРЕДОВИЩ НА БАЗІ МАТЕМАТИЧНИХ МОДЕЛЕЙ ТА СТАНДАРТІВ ISO ..... 313
Алексанян Андрій Ельдарович
ІНТЕГРАЦІЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ В SOC ДЛЯ ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ ..... 316
Вострих Д.О.
ТЕХНОЛОГІЯ ЗАХИСТУ СУЧАСНИХ МЕРЕЖ НА ОСНОВІ PALO ALTO NGFW ..... 318
Куценко Олексій Сергійович
ЗАХИСТ IoT-ПРИСТРОЇВ ТЕЛЕМАТИЧНИХ СИСТЕМ НА ЕТАПАХ ВПРОВАДЖЕННЯ ТА ЕКСПЛУАТАЦІЇ ..... 320
Піскунов Костянтин Валерійович
ТЕХНОЛОГІЯ ЗАПОБІГАННЯ ФІШИНГОВИМ АТАКАМ, СПРЯМОВАНИМ НА ВИКРАДЕННЯ ОБЛІКОВИХ ДАНИХ КОРИСТУВАЧІВ ..... 323
Черненко Д. А.
ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ ДАНИХ НА БАЗІ MICROSOFT PURVIEW DLP ..... 327
Райченко В. С.
ІНТЕГРОВАНИЙ ПІДХІД ДО ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: МОНІТОРИНГ, УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ТА АВТОМАТИЗАЦІЯ РЕАГУВАННЯ ..... 330
Рядий Д.О.
КОНТЕКСТНИЙ АНАЛІЗ HTTP-ЗАПИТІВ У СИСТЕМІ ЗАХИСТУ ВЕБ-ДОДАТКІВ OPEN-APPSEC ..... 333
Шулімова Д.Д.
ЗАЛЕЖНІСТЬ ІНФОРМАТИВНОСТІ ОЗНАК МЕРЕЖЕВОГО ТРАФІКУ ВІД ТИПУ АТАК ..... 335
Medynskyi O. R., Susukailo V. A.
A DIGITAL IMAGE VERIFICATION METHODOLOGY FOR CYBER INCIDENT INVESTIGATION IN THE ERA OF GENERATIVE ARTIFICIAL INTELLIGENCE ..... 337
Сушанов Павло Вікторович
ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ФІШИНГОВИХ АТАК ..... 340

Тишик Іван Ярославович
ВИЯВЛЕННЯ КІБЕРЗАГРОЗ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНОЇ КОРЕЛЯЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ..... 343
Верголяс О. О.
КОГНІТИВНА БЕЗПЕКА КРИТИЧНИХ АУДИТОРІЙ В УМОВАХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ, ПІДСИЛЕНИХ ГЕНЕРАТИВНИМ ШТУЧНИМ ІНТЕЛЕКТОМ ..... 346
Svedeniuk O.V., Kurii Y. O.
APPLICATION OF AI MODELS FOR AUTOMATING IOT INFRASTRUCTURE COMPLIANCE WITH ETSI EN 303 645 AND IEC 62443 STANDARDS ..... 348
Ковалівська К. В.
ДОСЛІДЖЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ ТА ПОСИЛЕННЯ АГРЕСІЇ РФ ..... 350
Ровда Володимир Володимирович
ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ОПТИМІЗАЦІЇ КАНАЛЬНОГО ТА МЕРЕЖЕВОГО РІВНІВ У ВИСОКОНАВАНТАЖЕНИХ ЛОКАЛЬНИХ РАДІОМЕРЕЖАХ..... 354
Лукінов Я.В., Нечитайло Ю.А.
ВИКОРИСТАННЯ СТОХАСТИЧНИХ МОДЕЛЕЙ ТА СТАТИСТИЧНОГО АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ Й ПРОТИДІЇ КІБЕРАТАКАМ У КІБЕРФІЗИЧНИХ СИСТЕМАХ ..... 358
Нестор Наталія Володимирівна
ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ДЕРЖАВНИХ РЕЄСТРІВ УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ..... 362
Леляк А. В., Астраханцев А. А.
ЗАХИСТ КАНАЛІВ В СИСТЕМАХ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ ВДОСКОНАЛЕНОЇ БІБЛІОТЕКИ OPENSCP ..... 365
Нетребко Є.Г., Мєшков В.І.
АНАЛІЗ УМОВ ВИБОРУ ЗАСОБІВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ ..... 369
Литвиненко Роман Геннадійович, Буняк Анастасія Володимирівна, Рябець Віктор Вікторович
SIEM-СИСТЕМИ ЯК ІНСТРУМЕНТ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ ТА АНАЛІЗУ ІНФОРМАЦІЇ ..... 372
Буханець І.С.
ПІДХІД ДО ВИЯВЛЕННЯ АНОМАЛІЙ ТА ЗАГРОЗ НУЛЬОВОГО ДНЯ В IoT-МЕРЕЖАХ НА ОСНОВІ ОДНОКЛАСОВОГО МАШИННОГО НАВЧАННЯ375
Коровкін А.В.
ПІДХІД ДО ВИЯВЛЕННЯ КІБЕРАТАК НА IoT-ПЕРИФЕРІЮ НА ОСНОВІ МІНІМІЗАЦІЇ ОЗНАК СИСТЕМНОГО МОНІТОРИНГУ МЕТОДАМИ МАШИННОГО НАВЧАННЯ..... 379

Правдивий В.С.
ПІДХІД ДО ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ IoT НА ОСНОВІ МУЛЬТИМОДАЛЬНОГО АНАЛІЗУ ТЕЛЕМЕТРІЇ МЕТОДАМИ МАШИННОГО НАВЧАННЯ..... 383
Шевченко О.О.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ НИЗЬКОІНТЕНСИВНИХ ТА ПРИХОВАНИХ КІБЕРАТАК НА IoT-ПРИСТРОЇ НА ОСНОВІ СТАТИСТИЧНОГО ПРОФІЛЮВАННЯ ТА МЕТОДІВ МАШИННОГО НАВЧАННЯ..... 386

*Романюк О.Н. — завідувач кафедри програмного забезпечення*
*Майданюк В.П. — професор кафедри програмного забезпечення*
*Нечипорук М.Л. — аспірант*
*Вінницький національний технічний університет, Вінниця, Україна*

# АПАРАТНЕ ПРИСКОРЕННЯ ШИФРУВАННЯ ЦИФРОВИХ ЗОБРАЖЕНЬ У ВБУДОВАНИХ СИСТЕМАХ

Анотація. Розглянуто апаратне прискорення шифрування цифрових зображень у вбудованих системах на основі FPGA. Запропоновано архітектуру прискорювача AES-GCM, яка поєднує конвеєрне шифрування, обчислення тегу автентифікації та передавання даних засобами прямого доступу до пам'яті. Визначено порядок захисту піксельних даних і метаданих, вимоги до унікальності початкових значень та організації буферів. Наведено розрахунок необхідної пропускної здатності для зображень високої роздільності. Сформульовано критерії перевірки коректності, продуктивності, використання ресурсів і енергетичних витрат.

**Актуальність дослідження.** Вбудовані системи відеоспостереження, промислової діагностики та дистанційного контролю формують цифрові зображення, які можуть містити конфіденційну інформацію. Захист потрібний під час зберігання кадрів і передавання каналами зв'язку. Програмне шифрування конкурує за процесорні ресурси з обробкою зображень та керуванням пристроєм. Доцільність окремого прискорювача визначається можливостями процесора, зокрема наявністю криптографічних інструкцій, вимогами до затримки й допустимим енергоспоживанням. FPGA дає змогу реалізувати спеціалізований тракт обробки та узгодити його з потоком графічних даних.

Мета роботи - розроблення архітектури апаратного прискорювача шифрування цифрових зображень із контролем цілісності для вбудованої системи. Об'єктом дослідження є захист потоку зображень у системі з процесором і програмованою логікою. Предметом дослідження є організація криптографічних обчислень, передавання даних і буферизації за обмежених апаратних ресурсів.

Для базового варіанта пропонується AES-128, який обробляє блоки по 128 біт і використовує ключ довжиною 128 біт [1]. Режим GCM забезпечує автентифіковане шифрування з асоційованими даними [2]. Піксельні дані шифрують, а відкриті метадані включають до перевірки цілісності. Застосування стандартизованої конструкції дає змогу перевіряти реалізацію за еталонними результатами. Апаратна оптимізація має зберігати алгоритм і формат криптографічних результатів.

Запропонований тракт містить контролер передавання, вхідний FIFO, модуль формування блоків, генератор лічильників, ядро AES, модуль виключного АБО, модуль GHASH і вихідний FIFO. Процесор задає адреси буферів, довжину повідомлення та параметри операції через регістровий інтерфейс. Передавання основного масиву виконує контролер прямого доступу

до пам’яті DMA. Модуль AES шифрує значення лічильника; результат поєднують із відкритими даними операцією виключного АБО. GHASH обчислює складову тегу автентифікації. Керування потоком має підтримувати призупинення передавання без втрати або повторного використання блоків.

Для AES порівнюють ітераційну реалізацію з повторним використанням раундового модуля та конвеєрну реалізацію з розділенням раундів. Перша потребує менше ресурсів, друга допускає частіше надходження нових блоків. Огляд апаратних реалізацій AES розглядає компроміс між пропускною здатністю, площею та енергоспоживанням [3]. Вибір залежить від результатів синтезу й обмежень конкретної FPGA. Розклад ключа доцільно формувати під час його встановлення, щоб не повторювати цю операцію для кожного блока одного повідомлення.

Продуктивність тракту визначається також GHASH, у якому існує залежність між послідовними блоками. Саме збільшення швидкості AES не гарантує такого самого прискорення всього AES-GCM. Для потрібної пропускної здатності слід узгодити інтервал приймання блоків обох модулів або застосувати математично еквівалентну паралельну організацію GHASH. Під час синтезу враховують затримки між модулями, тактову частоту, місткість FIFO та можливі паузи на інтерфейсі пам’яті.

Кадр подають як послідовність байтів у визначеному порядку компонентів і рядків. У дескрипторі зазначають фактичну довжину даних і крок рядка, щоб розрізняти пікселі та службове вирівнювання. Прискорювач контролює межі буферів і коректність останнього неповного блока. Для збереження застосовують контейнер із шифротекстом, початковим значенням, тегом і метаданими. Шифротекст не є звичайним файлом зображення, придатним для безпосереднього відкриття графічним декодером.

До асоційованих даних пропонується включати ширину, висоту, формат пікселів, ідентифікатор потоку, номер кадру та довжину повідомлення. Їх кодують однозначно, з фіксованим порядком полів. У базовому варіанті один кадр відповідає одному автентифікованому повідомленню. Якщо кадр поділяють на незалежні фрагменти, кожен із них отримує власне початкове значення, а номер фрагмента й загальну структуру кадру пов’язують із тегом через метадані. Приймач додатково перевіряє порядок і повноту фрагментів.

Для GCM необхідно забезпечувати унікальність початкового значення в межах використання одного ключа [2]. У пропонованій реалізації передбачають 96-бітове початкове значення та 128-бітовий тег. Лічильник повідомлень не повинен повторюватися після перезапуску: його стан зберігають надійно або встановлюють новий ключ перед початком нової сесії. На приймальній стороні відкриті дані дозволяють використовувати лише після успішної перевірки тегу. Захист від повторного надсилання кадрів забезпечують окремим контролем номерів повідомлень.

Ключі й проміжні значення зберігають у регістрах з обмеженим доступом і очищують після завершення сесії або помилки. У робочому режимі обмежують налагоджувальний доступ до криптографічного модуля. Окремого дослідження

потребують витоки через енергоспоживання, електромагнітне випромінювання та навмисне внесення збоїв. Висока швидкість обробки й збіг результатів з еталоном самі по собі не доводять стійкості апаратної реалізації до таких впливів.

Нестиснений кадр RGB розміром 1920×1080 за 8 біт на компонент містить 6 220 800 байтів. Для 30 кадрів за секунду необхідна швидкість обробки становить 186 624 000 байтів/с, або приблизно 1,49 Гбіт/с, без урахування службових даних. Якщо DMA зчитує відкриті дані й записує шифротекст у ту саму підсистему пам’яті, лише ці операції потребують сумарно щонайменше 373 248 000 байтів/с. Навантаження від отримання кадру та подальшого передавання враховують додатково.

За тактової частоти 100 МГц і приймання одного 128-бітового блока за такт теоретична пропускна здатність ядра становить 12,8 Гбіт/с. Це верхня оцінка для такого інтервалу приймання, а не виміряний результат прискорювача. Фактичну швидкість зменшують затримки DMA, обмеження пам’яті, обчислення тегу й обробка меж повідомлень. Для перекриття передавання та шифрування пропонується подвійна буферизація: один буфер обробляється, поки інший заповнюється. Власність буферів контролює драйвер із дотриманням правил узгодженості кешу.

Коректність перевіряють зіставленням із незалежною програмною реалізацією AES-GCM для різних довжин даних і метаданих. Тести охоплюють неповний останній блок, пошкодження шифротексту, метаданих і тегу, зупинки потоку та помилки DMA. Вимірюють час повної операції, сталу швидкість, затримку кадру, зайнятість процесора, апаратні ресурси та енергію на кадр. Порівняння виконують із оптимізованим програмним варіантом на тому самому процесорі, зазначаючи використання криптографічних інструкцій. Експериментальні значення прискорення потребують реалізації та вимірювання прототипу.

Висновки**.** Запропоновано архітектуру FPGA-прискорювача AES-GCM для захисту цифрових зображень у вбудованих системах. Узгодження криптографічного тракту, DMA та буферів є необхідною умовою досягнення потрібної швидкості. Наведений розрахунок визначає вимоги для потоку кадрів високої роздільності. Подальша робота передбачає реалізацію прототипу, порівняння ітераційної та конвеєрної архітектур і перевірку безпеки обробки кадрів.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. National Institute of Standards and Technology. Advanced Encryption Standard (AES). FIPS 197-upd1. 2023. DOI: 10.6028/NIST.FIPS.197-upd1.

2. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. 2007. DOI: 10.6028/NIST.SP.800-38D.

3. Renugadevi N., Thangallapally S., Vemula S. C., Julakanti S., Bhatnagar S. Methods for improving the implementation of advanced encryption standard hardware accelerator on field programmable gate array—A survey. Security and Privacy. 2022. Vol. 5, No. 6. e254. DOI: 10.1002/spy2.254.