КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1265
УДК 004.056.57

Фесьоха Віталій Вікторович
доктор філософії, доцент, докторант
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID: 0000-0001-6612-1970
vitaliifesokha@gmail.com

Субач Ігор Юрійович
доктор технічних наук, професор, завідувач кафедри
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0000-0002-9344-713X
igor_subach@ukr.net

Степаненко Крістіна Євгенівна
ад'юнкт
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-0647-0623
kristinastep567@gmail.com

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ НА МОБІЛЬНИХ КІНЦЕВИХ ПРИСТРОЯХ У ВІДОМЧИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. У контексті актуального наукового завдання підвищення рівня кіберзахисту мобільних кінцевих пристроїв (МКП) у відомчих інформаційно-комунікаційних системах (ВІКС) проведено аналіз існуючих підходів до виявлення кіберінцидентів на МКП та показано, що переважна їх більшість орієнтована на виявлення окремих ознак компрометації пристрою без урахування його ролі у функціонуванні інформаційно-комунікаційної системи (ІКС). Аналіз підходів до виявлення шкідливої активності та методів їх реалізації проведено за рівнями прояву кіберінцидентів: мобільного застосунку, операційної системи та пристрою, поведінки користувача і контексту використання, мережевої взаємодії, доступу до сервісів ІКС та впливу на функціонування ІКС. Для кожного рівня визначено характерні прояви кіберінцидентів, джерела ознак, критерії оцінювання та найбільш придатні підходи до їх виявлення. Окремо проведено порівняння функціональних можливостей сучасних класів засобів виявлення кіберінцидентів на МКП. Встановлено, що жоден із розглянутих підходів і класів засобів окремо не забезпечує повного охоплення всіх рівнів прояву кіберінцидентів на МКП у ВІКС. Обґрунтовано доцільність розробки архітектури багаторівневого виявлення кіберінцидентів на МКП у ВІКС, яка забезпечує формування структурованого опису поточного стану МКП у контексті його взаємодії з ІКС шляхом двостороннього обміну даними між МКП та ІКС щодо стану рівнів прояву кіберінциденту, аналізу структури сеансів взаємодії спеціалізованого клієнтського ПЗ з ВІКС, визначення інваріантів розвитку технік кібератак у таксономіях мобільних загроз, а також обміну досвідом виявлення між МКП через ІКС.

Ключові слова: кіберінцидент; мобільні кінцеві пристрої; інформаційно-комунікаційні системи; спеціалізоване програмне забезпечення; кіберзахист.

ВСТУП

На сьогодні МКП є важливим і водночас масовим компонентом сучасних ІКС, оскільки дають змогу кінцевим користувачам отримувати доступ до інформаційних ресурсів, користуватися сервісами та взаємодіяти з окремими функціями ІКС незалежно від місця перебування. Смартфони, планшети, портативні термінали та інші мобільні пристрої активно використовуються для отримання, відображення

(представлення) та передачі інформації, тоді як їх компрометація може призвести не лише до негативних наслідків для окремого користувача, а й створити передумови для порушення функціонування ІКС загалом. У зв'язку з цим, завдання виявлення кіберінцидентів на МКП є важливою складовою забезпечення кібербезпеки ІКС.

Постановка проблеми. Особливої актуальності зазначена проблематика набуває у випадках використання МКП для спеціалізованих функцій, зокрема шляхом застосування спеціалізованого програмного забезпечення (ПЗ) для взаємодії з ВІКС, які на відміну від загальнодоступних систем характеризуються підвищеними вимогами до кіберзахисту, надійності, живучості, гарантоздатності та безперервності функціонування. У таких умовах зростає значущість будь якого типового МКП, як наслідку характеру виконання завдань його засобами, що у свою чергу підвищує вимоги до точного і своєчасного виявлення кіберінцидентів на МКП у ВІКС. Крім того, приклади спроб шкідливого впливу, що набули широкого розголосу протягом останнього часу [1] підтверджують зростання інтенсивності кібератак, спрямованих саме на МКП у ВІКС. Так, зафіксовано численні випадки використання шкідливого ПЗ, замаскованого під легітимні військові застосунки [1], зокрема, у 2023 році було виявлено кампанію, в рамках якої відкритий код шпигунського ПЗ Spynote (SpyMax) для операційної системи Android було модифіковано та замасковано під інсталятор системи “Кропива”. Розповсюдження шкідливої програми здійснювалося поза межами офіційних платформ цифрової дистрибуції, переважно через відомі месенджери, зокрема Signal та Telegram, із використанням методів соціальної інженерії (інструменти віддаленого доступу та експлуатації відомих вразливостей ПЗ було замасковано під виглядом PDF-документів або архівів (ZIP, RAR)) [1].

Аналогічні інциденти були зафіксовані у 2024 році, коли здійснювалося розповсюдження шкідливих мобільних застосунків, що імітували роботу спеціалізованих систем, таких як Griselda (автоматизована система внесення, обробки та передачі інформації з використанням технологій штучного інтелекту) та система моніторингу “Очі”. Так, користувачам пропонувалося встановити APK-файли через підроблені веб ресурси або хмарні сервіси [2]. У випадку з Griselda розповсюджувалося шкідливе ПЗ типу mobile implant – Hydra, яке реалізовувало функції прихованої ексфільтрації інформації (перехоплення введених даних, викрадення облікових даних, доступ до контактної інформації, визначення та передачу GPS-координат пристрою) [2]. Однією з ключових можливостей такого ПЗ є викрадення даних сесій (HTTP Cookie), що дає змогу зловмиснику отримати доступ до ІКС без автентифікації шляхом використання вже активної сесії користувача. У випадку із застосунком “Очі” використовувалася модифікована версія легітимного ПЗ, до якої було додано сторонній програмний код, який забезпечував викрадення логіна і пароля користувача, а також передачу геолокаційних даних [2].

Наведені приклади демонструють, що сучасні способи реалізації кіберзагроз характеризуються активним використанням соціальної інженерії, маскуванням під легітимні або спеціальні застосунки, використанням модифікованого ПЗ, орієнтацією на викрадення сесійних даних, як ефективного механізму обходу автентифікації та прихованим характером функціонування шкідливого коду. Зазначене обумовлює доцільність подальших наукових досліджень щодо підвищення ефективності виявлення кіберінцидентів на МКП у ВІКС.

Аналіз останніх досліджень і публікацій [3-18] свідчить про значне зростання уваги наукової спільноти останнім часом щодо проблематики кіберзахисту МКП, що зумовлено стрімким поширенням мобільних технологій, розширенням їх функціональних можливостей та інтеграцією до сучасних ІКС. Узагальнення результатів проведеного аналізу дає змогу виділити такі основні групи оглядових робіт:

1. Порівняння методів виявлення шкідливого ПЗ на МКП [3-7], [14]. У роботах цієї групи основну увагу зосереджено на систематизації методів виявлення шкідливого ПЗ на мобільних пристроях, переважно в середовищі Android. Автори аналізують статичні, динамічні та гібридні підходи, методи машинного й глибокого навчання, типи ознак мобільних застосунків, використані набори даних і метрики ефективності виявлення. Разом з тим, зазначені роботи розглядають МКП як автономне середовище виконання застосунків, а кіберінцидент фактично зводиться до факту наявності шкідливого ПЗ. Тому поза основним фокусом залишаються функціонування в специфічних умовах, роль МКП як елемента ІКС, вплив компрометації пристрою на функціонування системи та інциденти, пов’язані не лише зі шкідливим ПЗ, а й із викраденням облікових, сесійних чи геолокаційних даних.

2. Огляд методів виявлення аномалій на МКП [3, 4, 10, 13, 15-17]. Даний напрям досліджень пов’язаний із аналізом підходів, у яких ознакою потенційного кіберінциденту вважається відхилення від типової поведінки мобільного пристрою, застосунку або користувача. У межах цього напряму розглядаються поведінкові моделі, побудовані на основі системних викликів, мережевої активності, часових шаблонів, ланцюгів Маркова, даних сенсорів смартфона та методів машинного навчання. Перевагою таких робіт є орієнтація на виявлення нових, модифікованих або прихованих проявів шкідливої активності, які не завжди можуть бути виявлені класичними методами розпізнавання.

Водночас їх обмеження полягає в тому, що аномалія здебільшого трактується як технічне відхилення у функціонуванні МКП, без достатнього врахування її зв'язку з кіберінцидентом, впливом на сервіси ІКС, доступність інформаційних ресурсів, цілісність даних або виконання критичних завдань.

3. Аналіз методів інспекції мережевого трафіка, мережевих взаємодій та комунікаційних шаблонів [3, 4, 10, 13, 17]. Окремий напрям становлять праці, у яких виявлення кіберзагроз на МКП пов'язується з аналізом мережевої активності пристрою, характеру його взаємодії з віддаленими ресурсами та відхилень у комунікаційних шаблонах. Так, розглядаються підходи до виявлення підозрілих з'єднань, нетипової інтенсивності передачі даних, звернень до шкідливих доменів або серверів керування, а також ознак прихованої ексфільтрації інформації. Перевагою цього напряму є можливість фіксації шкідливої активності навіть тоді, коли саме ПЗ замасковане під легітимний застосунок або має обмежені локальні прояви на пристрої. Обмеженням відповідних робіт є те, що мережеві ознаки здебільшого аналізуються як технічні індикатори компрометації, без достатнього врахування змісту взаємодії МКП із сервісами ІКС, наслідків порушення комунікації та впливу інцидентів на функціонування системи загалом.

4. Застосування методів машинного навчання та штучного інтелекту [3, 6, 8, 9, 12, 17]. Значна частина сучасних оглядових робіт присвячена використанню методів машинного навчання, глибокого навчання та штучного інтелекту для виявлення шкідливого ПЗ і кібератак на МКП. У межах цього напряму аналізуються підходи, що ґрунтуються на автоматичному виділенні ознак із застосунків, поведінки пристрою, мережевої активності, системних викликів, дозволів, журналів подій і сенсорних даних, а також порівнюються алгоритми класифікації, нейронні мережі, ансамблеві моделі та глибокі архітектури. Перевагою таких робіт є узагальнення можливостей зазначених методів для підвищення точності виявлення відомих і нових кіберінцидентів, зокрема в умовах великої кількості мобільних застосунків та різнорідних даних. Обмеженням даних оглядів є переважна орієнтація на якість класифікації та експериментальні метрики, тоді як питання інтерпретованості рішень, стійкості моделей до зміни поведінки кібератак, придатності до роботи в умовах обмежених ресурсів МКП розглядаються недостатньо.

5. Комплексних підходів, в яких кіберзахист МКП розглядається як поєднання сигнатурних, локальних, мережевих, поведінкових способів виявлення кіберінцидентів [3-5, 7, 10, 11, 14, 15, 18]. Дану групу становлять роботи, у яких кіберзахист МКП розглядається як інтеграція кількох способів виявлення кіберінцидентів, оскільки зазначається, що жоден з окремих способів не забезпечує ефективного виявлення кіберінцидентів, особливо в умовах застосування поліморфного та метаморфного ПЗ і використання прихованих каналів передачі даних. Автори аналізують комбіновані схеми, у яких статичні ознаки доповнюються динамічними, локальні індикатори - мережевими, а сигнатурні методи поведінковими та/або інтелектуальними методами. Поряд з цим, обмеженням таких робіт є те, що комплексність здебільшого розуміється як поєднання технічних способів виявлення на рівні пристрою або застосунку, тоді як недостатньо враховується системний контекст: роль МКП у складі ІКС та необхідність оцінки ризиків для функціонування системи загалом.

На основі викладеного можна зробити висновок, що існуючі дослідження хоч і забезпечують ґрунтовну систематизацію методів виявлення шкідливого ПЗ, аномальної поведінки, статичного та динамічного аналізу, ознак компрометації для кіберзахисту МКП, все ж демонструють досить вузький підхід до врахування специфіки функціонування МКП як елемента ІКС, що актуалізує завдання подальшого аналізу існуючих підходів до виявлення кіберінцидентів з позиції їх спроможності до виявлення кіберінцидентів на МКП у ВІКС.

Метою статті є проведення порівняльного аналізу сучасних підходів до виявлення кіберінцидентів на МКП у ВІКС.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Особливістю виявлення кіберінцидентів на МКП у ВІКС є те, що сам мобільний пристрій не становить цінності окремо від тих функцій, які він забезпечує у складі ІКС. У даному випадку МКП використовується як засіб роботи зі спеціалізованим застосунком, автентифікації користувача, доступу до сервісів, передачі даних і виконання окремих службових функцій. Відтак, кіберінцидент на МКП не завжди може бути коректно описаний лише як наявність шкідливого ПЗ або аномальна активність пристрою, оскільки його прояви можуть охоплювати підміну чи модифікацію спеціалізованого застосунку, несанкціоноване використання дозволів, приховану активність у середовищі операційної системи (ОС), зміну поведінки користувача, передачу даних поза дозволеними каналами, використання сесійних або облікових даних для доступу до сервісів ІКС, а також подальший вплив на функціонування системи.

У зв'язку з цим, подальший аналіз існуючих підходів до виявлення кіберінцидентів на МКП доцільно проводити за рівнями, на яких можуть проявлятися ознаки кіберінцидентів, що дає змогу не обмежуватися загальноприйнятою класифікацією на статичні, динамічні, поведінкові, мережеві, а визначити, яку саме частину кіберінциденту вони здатні фіксувати (джерело ознак та які саме події може бути зафіксовано). З урахуванням зазначеного доцільно виділити такі рівні прояву кіберінцидентів на МКП у ВІКС (рисунок 1): рівень мобільного застосунку; рівень ОС та пристрою; рівень поведінки користувача і контексту використання; рівень мережевої взаємодії; рівень доступу до сервісів ІКС; рівень впливу на функціонування ІКС.

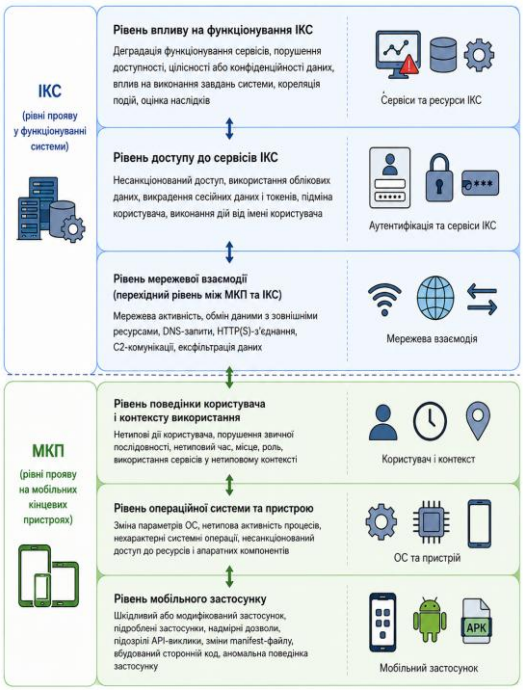

Рис. 1. Рівні прояву кіберінцидентів на МКП у ВІКС

Рівень мобільного застосунку [3-9, 11, 12]. На рівні мобільного застосунку кіберінцидент проявляється через наявність шкідливого або модифікованого виконуваного файлу застосунку, використання підроблених застосунків, надмірних дозволів, підозрілих API-викликів, змін manifest-файлу, вбудованого стороннього коду або аномальної поведінки ПЗ під час функціонування. У зв'язку з цим, існуючі підходи до виявлення кіберінцидентів на МКП доцільно аналізувати за їх здатністю виявляти відповідні прояви компрометації мобільного застосунку. Результати порівняння підходів до виявлення кіберінцидентів на рівні мобільного застосунку наведено в таблиці 1.

Таблиця 1

Результати порівняння підходів до виявлення кіберінцидентів на рівні мобільного застосунку

Критерії порівняння / Підходи	Тип аналізу застосунку	Джерело ознак	Здатність до виявлення модифікованих застосунків	Стійкість до обфускації	Необхідність виконання застосунку	Інтерпретованість	Придатність до використання на МКП	Обчислювальна складність	Верифікованість
Сигнатурні методи	Статичний	Сигнатури коду, API-виклики, manifest, дозволи застосунку	Низька	Низька	Ні	Висока	Висока	Низька	Висока

Продовження таблиці 1

Методи на основі машинного та глибокого навчання	Статичний / динамічний/ гібридний	APK-структура, API, поведінкові та мережеві ознаки	Середня/ Висока	Середня	Частково/Так	Низька	Обмежена	Висока	Низька
Поведінковий аналіз	Динамічний	Поведінка застосунку під час виконання, системні виклики	Висока	Висока	Так	Середня	Обмежена	Середня	Середня
Механізми контролю доступу	Статичний	Дозволи застосунку, політики доступу	Низька	Низька	Ні	Висока	Висока	Низька	Висока
Декларативний підхід	Статичний	Правила, попередньо визначені індикатори	Низька	Низька	Ні	Висока	Висока	Низька	Висока

На даному рівні виявлення кіберінцидентів орієнтовано на встановлення факту наявності на МКП шкідливого ПЗ, яке може використовуватися як початковий засіб компрометації мобільного пристрою. Як джерела ознак використовуються дозволи застосунку, API-виклики, manifest-файли, системні бібліотеки, структура виконуваних файлів, поведінкові характеристики застосунків, системні журнали подій та правила безпеки. Значна частина існуючих підходів [3-9], [11], [12] забезпечує ефективне виявлення відомого шкідливого ПЗ та окремих модифікованих застосунків, однак їх ефективність суттєво знижується в умовах використання механізмів обфускації коду або прихованої шкідливої активності.

Як видно з таблиці 1, сигнатурні методи характеризуються відносно низькою обчислювальною складністю, високою швидкістю аналізу та придатністю до використання безпосередньо на МКП, однак мають обмежену стійкість до механізмів обфускації та не забезпечують у повній мірі аналіз поведінки застосунку під час виконання.

Методи на основі машинного, глибокого навчання та поведінковий аналіз забезпечують більш високий рівень виявлення прихованої або модифікованої зловмисної активності, проте потребують значних обчислювальних ресурсів, мають обмежену інтерпретованість результатів та часто вимагають виконання застосунку. У свою чергу механізми контролю доступу та декларативний підхід орієнтовані переважно на аналіз дозволів застосунку, політик безпеки та визначених правил функціонування застосунків, однак їх ефективність суттєво залежить від повноти правил і не забезпечує якісного виявлення нових або прихованих кібератак.

Особливістю виявлення кіберінцидентів на даному рівні є можливість раннього виявлення потенційного джерела компрометації ще до активної взаємодії застосунку з ІКС або на початкових етапах його функціонування на МКП, але без повного розуміння кіберінциденту як події (ланцюга подій) в системі. Так, досить рідко можливо визначити чи було здійснено викрадення сесійних даних, чи відбувся несанкціонований доступ до сервісів ІКС або які саме дані було скомпрометовано.

Рівень ОС та пристрою [7, 8, 10, 12-17]. На рівні ОС та пристрою кіберінцидент, як правило, проявляється через зміну параметрів функціонування МКП, нетипову активність процесів, виконання нехарактерних системних операцій, зміну режимів використання ресурсів пристрою, а також несанкціонований доступ до інформаційних ресурсів і апаратних компонентів. Результати порівняння підходів до виявлення кіберінцидентів на рівні ОС та пристрою наведено в таблиці 2.

Таблиця 2

Результати порівняння підходів до виявлення кіберінцидентів на рівні ОС та пристрою

Критерії порівняння / Підходи	Тип події	Глибина моніторингу	Здатність виявляти приховану активність	Вплив на ресурси МКП	Робота в реальному часі	Залежність від прав доступу	Верифіко-ваність	Обчислювальна складність
Поведін-ковий аналіз	Процеси, системні події, системні виклики, фонова активність	Висока	Висока	Середній	Так	Висока	Середня	Середня
Методи на основі машинного та глибокого навчання	Процеси, системні події, показники використання ресурсів, журнали активності	Висока	Висока	Високий	Так	Висока	Низька	Висока
Механізми контролю доступу	Події доступу до файлів, контактів, геолокації, камери, мікрофона та інших ресурсів	Середня	Низька	Низький	Так	Висока	Висока	Низька
Деклара-тивний підхід	Порушення визначених правил та політик безпеки	Середня	Низька	Низький	Так	Середня	Висока	Низька
Апаратний захист	Критичні системні та апаратні події, доступ до захищених середовищ виконання	Висока	Середня	Низький	Так	Низька	Висока	Низька

На даному рівні виявлення кіберінцидентів орієнтовано на фіксацію відхилень у функціонуванні ОС та апаратних компонентів МКП, які можуть свідчити про приховану діяльність ШПЗ або несанкціоноване використання ресурсів пристрою. Як джерела ознак використовуються системні події, процеси, журнали активності, показники використання ресурсів, інформація про доступ до захищених даних і апаратних компонентів, а також результати моніторингу взаємодії застосунків із системним середовищем.

Поведінковий аналіз, підходи на основі машинного та глибокого навчання забезпечують найбільшу глибину моніторингу та дають змогу виявляти приховану активність навіть за відсутності відомих сигнатур або правил. Разом із цим, їх застосування пов’язане зі значним навантаженням на ресурси МКП, необхідністю накопичення великих обсягів даних та складністю верифікації результатів. Механізми контролю доступу та декларативний підхід дають змогу виявляти відхилення від визначених політик безпеки та несанкціоновані спроби доступу до ресурсів пристрою, проте їх результативність залежить від коректності налаштування політик, повноти правил контролю та доступності системних даних для аналізу. У свою чергу апаратний захист забезпечує додатковий контроль окремих критичних операцій та доступу до захищених середовищ виконання, проте його функціональні можливості обмежуються архітектурними особливостями конкретного пристрою.

Особливістю виявлення кіберінцидентів на даному рівні є можливість фіксації прихованої

активності незалежно від способу її реалізації та незалежно від конкретного застосунку, який її ініціює. Однак, варто зазначити, що компрометація застосунку може бути здійснена через вразливість ОС, де прихована ексфільтрація даних може не викликати підозри. До того ж, навіть за наявності інформації про аномальну системну активність часто складно встановити кінцеву мету зловмисника, факт компрометації сервісів ІКС або характер інформації, яка була отримана чи передана в результаті кібератаки, що обумовлює необхідність подальшого аналізу мережевих взаємодій та використання сервісів ІКС для повного встановлення змісту кіберінциденту.

Рівень поведінки користувача та контексту використання [6, 8, 12, 13, 15-17]. Даний рівень характеризується тим, що джерелом інформації для виявлення кіберінцидентів виступають закономірності взаємодії користувача з МКП. При цьому потенційними індикаторами кіберінциденту можуть бути нетиповий час активності виконання нехарактерних операцій, порушення типової послідовності дій або використання сервісів ІКС у нетиповому контексті. Результати порівняння підходів до виявлення кіберінцидентів на рівні поведінки користувача та контексту використання наведено в таблиці 3.

Таблиця 3

Результати порівняння підходів до виявлення кіберінцидентів на рівні поведінки користувача та контексту використання

Критерії порівняння / Підходи	Тип контекстних ознак	Здатність виявляти нетипову поведінку	Врахування службового сценарію	Персоналізація моделі	Стійкість до зміни поведінки
Поведінковий аналіз	Час активності, послідовність дій, сценарії використання, поведінкові шаблони	Висока	Середня	Висока	Середня
Методи на основі машинного та глибокого навчання	Час, місце, тип дії, роль користувача, сценарії використання, багатовимірні поведінкові ознаки	Висока	Висока	Висока	Висока
Декларативний підхід	Наперед визначені правила, часові та рольові обмеження, дозволені сценарії роботи	Низька	Висока	Низька	Низька

На відміну від попередніх рівнів прояву кіберінцидентів, де основна увага приділяється технічним ознакам компрометації, на цьому рівні основне значення мають контекстні ознаки, зокрема час виконання дій, місце використання пристрою, тип операції, роль користувача та сценарій використання МКП, оскільки сукупність саме таких ознак дає змогу формувати профілі типової поведінки та виявляти відхилення від них.

Проведений аналіз показує, що на даному рівні найбільш поширеними підходами є поведінковий аналіз і підходи на основі машинного і глибокого навчання, які забезпечують можливість виявлення нетипових дій користувача навіть за відсутності відомих ознак компрометації та здатні враховувати значну кількість взаємопов’язаних параметрів. Крім того, зазначені підходи підтримують персоналізацію моделей, що дає змогу адаптувати процес виявлення до особливостей конкретного користувача або категорії користувачів. Але їх ефективність значною мірою залежить від наявності репрезентативних даних для формування поведінкових профілів та зберігає чутливість до природних змін поведінки користувача, які можуть виникати під впливом різноманітних факторів. Окреме місце посідає декларативний підхід, у межах якого оцінка дій користувача здійснюється на основі наперед визначених правил, політик та сценаріїв використання, що забезпечує високу інтерпретованість результатів та можливість їх подальшої перевірки, однак має обмежені можливості щодо виявлення нових або раніше неописаних моделей поведінки.

Особливістю даного рівня є перехід від аналізу окремих технічних подій до оцінювання відповідності дій користувача типовому сценарію роботи зі спеціалізованим застосунком, що є важливим у ВІКС, оскільки доступ до геолокації, службових даних, повідомлень або мережевих ресурсів може бути штатною функцією спеціалізованого ПЗ, але набувати ознак кіберінциденту у разі зміни контексту: нетипового часу, місця, послідовності дій, ролі користувача або характеру звернення до сервісів ІКС.

Рівень мережевої взаємодії [4, 5, 10, 12, 13, 17]. Незалежно від способу реалізації кібератак, їх виконання у більшості випадків супроводжується мережевою активністю, пов'язаною з обміном даними між МКП та зовнішніми інформаційними ресурсами, яка може проявлятися у вигляді DNS-запитів, HTTP(S)-з'єднань, обміну даними із серверами керування, передачі службової інформації, викрадення облікових або сесійних даних, а також прихованої ексфільтрації інформації. Внаслідок цього мережеві події розглядаються як один із найбільш інформативних проявів кіберінцидентів, оскільки достатньо повно відображають не лише факт компрометації пристрою, а й вектор шкідливого впливу. Результати порівняння підходів до виявлення кіберінцидентів на рівні мережевої взаємодії наведено в таблиці 4.

Таблиця 4

Результати порівняння підходів до виявлення кіберінцидентів на рівні мережевої взаємодії

Критерії порівняння / Підходи	Тип мережевих ознак	Здатність виявляти ексфільтрацію	Здатність виявляти C2-комунікації	Робота з шифрованим трафіком	Контекст взаємодії з ІКС	Верифікованість	Обчислювальна складність
Захист мережевих з'єднань	DNS-запити, HTTP(S)-сесії, мережеві потоки, IP-адреси, доменні імена, мережеві з'єднання	Висока	Висока	Середня	Середня	Середня	Середня
Поведінковий аналіз	Шаблони мережевої активності, частота та послідовність з'єднань, аномалії трафіка	Середня	Висока	Середня	Висока	Середня	Середня
Підходи на основі машинного та глибокого навчання	Статистичні характеристики трафіка, часові параметри, поведінкові та мережеві ознаки	Висока	Висока	Висока	Висока	Низька	Висока

На відміну від рівнів мобільного застосунку та ОС, де аналізуються переважно локальні ознаки компрометації, мережевий рівень забезпечує спостереження за зовнішніми проявами діяльності МКП. Джерелами ознак виступають характеристики мережевого трафіка, параметри DNS-запитів, HTTP(S)-сесій, особливості встановлення мережевих з'єднань, часові характеристики передавання даних, мережеві потоки та індикатори взаємодії із зовнішніми ресурсами.

Проведений аналіз показує, що центральне місце на даному рівні займає підхід до захисту мережевих з'єднань, який реалізується через аналіз мережевого трафіка, системи виявлення та запобігання вторгненням, засоби аналізу мережевої поведінки та моніторинг взаємодії з віддаленими ресурсами. Зазначений підхід забезпечує ефективне виявлення підозрілих комунікацій, ознак ексфільтрації даних та взаємодії з серверами керування, проте його можливості суттєво ускладнюються в умовах використання зашифрованого трафіка або легітимних сервісів для приховування каналів зв'язку.

Для підвищення ефективності виявлення мережевих кібератак активно використовуються також поведінковий аналіз та підходи на основі машинного та глибокого навчання, які забезпечують виявлення аномалій у мережевій активності, нетипових шаблонів взаємодії та прихованих каналів передавання інформації. Проте, їх застосування супроводжується підвищенням обчислювальної складності та залежністю від якості вихідних даних, що особливо актуально для мобільних мереж зі змінними параметрами зв'язку.

Ключовою перевагою даного рівня є можливість безпосереднього спостереження за реалізацією кіберінциденту, зокрема передаванням даних за межі пристрою, взаємодією із зовнішніми вузлами та використанням віддалених сервісів. Разом з тим навіть за наявності детальної інформації про мережеві

з'єднання не завжди можливо однозначно визначити джерело формування мережевої активності, конкретний застосунок або процес, що її ініціював, а також реальний вплив таких дій на функціонування ІКС. Саме тому результати мережевого аналізу потребують кореляції з даними інших рівнів прояву кіберінциденту.

Рівень доступу до сервісів ІКС [10, 12, 13, 16, 17]. Характерна особливість даного рівня полягає в тому, що об'єктом аналізу є не сам МКП, а характер використання його облікових даних і цифрових ідентифікаторів під час доступу до ресурсів ІКС, що потенційно надає можливість встановлення зв'язку між кіберінцидентом та конкретним сервісом ІКС, до якого здійснюється доступ. Саме на цьому рівні можуть бути виявлені ознаки викрадення сесійних даних, повторного використання токенів доступу, компрометації облікових записів, підміни користувача або виконання дій від його імені без фактичної участі власника МКП. Основними джерелами інформації виступають журнали автентифікації, дані про активні сесії, токени доступу, журнали звернень до сервісів та результати виконання операцій у межах ІКС. Результати порівняння підходів до виявлення кіберінцидентів на рівні доступу до сервісів ІКС наведено в таблиці 5.

Результати проведеного аналізу свідчать, що найбільш придатними методами для вирішення таких завдань є поведінковий аналіз, підходи на основі машинного та глибокого навчання, а також декларативний підхід. При цьому поведінковий аналіз забезпечує можливість виявлення відхилень від типових моделей використання сервісів, машинне навчання дає змогу виявляти складні закономірності доступу та приховані ознаки компрометації облікових записів, а декларативний підхід – контроль дотримання визначених політик доступу та правил автентифікації.

Таблиця 5

Результати порівняння підходів до виявлення кіберінцидентів на рівні доступу до ІКС

Критерії порівняння / Підходи	Тип ознак доступу	Виявлення викрадення сесії	Виявлення несанкціонованого доступу	Зв'язок із конкретним сервісом ІКС	Аналіз контексту доступу	Тип ознак доступу	Виявлення викрадення сесії
Поведінковий аналіз	Журнали автентифікації, історія сесій, послідовність дій користувача, шаблони використання сервісів	Середня	Висока	Висока	Висока	Середня	Середня
Підходи на основі машинного та глибокого навчання	Події входу, характеристики сесій, токени доступу, поведінкові та статистичні ознаки використання сервісів	Висока	Висока	Висока	Висока	Низька	Висока
Декларативний підхід	Правила автентифікації, політики доступу, рольові моделі, журнали порушення політик	Низька	Середня	Висока	Середня	Висока	Низька

Рівень впливу на функціонування ІКС [10, 12, 13, 16, 17] доцільно розглядати як завершальний рівень аналізу, на якому ознаки кіберінциденту оцінюються не з позиції факту компрометації МКП, а можливих наслідків для роботи ВІКС, де ключовим є встановлення того, чи призвели події на МКП до порушення доступу до сервісів ІКС, зміни або витоку інформації з обмеженим доступом, зниження доступності окремих функцій, порушення цілісності інформації або втрати довіри до результатів роботи спеціалізованого ПЗ. Так, наприклад, викрадення сесійних даних є не лише фактом компрометації МКП, а й передумовою загрози для самої ІКС. Результати порівняння підходів до виявлення кіберінцидентів на рівні впливу на функціонування ІКС наведено в таблиці 6.

Таблиця 6

Результати порівняння підходів до виявлення кіберінцидентів на рівні впливу на функціонування ІКС

Підходи \ Критерії порівняння	Зв'язок події з функціями ІКС	Оцінка критичності інциденту	Оцінка впливу на сервіси	Оцінка ризику порушення КДЦ даних	Підтримка пріоритизації і реагування	Можливість кореляції подій
Поведінковий аналіз	Середній	Середня	Середня	Середня	Середня	Висока
Підходи на основі машинного та глибокого навчання	Високий	Висока	Висока	Висока	Висока	Висока
Декларативний підхід	Високий	Висока	Середня	Висока	Висока	Середня

На даному рівні джерелами ознак виступають результати кореляції подій, журнали безпеки, інформація про функціонування сервісів, взаємозв'язки між компонентами системи, дані систем моніторингу та реагування на інциденти, а також показники, що характеризують доступність, цілісність і конфіденційність інформації. Основна увага приділяється не окремій події, а її наслідкам для функціонування ІКС та взаємозв'язку з іншими подіями безпеки.

Результати аналізу свідчать, що найбільш придатними для вирішення таких завдань є підходи на основі машинного та глибокого навчання, поведінковий аналіз та декларативний підхід. Їх застосування забезпечує виявлення взаємозалежних подій, оцінку ступеня впливу кіберінциденту на окремі сервіси ІКС та визначення потенційних ризиків порушення доступності, цілісності або конфіденційності даних. Крім того, зазначені підходи можуть використовуватися для підтримки процесів пріоритизації реагування, коли декілька одночасних інцидентів мають різний вплив на функціонування системи. Проте, оцінювання впливу кіберінциденту значною мірою залежить від повноти інформації про архітектуру ІКС, взаємозв'язки між її компонентами та можливості кореляції подій, отриманих на різних рівнях виявлення. Саме тому ефективне визначення наслідків кіберінциденту потребує комплексного використання результатів аналізу мобільного застосунку, ОС, поведінки користувача, мережевої взаємодії та доступу до сервісів ІКС.

За результатами порівняння підходів на кожному рівні доцільно перейти до визначення методів [18], які можуть бути використані для реалізації виявлення кіберінцидентів на МКП у ВІКС. Для цього з попереднього аналізу відібрано критерії, які найбільшою мірою відображають специфіку використання МКП як засобу роботи зі спеціалізованим ПЗ. Узагальнення обраних критеріїв та можливих методів їх реалізації наведено в таблиці 7.

Таблиця 7

Узагальнення обраних критеріїв та можливих методів їх реалізації

Рівень прояву кіберінциденту	Критерії з урахуванням специфіки МКП у ВІКС	Існуючі методи реалізації
Рівень мобільного застосунку	джерело ознак; здатність виявляти модифіковані застосунки; стійкість до обфускації; потреба у виконанні застосунку; інтерпретованість	сигнатурний аналіз; евристичний аналіз; аналіз графів викликів; дерева рішень; SVM; Random Forest; нейронні мережі; нечітка логіка; експертні системи; штучні імунні системи
Рівень ОС та пристрою	тип контрольованих подій; глибина моніторингу; здатність виявляти приховану активність; ресурсна складність; робота в реальному часі; рівень хибних спрацювань	аналіз системних викликів; статистичний аналіз; кластерний аналіз; аналіз часових рядів; Isolation Forest; One-Class SVM; автоенкодери; нечітка логіка; експертні системи; штучні імунні системи
Рівень поведінки користувача та контексту використання	тип контекстних ознак; здатність виявляти нетипову поведінку; урахування службового сценарію; персоналізація моделі; стійкість до зміни поведінки; пояснюваність	профілювання поведінки користувача; кластерний аналіз; марковські моделі; байєсівські мережі; дерева рішень; LSTM/GRU; нечітка логіка; експертні системи

Продовження таблиці 1

Продовження таблиці 7

Рівень мережевої взаємодії	тип мережевих ознак; здатність виявляти ексфільтрацію; здатність виявляти зв'язок із серверами керування шкідливою активністю; робота із зашифрованим трафіком; контекст взаємодії з ІКС	статистичний аналіз трафіка; аналіз мережевих потоків; аналіз DNS-запитів; аналіз HTTP(S)-сесій; аналіз ентропії; спектральний аналіз; фрактальний аналіз; кластерний аналіз; SVM; Random Forest; автоенкодери; нейронні мережі; нечітка логіка
Рівень доступу до сервісів ІКС	тип ознак доступу; виявлення викрадення сесії; виявлення несанкціонованого доступу; зв'язок із конкретним сервісом ІКС; контекстність доступу; інтерпретованість	аналіз журналів автентифікації; аналіз сесій і токенів доступу; аналіз прав доступу; аналіз запитів до сервісів; кореляційний аналіз; графові методи; байєсівські мережі; дерева рішень; нечітка логіка; експертні системи
Рівень впливу на функціонування ІКС	зв'язок події з функціями ІКС; оцінювання критичності інциденту; вплив на сервіси; вплив на дані; підтримка пріоритизації реагування; можливість кореляції подій	графові методи; кореляційний аналіз подій; аналіз залежностей; аналіз станів системи; байєсівські мережі; нечітка логіка; експертні системи; метод аналізу ієрархій

Вибір критеріїв для кожного рівня обумовлено тим, що в системах ВІКС МКП не розглядається як ізольований мобільний пристрій, а виступає засобом доступу до функцій ІКС через спеціалізоване ПЗ.

На рівні мобільного застосунку найбільше значення мають критерії, пов'язані з виявленням підміни, модифікації, обфускації або невідповідності застосунку його заявленому призначенню.

На рівні ОС та пристрою обрані критерії пов'язані з необхідністю фіксації прихованої активності, яка може не проявлятися безпосередньо у застосунку, але реалізується через процеси, системні події, доступ до ресурсів пристрою, сенсорів або захищених даних. Так, для МКП у ВІКС навіть зовні легітимний застосунок або скомпрометований процес може ініціювати збирання, оброблення чи передавання інформації з обмеженим доступом.

На рівні поведінки користувача та контексту використання ключовими є критерії, що дають змогу враховувати роль користувача, час, місце, тип операції та сценарій роботи зі спеціалізованим ПЗ. У ВІКС одна й та сама дія може бути штатною в одному службовому сценарії та підозрілою в іншому, тому методи цього рівня мають забезпечувати не лише виявлення нетипової поведінки, а й її пояснення з урахуванням контексту використання МКП.

На рівні мережевої взаємодії обрані критерії орієнтовані на виявлення передачі даних поза дозволеними каналами, ексфільтрації, взаємодії із зовнішніми ресурсами та зв'язку із невідомими серверами. Для ВІКС це має особливе значення, оскільки компрометація МКП часто набуває практичного змісту саме тоді, коли службові, сесійні, облікові або геолокаційні дані залишають межі дозволеного інформаційного контуру.

На рівні впливу на функціонування ІКС обрані критерії дають змогу перейти від факту компрометації або підозрілої активності до оцінювання її значення для ВІКС. Мова йде про встановлення зв'язку події з функціями ІКС, впливом на сервіси, дані, доступність, цілісність, конфіденційність та необхідність пріоритизації реагування. Саме цей рівень дозволяє відрізнити окрему ознаку на МКП від кіберінциденту, який має наслідки для функціонування ІКС.

Таким чином, наведене узагальнення окрім потенційної ролі існуючих підходів дає змогу визначити групи методів, найбільш придатних для реалізації виявлення кіберінцидентів на різних рівнях їх прояву. Так, на рівнях мобільного застосунку, ОС, пристрою та мережевої взаємодії доцільними є методи, орієнтовані на виявлення локальних технічних і поведінкових ознак компрометації, зокрема евристичний, статистичний, кластерний аналіз, методи машинного та глибокого навчання, штучні імунні системи й автоенкодери. Тоді як на рівнях доступу до сервісів ІКС і впливу на її функціонування більшого значення набувають методи, здатні встановлювати зв'язки між подіями, користувачем, сесіями, обліковими даними, сервісами та наслідками для виконання покладених в основу функцій, зокрема графові методи, кореляційний аналіз, байєсівські мережі, нечітка логіка та експертні системи.

Однак, зазначені методи здебільшого орієнтовані або на виявлення окремих ознак компрометації, або на їх подальшу кореляцію, тоді як структура самого сеансу взаємодії спеціалізованого клієнтського

ПЗ з серверною частиною ВІКС, де поєднуються автентифікація, використання сесійних параметрів, звернення до сервісів, передавання службових даних і виконання функцій ІКС залишається недостатньо дослідженою.

Після огляду рівнів прояву кіберінцидентів у ВІКС та відповідної науково-методичної основи їх виявлення доцільно розглянути класи засобів [16, 19-25], які можуть забезпечувати практичну їх реалізацію. Так, порівняння засобів доцільно проводити за здатністю охоплювати різні рівні прояву кіберінцидентів. Порівняльна характеристика класів засобів виявлення кіберінцидентів на МКП у ВІКС наведена в таблиці 8.

Таблиця 8

Порівняльна характеристика класів засобів виявлення кіберінцидентів на МКП у ВІКС

Клас засобів	Основне призначення	Рівні охоплення	Методична основа виявлення	Обмеження для ВІКС
Антивіруси для МКП	виявлення шкідливих і підозрілих застосунків	мобільний застосунок; частково ОС	сигнатурний аналіз; евристичний аналіз; аналіз дозволів; аналіз API-викликів; ML-класифікація	слабко враховує доступ до ІКС, сесії та наслідки для ІКС
MTD/Mobile Threat Defense	виявлення загроз на мобільному пристрої	застосунок; ОС; пристрій; мережа; частково поведінка	поведінковий аналіз; ML; аналіз системних подій; аналіз мережевих потоків; евристичні правила	обмежено пов’язує події на МКП із конкретними сервісами ІКС
MDM/EMM /UEM	керування пристроями, політиками та конфігураціями	ОС; пристрій; доступ; частково застосунок	декларативні правила; експертні правила; аналіз відповідності конфігурацій	орієнтованість на керування, ніж на глибоке виявлення кіберінцидентів
EDR	моніторинг кінцевих пристроїв і реагування	ОС; пристрій; поведінка; частково мережа	поведінковий аналіз; графи подій; ML; кореляційний аналіз; експертні правила	класичний EDR не завжди адаптований до МКП і спеціалізованого мобільного ПЗ
NDR/ IDS/ IPS	виявлення загроз у мережевій взаємодії	мережа; частково доступ до сервісів	сигнатурний аналіз; статистичний аналіз трафіка; аналіз ентропії; кластерний аналіз; ML/DL	не завжди визначає, який застосунок, користувач спричинили активність
IAM/Zero Trust	контроль ідентичності, сесій і доступу	доступ до сервісів ІКС; частково поведінка	аналіз сесій; аналіз токенів; байєсівські мережі; нечітка логіка; експертні правила; графові методи	слабко охоплює локальну компрометацію МКП і шкідливу активність застосунку
SIEM	централізований збір і кореляція подій	усі рівні за наявності джерел журналів	кореляційний аналіз; експертні правила; графи подій; ML; аналіз часових послідовностей	ефективність залежить від повноти підключених джерел і якості правил кореляції
XDR	об’єднане виявлення та реагування за різними джерелами	застосунок; пристрій; мережа; доступ; сервіси ІКС	кореляція подій; ML/DL; поведінкова аналітика; графи атак/подій; байєсівські мережі; нечітка логіка; експертні правила	потребує глибокої інтеграції з МКП, сервісами ІКС, засобами доступу й мережевими джерелами

Таким чином, проведений аналіз класів засобів виявлення кіберінцидентів на МКП у ВІКС показує, що їх функціональні можливості суттєво відрізняються як за рівнями охоплення проявів кіберінцидентів (жоден клас не забезпечує повного охоплення всіх рівнів прояву кіберінциденту), так і за науково-методичною основою виявлення.

Антивірусне ПЗ та MTD-засоби найбільш придатні для виявлення загроз на рівні застосунку, ОС і пристрою, але мають обмежені можливості щодо встановлення зв'язку з конкретними сервісами ІКС. MDM/UEM-засоби (Mobile Device Management / Unified Endpoint Management) ефективні для контролю конфігурацій і політик використання МКП, однак не орієнтовані безпосередньо на глибоке виявлення кіберінцидентів. NDR/IDS/IPS (Network Detection and Response / Intrusion Detection System / Intrusion Prevention System) забезпечують ефективний аналіз мережевої взаємодії, але не завжди дають змогу встановити, який застосунок чи сесія спричинили підозрілу активність. IAM/Zero Trust-засоби (Identity and Access Management / Zero Trust Architecture) є важливими для контролю доступу до сервісів ІКС, проте не охоплюють повною мірою локальні прояви компрометації МКП. Найбільш повне охоплення забезпечують SIEM- та XDR-рішення (Security Information and Event Management/Extended Detection and Response), але їх ефективність залежить від повноти інтеграції з МКП, сервісами ІКС, засобами контролю доступу та мережевими джерелами подій.

Результати проведеного аналізу свідчать, що існуючі підходи та засоби виявлення кіберінцидентів на МКП у ВІКС переважно орієнтовані на виявлення окремих індикаторів компрометації, а структурні особливості взаємодії спеціалізованого ПЗ, закономірності побудови сеансів комунікації та інваріантні ознаки поведінки кібератак враховуються недостатньо, що обмежує можливості їх виявлення в умовах зміни способів їх реалізації, використання механізмів приховування активності та модифікації окремих етапів.

У зв'язку з цим, підвищення ефективності виявлення кіберінцидентів на МКП у ВІКС доцільно пов'язувати із розробкою архітектури багаторівневого виявлення кіберінцидентів для забезпечення цілісного охоплення всіх рівнів їх прояву. У такому випадку результат виявлення кіберінциденту, окрім локальної ідентифікації, набуває вигляду структурного опису поточного стану МКП у контексті взаємодії з ВІКС.

Для реалізації запропонованої архітектури доцільно передбачити:

– двосторонній обмін інформацією між МКП та ІКС: у процесі взаємодії МКП з ІКС засобами спеціалізованого ПЗ до підсистеми кіберзахисту ІКС передається узагальнена інформація щодо стану досліджуваних рівнів прояву кіберінцидентів на МКП (цілісність застосунку, параметри ОС і пристрою, контекст поведінки користувача), тоді як ІКС на основі отриманих даних, характеристик мережевої взаємодії, стану сесії та ознак доступу до сервісів, а також визначення належності користувача до певної категорії, оцінки ризику для конкретних сервісів приймає рішення щодо загального стану взаємодії з користувачем;

– дослідження структури сеансів взаємодії спеціалізованого клієнтського ПЗ з серверною частиною ВІКС: виявлення інваріантних характеристик нормальної взаємодії (типових послідовностей операцій, сталих зв'язків між запитами, сесіями, ролями користувачів, сервісами, переданими даними), де їх порушення може свідчити про приховану скомпрометовану взаємодію;

– визначення інваріантів розвитку технік кібератак в офіційних таксономіях кібератак на мобільні пристрої: аналіз персистентних структурних характеристик класів мобільних кібератак, зокрема зв'язків між техніками, етапами кібератаки, способами доступу, закріплення, ексфільтрації та впливу на МКП, що сприятиме підвищенню ефективності виявлення варіацій способів реалізації кіберзагроз;

– обмін досвідом виявлення кіберінцидентів між МКП через ІКС: ознаки, виявлені на одному пристрої, використовуються для уточнення правил, моделей або інваріантів поведінки в ВІКС для інших пристроїв відповідної категорії користувачів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті проведено аналіз існуючих підходів до виявлення кіберінцидентів на МКП у ВІКС. На відміну від більшості відомих досліджень, аналіз проведено за рівнями прояву кіберінцидентів, на яких для кожного з них встановлено джерела ознак, критерії оцінювання та найбільш придатні методи їх виявлення.

За результатами проведеного аналізу встановлено, що існуючі підходи та засоби виявлення кіберінцидентів забезпечують ефективне вирішення окремих завдань кіберзахисту МКП, однак переважно орієнтовані на аналіз окремих ознак компрометації та не забезпечують повного охоплення всіх рівнів прояву кіберінцидентів у ВІКС. Показано, що антивірусні засоби, MTD, EDR, NDR/IDS/IPS, IAM, Zero Trust, SIEM та XDR мають різні рівні функціонального охоплення та використовують різні

джерела даних, а їх ефективне застосування потребує комплексного використання результатів аналізу, отриманих на різних рівнях функціонування МКП та ІКС.

Разом із цим встановлено, що існуючі підходи та засоби недостатньо враховують взаємозв'язки між подіями, які виникають на різних рівнях прояву кіберінцидентів, а також особливості взаємодії спеціалізованого ПЗ на МКП із сервісами ІКС, внаслідок чого ускладнюється встановлення цілісної картини розвитку кіберінциденту, визначення його наслідків для функціонування ІКС та виявлення складних багатоетапних кібератак, окремі прояви яких можуть спостерігатися на різних рівнях функціонування системи.

Таким чином, результати проведеного аналізу створюють підґрунтя для розробки архітектури виявлення кіберінцидентів на МКП у ВІКС, яка враховує всі рівні прояву кіберінцидентів, особливості взаємодії МКП із сервісами ІКС та взаємозв'язки між подіями, що виникають у процесі їх функціонування, що надає змогу перейти від ізольованого виявлення окремих ознак компрометації до формування контекстно орієнтованої моделі кіберінциденту, у якій враховується як локальний стан МКП, так і його роль у функціонуванні ВІКС.

Перспективним напрямком подальших наукових досліджень є розробка моделі визначення інваріантних компонент в розвитку технік кібератак на МКП як елементу запропонованої архітектури.

ДЕКЛАРАЦІЯ ПРО ШТУЧНИЙ ІНТЕЛЕКТ

Інструменти штучного інтелекту використовувались для мовно-стилістичного редагування тексту та не впливали на науковий зміст, результати та висновки дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. State Service of Special Communications and Information Protection of Ukraine. (2024). Russian cyber operations: New targets, tools, and groups. Analysis of hacker attacks against Ukraine in the second half of 2023. https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku
2. State Service of Special Communications and Information Protection of Ukraine. (2025). Russian cyber operations: Attack automation, espionage against the defense sector, and new tactics. Analysis for the second half of 2024. https://cip.gov.ua/ua/news/russian-cyber-operations-attack-automation-espionage-against-defense-sector-and-new-tactics-analysis-for-the-second-half-of-2024
3. Dahiya, A., Singh, S., & Shrivastava, G. (2023). Android malware analysis and detection: A systematic review. Expert Systems. https://doi.org/10.1111/exsy.13488
4. Manzil, H. H. R., & Naik, S. M. (2023). Detection approaches for Android malware: Taxonomy and review analysis. Expert Systems with Applications, 122255. https://doi.org/10.1016/j.eswa.2023.122255
5. Kim, Y.-K., et al. (2022). A systematic literature review on mobile malware detection methods. Communications in Computer and Information Science, 263-288. https://doi.org/10.1007/978-981-16-9576-6_19
6. Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android mobile malware detection using machine learning: A systematic review. Electronics, 10(13), 1606. https://doi.org/10.3390/electronics10131606
7. Sharma, T., & Rattan, D. (2021). Malicious application detection in Android: A systematic literature review. Computer Science Review, 40, 100373. https://doi.org/10.1016/j.cosrev.2021.100373
8. Liu, Y., et al. (2022). Deep learning for Android malware defenses: A systematic literature review. ACM Computing Surveys. https://doi.org/10.1145/3544968
9. Chowdhury, N.-U.-R., et al. (2024). Android malware detection using machine learning: A review. In Lecture Notes in Networks and Systems (pp. 507-522). Springer. https://doi.org/10.1007/978-3-031-47715-7_35
10. Joshi, P., et al. (2016). Protego: A passive intrusion detection system for Android smartphones. In 2016 International Conference on Computing, Analytics and Security Trends (CAST). IEEE. https://doi.org/10.1109/CAST.2016.7914972
11. Faruki, P., et al. (2015). Android security: A survey of issues, malware penetration, and defenses. IEEE Communications Surveys & Tutorials, 17(2), 998-1022. https://doi.org/10.1109/COMST.2014.2386139
12. Al Hwaitat, A. K., et al. (2024). Overview of mobile attack detection and prevention techniques using machine learning. International Journal of Interactive Mobile Technologies, 18(10), 125-157. https://doi.org/10.3991/ijim.v18i10.46485

13. Shabtai, A., Kanonov, U., & Elovici, Y. (2010). Intrusion detection for mobile devices using the knowledge-based temporal abstraction method. Journal of Systems and Software, 83(8), 1524-1537. https://doi.org/10.1016/j.jss.2010.03.046
14. Arp, D., et al. (2014). Drebin: Effective and explainable detection of Android malware in your pocket. In Network and Distributed System Security Symposium (NDSS 2014). https://doi.org/10.14722/ndss.2014.23247
15. Mariconti, E., et al. (2017). MaMaDroid: Detecting Android malware by building Markov chains of behavioral models. In Network and Distributed System Security Symposium (NDSS 2017). https://doi.org/10.14722/ndss.2017.23353
16. Sun, M., et al. (2017). Monet: A user-oriented behavior-based malware variants detection system for Android. IEEE Transactions on Information Forensics and Security, 12(5), 1103-1112. https://doi.org/10.1109/TIFS.2016.2646641
17. de Wit, S. P., Bucur, D., & van der Ham, J. (2021). Dynamic detection of mobile malware using smartphone data and machine learning. Digital Threats: Research and Practice. https://doi.org/10.1145/3484246
18. Subach, I., Fesokha, V., & Fesokha, N. (2017). Analysis of existing intrusion prevention solutions in information and telecommunication networks. Information Technology and Security, 5. https://ela.kpi.ua/server/api/core/bitstreams/39ab1c66-105d-4a53-a344-f300752e6be0/content
19. Fesokha, V. V., Kysylenko, D. Y., & Nesterov, O. M. (2023). Analysis of the capability of existing antivirus protection systems and the methods underlying them to detect new malware in military information systems. Systems and Technologies of Communications, Informatization and Cybersecurity, 3. https://journal.viti.edu.ua/index.php/cicst/article/view/49
20. Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise (NIST SP 800-124 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-124r1
21. Rose, S., et al. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
22. Scarfone, K. A., & Mell, P. M. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94
23. Franklin, J. M., et al. (2020). Mobile device security: Corporate-owned personally-enabled (COPE) (NIST SP 1800-21). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-21
24. Subach, I., Mogylevych, D., Mykytiuk, A., Kubrak, V., & Fesokha, V. (2022). Models of fuzzy identification of cyber incidents in information and communication systems by intelligent SIEM systems. In Proceedings of the XXII International Scientific and Practical Conference “Information Technologies and Security (ITS-2022)” (pp. 151-160). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3503/paper14.pdf
25. Alshamrani, A., et al. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877. https://doi.org/10.1109/COMST.2019.2891891
26. Fesokha, V., Subach, I., & Kopych, D. (2026). Concept of cyber incident detection in a SIEM system based on the integration of fuzzy hypergraph structures and generative artificial intelligence models. Telecommunication and Information Technologies, 1, 15-22. https://tit.duikt.edu.ua/telecommunication/article/view/2694/2575

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Vitalii Fesokha
PhD in Information systems and technologies, Associate Professor, Postdoctoral researcher
Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine
ORCID: 0000-0001-6612-1970
vitaliifesokha@gmail.com

Ihor Subach
Doctor of Technical Science, Professor, Head of the Department
Institute of Special Communications and Information Protection
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0002-9344-713X
igor_subach@ukr.net

Kristina Stepanenko
postgraduate student
Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine
ORCID: 0000-0002-0647-0623
kristinastep567@gmail.com

METHODS AND MEANS OF DETECTION OF CYBER INCIDENTS ON MOBILE TERMINAL DEVICES IN WELL-KNOWN INFORMATION AND COMMUNICATION SYSTEMS

Abstract. In the context of the current scientific task of improving the level of cyber protection of mobile endpoint devices (MEDs) in departmental information and communication systems (DICSs), an analysis of existing approaches to detecting cyber incidents on MEDs was carried out. It is shown that the vast majority of these approaches are focused on identifying individual indicators of device compromise without taking into account the device's role in the functioning of the information and communication system (ICS). The analysis of approaches to detecting malicious activity and the methods used for their implementation was conducted according to the levels at which cyber incidents manifest themselves: the mobile application level, the operating system and device level, the level of user behavior and usage context, the level of network interaction, the level of access to ICS services, and the level of impact on ICS functioning. For each level, characteristic manifestations of cyber incidents, sources of indicators, evaluation criteria, and the most suitable detection approaches were identified. A separate comparison of the functional capabilities of modern classes of tools for detecting cyber incidents on MEDs was also carried out. It was established that none of the considered approaches or classes of tools, when used separately, provides full coverage of all levels at which cyber incidents on MEDs manifest themselves in DICSs. The feasibility of developing an architecture for multilevel detection of cyber incidents on MEDs in DICSs is substantiated. This architecture ensures the formation of a structured description of the current state of an MED in the context of its interaction with the ICS through bidirectional data exchange between the MED and the ICS regarding the state of the cyber incident manifestation levels, analysis of the structure of interaction sessions between specialized client software and the DICS, identification of invariants in the development of cyberattack techniques in mobile threat taxonomies, and exchange of detection experience between MEDs through the ICS.

Keywords: cyber incident; mobile endpoint devices; information and communication systems; specialized software; cyber protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. State Service of Special Communications and Information Protection of Ukraine. (2024). Russian cyber operations: New targets, tools, and groups. Analysis of hacker attacks against Ukraine in the second half of 2023. https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku

2. State Service of Special Communications and Information Protection of Ukraine. (2025). Russian cyber operations: Attack automation, espionage against the defense sector, and new tactics. Analysis for the second half of 2024. https://cip.gov.ua/ua/news/russian-cyber-operations-attack-automation-espionage-against-defense-sector-and-new-tactics-analysis-for-the-second-half-of-2024
3. Dahiya, A., Singh, S., & Shrivastava, G. (2023). Android malware analysis and detection: A systematic review. Expert Systems. https://doi.org/10.1111/exsy.13488
4. Manzil, H. H. R., & Naik, S. M. (2023). Detection approaches for Android malware: Taxonomy and review analysis. Expert Systems with Applications, 122255. https://doi.org/10.1016/j.eswa.2023.122255
5. Kim, Y.-K., et al. (2022). A systematic literature review on mobile malware detection methods. Communications in Computer and Information Science, 263-288. https://doi.org/10.1007/978-981-16-9576-6_19
6. Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android mobile malware detection using machine learning: A systematic review. Electronics, 10(13), 1606. https://doi.org/10.3390/electronics10131606
7. Sharma, T., & Rattan, D. (2021). Malicious application detection in Android: A systematic literature review. Computer Science Review, 40, 100373. https://doi.org/10.1016/j.cosrev.2021.100373
8. Liu, Y., et al. (2022). Deep learning for Android malware defenses: A systematic literature review. ACM Computing Surveys. https://doi.org/10.1145/3544968
9. Chowdhury, N.-U.-R., et al. (2024). Android malware detection using machine learning: A review. In Lecture Notes in Networks and Systems (pp. 507-522). Springer. https://doi.org/10.1007/978-3-031-47715-7_35
10. Joshi, P., et al. (2016). Protego: A passive intrusion detection system for Android smartphones. In 2016 International Conference on Computing, Analytics and Security Trends (CAST). IEEE. https://doi.org/10.1109/CAST.2016.7914972
11. Faruki, P., et al. (2015). Android security: A survey of issues, malware penetration, and defenses. IEEE Communications Surveys & Tutorials, 17(2), 998-1022. https://doi.org/10.1109/COMST.2014.2386139
12. Al Hwaitat, A. K., et al. (2024). Overview of mobile attack detection and prevention techniques using machine learning. International Journal of Interactive Mobile Technologies, 18(10), 125-157. https://doi.org/10.3991/ijim.v18i10.46485
13. Shabtai, A., Kanonov, U., & Elovici, Y. (2010). Intrusion detection for mobile devices using the knowledge-based temporal abstraction method. Journal of Systems and Software, 83(8), 1524-1537. https://doi.org/10.1016/j.jss.2010.03.046
14. Arp, D., et al. (2014). Drebin: Effective and explainable detection of Android malware in your pocket. In Network and Distributed System Security Symposium (NDSS 2014). https://doi.org/10.14722/ndss.2014.23247
15. Mariconti, E., et al. (2017). MaMaDroid: Detecting Android malware by building Markov chains of behavioral models. In Network and Distributed System Security Symposium (NDSS 2017). https://doi.org/10.14722/ndss.2017.23353
16. Sun, M., et al. (2017). Monet: A user-oriented behavior-based malware variants detection system for Android. IEEE Transactions on Information Forensics and Security, 12(5), 1103-1112. https://doi.org/10.1109/TIFS.2016.2646641
17. de Wit, S. P., Bucur, D., & van der Ham, J. (2021). Dynamic detection of mobile malware using smartphone data and machine learning. Digital Threats: Research and Practice. https://doi.org/10.1145/3484246
18. Subach, I., Fesokha, V., & Fesokha, N. (2017). Analysis of existing intrusion prevention solutions in information and telecommunication networks. Information Technology and Security, 5. https://ela.kpi.ua/server/api/core/bitstreams/39ab1c66-105d-4a53-a344-f300752e6be0/content
19. Fesokha, V. V., Kysylenko, D. Y., & Nesterov, O. M. (2023). Analysis of the capability of existing antivirus protection systems and the methods underlying them to detect new malware in military information systems. Systems and Technologies of Communications, Informatization and Cybersecurity, 3. https://journal.viti.edu.ua/index.php/cicst/article/view/49
20. Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise (NIST SP 800-124 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-124r1
21. Rose, S., et al. (2020). Zero trust architecture (NIST SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
22. Scarfone, K. A., & Mell, P. M. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

23. Franklin, J. M., et al. (2020). Mobile device security: Corporate-owned personally-enabled (COPE) (NIST SP 1800-21). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-21
24. Subach, I., Mogylevych, D., Mykytiuk, A., Kubrak, V., & Fesokha, V. (2022). Models of fuzzy identification of cyber incidents in information and communication systems by intelligent SIEM systems. In Proceedings of the XXII International Scientific and Practical Conference "Information Technologies and Security (ITS-2022)" (pp. 151-160). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3503/paper14.pdf
25. Alshamrani, A., et al. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877. https://doi.org/10.1109/COMST.2019.2891891
26. Fesokha, V., Subach, I., & Kopych, D. (2026). Concept of cyber incident detection in a SIEM system based on the integration of fuzzy hypergraph structures and generative artificial intelligence models. Telecommunication and Information Technologies, 1, 15-22. https://tit.duikt.edu.ua/telecommunication/article/view/2694/2575

Отримано редакцією журналу / Received: 28.02.26
Прорецензовано / Revised: 03.03.26
Схвалено до друку / Accepted: 25.06.26