УДК 004.946.056 **doi: 10.32620/aktt.2023.6.10**

В. В. НАРОЖНИЙ, В. С. ХАРЧЕНКО

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

РИЗИК-ОРІЄНТОВАНЕ ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ДОДАТКІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ З ВИКОРИСТАННЯМ IMECA-АНАЛІЗУ

Предметом *дослідження є метод аналізу загроз, вразливостей та вибору контрзаходів для забезпечення кібербезпеки в додатках доповненої реальності (AR)* ***Метою*** *є збільшення повноти оцінювання кіберебезпеки додатків AR шляхом використання формалізованої процедури виявлення та аналізу ризиків поширених загроз, вразливостей та типів атак. Дослідження базується на відомомому методі IMECA (аналізу видів, наслідків та критичності втручань), який структурує процедуру аналізу та мінімізації ризиків шляхом введення відповідних контрзаходів для забезпечення прийнятних ризиків кібербезпеки.* ***Завдання:*** *обґрунтувати множину основних загроз кібербезпеці, характерних для AR додатків; визначити та описати вразливі до загрузки місця в системах AR; надати детальну класифікацію різних кібератак, спрямованих на платформи AR, враховуючі результати дослідження нещодавніх інцидентів; використати метод IMECA для структурованого опису і аналізу питань кібербезпеки та запропонувати надійні контрзаходи. Відповідно до поставлених завдань, були отримані наступні* ***результати:*** *1) класифікація загроз з детальним описом того, як кожна з них може потенційно вплинути на додатки AR, а саме таких загроз як програмне втручання, несанкціонований доступ і вбудовування шкідливого обладнання; 2) критичний аналіз слабких місць систем AR, зокрема, незахищеного зберігання даних і недостатньої автентифікації до використання сенсорів, що забезпечує розуміння можливих векторів атак; 3) детальний опис різних методологій атак, включаючи фішинг у AR, шкідливе програмне забезпечення для AR та атаки "людина посередині", кожна з яких проілюстрована прикладами з реального світу або гіпотетичними сценаріями. Використано системний підхід з використанням фреймворку IMECA для ідентифікації, оцінювання та забезпечення кібербезпеки додатків AR з використанням множини запропонованих контрзаходів.* ***Висновки.*** *Технологія AR, попри її революційність і великий потенціал, породжує унікальний набір викликів щодо кібербезпеки. Ці виклики пов'язані з імерсивним характером технології, залежністю від даних у реальному часі та інтеграцією з фізичним світом. Дослідження підкреслює, що розуміння ландшафту загроз у поєднанні зі структурованим IMECA підходом до управління ризиками є вирішальним для безпечного розвитку додатків AR. Розробники, користувачі та менеджери, відповідальні за політики безпеки, повинні бути проактивними, інноваційними та суголосними у своєму підході до кібербезпеки в системах AR.*

Ключові слова: *доповнена реальність (AR); кібербезпека; IMECA; конфіденційність даних; оцінка вразливостей.*

Вступ

У швидко змінюваному цифровому світі, доповнена реальність (AR) є ключовою технологією, що реформує багато сфер, зокрема, підвищуючи якість взаємодії та зв'язуючи віртуальне з реальним. Зростання її використання у повсякденному житті і критично важливих системах висуває на передній план необхідність захисту від кіберзагроз. Враховуючи її інтерактивність, безпека стає складним завданням. Ця стаття має на меті проаналізувати середовище кібербезпеки доповненої реальності, визначити основні загрози, вразливості та типи атак, а також використати структуру IMECA для структурованого аналізу.

Поява технології доповненої реальності ознаменувалася значним розвитком апаратного та програмного забезпечення, що уможливило інтеграцію цифрового контенту з фізичним середовищем у реальному часі. Її використання варіюється від роздрібної торгівлі до медицини та оборони, збагачуючи різні сфери.

Проблеми кібербезпеки для доповненої реальності є різноманітними і стосуються питань конфіденційності, цілісності та доступності даних.

Загрози можуть виникати з різних джерел, включаючи зловмисників, які використовують вразливості системи для здійснення атак, таких як фішинг, шкідливе програмне забезпечення або атаки "людина посередині".

Мотивація цього дослідження зумовлена зростаючою поширеністю та ускладненням кіберзагроз, націлених на додатки доповненої реальності. Потенціал впливу доповненої реальності не лише на цифрову, але й на фізичну сферу значно підвищує ризики, роблячи потребу в надійних заходах кібербезпеки актуальною.

Метою даної роботи є підвищення розуміння кібербезпеки в контексті доповненої реальності (AR), використовуючи формалізований процес ідентифікації та оцінки загальнопоширених ризиків, загроз та атак. Зосереджуючись на класифікації та аналізі цих викликів, дослідження має на меті розробити комплексні стратегії безпеки, специфічні для AR систем. Через використання методу IMECA, дослідження набуває структурованого характеру, що сприяє глибшому аналізу і встановленню дієвих заходів контролю і політик забезпечення надійного кібербезпекового середовища в AR додатках.

Для досягнення поставленої мети необхідно вирішити наступні **завдання**: 1) класифікація загроз з детальним описом того, як кожна з них може потенційно вплинути на додатки AR, а саме таких загроз як програмне втручання, несанкціонований доступ і вбудовування шкідливого обладнання; 2) критичний аналіз слабких місць систем AR, зокрема, незахищеного зберігання даних і недостатньої автентифікації до використання сенсорів, що забезпечує розуміння можливих векторів атак; 3) детальний опис різних методологій атак, включаючи фішинг у AR, шкідливе програмне забезпечення для AR та атаки "людина посередині", кожна з яких проілюстрована прикладами з реального світу або гіпотетичними сценаріями. Використано системний підхід з використанням фреймворку IMECA для ідентифікації, оцінювання та забезпечення кібербезпеки додатків AR з використанням множини запропонованих контрзаходів.

Вирішуючи ці завдання, стаття надасть корисну інформацію та рекомендації для розробників та користувачів, які беруть участь у розробці, впровадженні та регулюванні технологій доповненої реальності.

1. Сучасний стан кібербезпеки доповненої реальності

Нещодавні дослідження перейшли від теоретичних дискусій до емпіричного аналізу, що відображає зростаючу кількість реальних застосувань та інцидентів, пов'язаних з доповненою реальністю. Дослідники задокументували різні вектори атак, характерні для доповненої реальності, включаючи просторове втручання, підміну датчиків і несанкціонований доступ до чутливих оверлеїв. У літературі все частіше вказується на потребу в надійних механізмах автентифікації, безпечній передачі даних і методах збереження конфіденційності в системах доповненої реальності [1].

Паралельно з цим значна увага приділяється розробці та стандартизації найкращих практик безпеки доповненої реальності. Галузеві групи та регуляторні органи почали розробляти керівні принципи та рамки для захисту додатків доповненої реальності. Ці зусилля спрямовані на надання розробникам і користувачам знань та інструментів, необхідних для захисту від кіберзагроз. Однак у літературі також висвітлюються проблеми, пов'язані з впровадженням цих практик, від технічних обмежень до опору користувачів і швидкого темпу технологічних змін [2].

Ще однією важливою сферою досліджень є психологічні та людські аспекти безпеки доповненої реальності. Дослідники вивчають, як користувачі взаємодіють з AR-додатками, а також потенціал для соціальної інженерії та фішингових атак, які використовують технологію занурення в середовище. Цей напрям досліджень підкреслює важливість навчання користувачів і розробки інтуїтивно зрозумілих, безпечних користувацьких інтерфейсів [3].

2. Аналіз загроз та вразливостей у додатках доповненої реальності

Поширення технології доповненої реальності (AR) відкриває новий вимір взаємодії між користувачами та цифровою інформацією, накладаючи створений комп'ютером контент на реальний світ. Хоча ця технологія покращує користувацький досвід і відкриває нові додатки, вона також створює специфічний набір загроз і вразливостей, які потребують ретельного аналізу та усунення.

Перш ніж заглиблюватися в конкретні загрози та вразливості, важливо зрозуміти екосистему доповненої реальності. За своєю суттю, екосистема доповненої реальності призначена для накладання цифрового контенту на фізичний світ таким чином, щоб покращити сприйняття та взаємодію користувачів. Це досягається завдяки поєднанню технологій і процесів, які включають:

– Апаратне забезпечення: Пристрої та датчики, які фіксують та взаємодіють з реальним світом і відображають доповнений контент;

– Програмне забезпечення: Додатки та операційні системи, які обробляють дані та відтворюють досвід доповненої реальності;

– Мережеві комунікації: Інфраструктура, яка забезпечує обмін даними та зв'язок між пристроями, користувачами та сервісами.

Апаратні компоненти. Розуміння апаратних компонентів є дуже важливим, оскільки вони часто є

першою точкою взаємодії для користувачів і можуть бути джерелом вразливостей. До апаратних компонентів входить:

– Пристрої відображення. Це компоненти, призначені для користувача, такі як окуляри доповненої реальності, гарнітури та мобільні пристрої. Вони відповідають за представлення доповненого контенту користувачеві;

– Датчики та пристрої введення. Доповнена реальність значною мірою покладається на датчик для розуміння та взаємодії з реальним світом. Це камери, GPS, акселерометри, гіроскопи тощо. Пристрої введення також можуть включати сенсорні екрани, системи розпізнавання жестів і голосове керування;

– Обчислювальні блоки. Обчислювальну потужність, необхідну для запуску додатків доповненої реальності, забезпечують процесори, вбудовані в пристрої або доступні віддалено. Ці блоки повинні виконувати складні завдання, такі як обробка зображень, розпізнавання об'єктів і просторове картографування.

Компоненти програмного забезпечення. Програмне забезпечення в системі доповненої реальності - це те, що втілює доповнену реальність у життя, що робить його критично важливим компонентом як для функціональності, так і для безпеки. До програмного забезпечення входить:

– Операційні системи та платформи. Як і у випадку з ПК або смартфонами, пристрої доповненої реальності працюють під управлінням операційних систем, призначених для управління апаратними ресурсами і надання загальних послуг для прикладного програмного забезпечення;

– AR-додатки. Це програми, з якими взаємодіють користувачі. Вони варіюються від ігор та освітніх інструментів до професійних і промислових додатків. Складність і функціональність цих додатків може дуже різнитися;

– Фреймворки та інструменти розробки. Використовуються для створення AR-додатків. Популярні фреймворки включають ARKit, ARCore та Unity. Безпека цих інструментів є життєво важливою, оскільки вразливості можуть поширюватися на кілька додатків.

Мережеві комунікації. Пристрої доповненої реальності часто потребують зв'язку із зовнішніми серверами, сервісами та іншими пристроями для правильної роботи, що робить мережеві комунікації життєво важливим компонентом екосистеми доповненої реальності. Мережеві комунікації включають такі компоненти:

– Передача даних. Сюди входить передача даних датчиків на сервери для обробки, завантаження цифрового контенту для накладання в середовищі користувача, а також завантаження даних користувача для зберігання або аналізу.

– Протоколи підключення. Пристрої доповненої реальності можуть використовувати різні протоколи для підключення, включаючи Wi-Fi, Bluetooth, NFC і стільникові мережі. Кожен з них має свої власні наслідки для безпеки та вразливості;

– Хмарна та серверна інфраструктура. Багато додатків доповненої реальності покладаються на хмарні сервіси для зберігання даних, обчислювальних потужностей і доступу до сторонніх сервісів [4].

Загрози для додатків доповненої реальності. Загрози в контексті кібербезпеки доповненої реальності стосуються потенційних дій або подій, які можуть використовувати вразливості для заподіяння шкоди. Основні загрози включають порушення конфіденційності, крадіжка інтелектуальної власності, атаки на цілісність даних та порушення роботи сервісів.

Порушення конфіденційності. Враховуючи персональні дані та дані про навколишнє середовище, які збирають програми доповненої реальності, існує значний ризик доступу до конфіденційної інформації та її зловживання несанкціонованими особами.

Крадіжка інтелектуальної власності. Додатки доповненої реальності часто використовують запатентовані алгоритми та контент, які можуть стати мішенню для крадіжки або копіювання.

Атаки на цілісність даних. Маніпуляції з даними можуть призвести до того, що система доповненої реальності відображатиме або оброблятиме некоректну інформацію, що матиме реальні наслідки;

Порушення роботи сервісів. Атаки на кшталт відмови в обслуговуванні (DoS) можуть погіршити функціональність додатків доповненої реальності, впливаючи на користувацький досвід і безпеку

Вразливості в системах доповненої реальності. Вразливості - це слабкі місця або недоліки в системі доповненої реальності, які можуть бути використані зловмисниками для заподіяння шкоди. Вони можуть існувати в будь-якій частині системи, від апаратного до програмного забезпечення, і навіть у поведінці користувача. До найпоширеніших вразливостей належать: незахищене зберігання та передача даних, експлуатація датчиків та вразливості програмного забезпечення [5].

Незахищене зберігання та передача даних. Недостатні заходи безпеки можуть призвести до перехоплення, модифікації або викрадення даних.

Недостатня автентифікація та авторизація. Слабкі місця у перевірці ідентифікаційних даних та дозволів користувачів можуть призвести до несанкціонованого доступу або дій.

Експлуатація датчиків. Доповнена реальність значною мірою покладається на датчики для взаємодії з реальним світом. Компрометація цих датчиків може призвести до потрапляння в систему підроблених даних.

Вразливості програмного забезпечення. Помилки або недоліки в програмному забезпеченні доповненої реальності можуть бути використані для виконання шкідливого коду або порушення роботи сервісів [6].

– Типи атак на системи доповненої реальності. На основі виявлених загроз і вразливостей можна організувати різні типи атак на системи доповненої реальності, зокрема:

– Фішинг в доповненій реальності. оманливі накладки або контент можуть змусити користувачів розкрити особисту інформацію або облікові дані;

– Шкідливе програмне забезпечення для доповненої реальності. Шкідливе програмне забезпечення, призначене для націлювання та використання систем доповненої реальності, потенційно беручи під контроль або викрадаючи дані;

– Атаки типу "людина посередині". Перехоплення зв'язку між пристроєм доповненої реальності та серверами з метою викрадення або маніпулювання даними;

– Апаратне втручання. Безпосереднє втручання у фізичні компоненти пристроїв доповненої реальності з метою зміни їхньої функціональності або викрадення даних [7].

Застосування програми IMECA до кібербезпеки доповненої реальності. Для систематичного усунення виявлених загроз і вразливостей можна застосувати фреймворк IMECA (Identification, Measurement, Evaluation, Control, and Assurance - Ідентифікація, вимірювання, оцінка, контроль і забезпечення):

– Ідентифікація. Каталогізація активів систем ДР та виявлення потенційних загроз і вразливостей;

– Вимірювання. Оцінка впливу та ймовірності використання вразливостей виявленими загрозами;

– Оцінка. Визначення пріоритетності ризиків на основі їхньої серйозності та критичності системи;

– Контроль. Впровадження заходів для зменшення або усунення ризиків, таких як шифрування, контроль доступу та регулярний аудит безпеки.

– Забезпечення. Постійний моніторинг ефективності засобів контролю та їх оновлення у відповідь на нові загрози або зміни в системі.

3. Аналіз типів атак на додатки доповненої реальності

Атаки на застосунки доповненої реальності можна широко класифікувати залежно від їхньої мети та методу. Вони можуть бути спрямовані на апаратне, програмне забезпечення або мережеві комунікації систем доповненої реальності і варіюватися від витоку даних до порушення роботи сервісів (табл. 1).

Матриця критичності відображає серйозність кожного типу атаки за відсутності контрзаходів. Вона базується на потенційному впливі та ймовірності виникнення, забезпечуючи візуальне представлення, що допомагає визначити пріоритети у забезпеченні безпеки.

Таблиця 1

Типи атак в доповненій реальності

№	Загроза	Цільовий компонент	Вразливість	Атака	Наслідки	Ризик: ймовірність/ серйозність/ критичність	Контрзаходи
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Фішинг в AR	Взаємодія з користувачем	Довіра користувачів та недоліки дизайну інтерфейсу	Оманливий контент і накладання	Крадіжка даних, несанкціонований доступ	М/М/М	Навчання користувачів, безпечний дизайн, механізми автентифікації
2	Шкідливе програмне забезпечення AR	Програмне забезпечення	Вразливості програмного забезпечення, небезпечні API	Встановлення шкідливого програмного забезпечення	Пошкодження даних, несанкціонований контроль	Н/Н/Н	Регулярні оновлення, антивірусне програмне забезпечення,

Продовження табл. 1

1	2	3	4	5	6	7	8
3	Людина посередині (MitM)	Мережа	Незахищені протоколи зв'язку	Перехоплення та зміна даних	Витік даних, перехоплення сеансу	Н/М/Н	Шифрування, безпечні протоколи зв'язку
4	Спуфінг-атаки	Датчики	Слабкі сторони перевірки даних з датчиків	Подача неправдивих даних на датчики	Дезінформація, фізична шкода	М/Н/Н	Перевірка даних датчиків, виявлення аномалій
5	Відмова в обслуговуванні (DoS)	Мережа/ Сервіс	Пропускна здатність мережі та відмовостійкість сервісів	Перевантаження мережі/сервісу	Перебої в обслуговуванні	Н/Н/Н	Обмеження швидкості, резервування конфігурацій
6	Ін'єкція коду	Програмне забезпечення	Уразливості при обробці вводу	Впровадження шкідливого коду	Несправність, несанкціонований доступ	Н/Н/Н	Перевірка вхідних даних, безпечне кодування

Аналіз матриці критичності без контрзаходів (табл. 2).

Таблиця 2

Матриця критичності

Ймовірність виникнення \ Серйозність	Низька	Середня	Висока
Низька			
Середня		1	4
Висока		3	1, 2, 5, 6

Висока ймовірність і висока серйозність (критичність: висока).

Фішинг у доповненій реальності, шкідливе програмне забезпечення для доповненої реальності, MitM-атаки, DoS-атаки, ін'єкції коду.

Ці загрози позначені як високовірогідні через часту появу та зростаючу витонченість зловмисників. Вони також позначені як високосерйозні, оскільки наслідки можуть бути надзвичайно шкідливими, включаючи значні витоки даних, втрату сервісів і несанкціонований контроль над системами.

Середня ймовірність і висока серйозність (критичність: висока).

Спуфінгові атаки. Ймовірність спуфінг-атак дещо нижча порівняно з іншими, можливо, через специфічні умови або технічні знання, необхідні для їх ефективного виконання проти систем штучного інтелекту. Однак, коли вони все ж відбуваються, їхні наслідки дуже серйозні, оскільки вони можуть призвести до дезінформації та фізичної шкоди, особливо з огляду на імерсивну природу доповненої реальності.

Незважаючи на середню ймовірність, висока тяжкість наслідків робить спуфінг-атаки загрозою високого рівня критичності. Вкрай важливо усунути ці ризики через потенційний значний вплив на безпеку користувачів та цілісність системи.

Аналіз типів атак на додатки доповненої реальності в поєднанні з матрицею критичності підкреслює нагальну потребу в надійних заходах безпеки. Кожен тип атаки становить значний ризик, особливо за відсутності контрзаходів. Розуміючи критичність цих загроз, зацікавлені сторони в екосистемі доповненої реальності можуть розставити пріоритети у своїх зусиллях з безпеки, зосередившись на найсерйозніших ризиках у першу чергу. Впровадження комплексних стратегій безпеки, включаючи регулярні оновлення, навчання користувачів і технічний контроль, має вирішальне значення для зменшення цих ризиків і забезпечення безпечного та надійного використання технології доповненої реальності.

4. Рекомендації щодо захисту додатків доповненої реальності

Рекомендації поділено на стратегії розробки, впровадження та експлуатації, щоб забезпечити комплексний підхід до безпеки доповненої реальності.

1. Стратегії розробки.

Безпека за дизайном.

Принцип: інтегрувати безпеку на ранніх стадіях розробки AR-додатків.

Реалізація: проведення моделювання загроз, характерних для сценаріїв доповненої реальності, визначення потенційних векторів атак і розробка архітектури, стійкої до цих загроз.

Технології, що підвищують конфіденційність.

Принцип: захищати конфіденційність користувачів шляхом мінімізації витоку даних і посилення контролю користувача над особистою інформацією.

Реалізація: використовувати такі методи, як анонімізація даних, безпечні багатосторонні обчислення або диференційована конфіденційність особливо при обробці конфіденційних даних користувача, таких як місцезнаходження або візуальні дані [8].

Безпечний життєвий цикл розробки.

Принцип: дотримування процесу безпечного життєвого циклу розробки (SDLC), який включає контрольні точки та перевірки безпеки.

Реалізація: регулярне проведення аудиту безпеки, перевірку коду та оцінку вразливостей протягом циклів розробки та оновлення.

2.Стратегії впровадження.

Надійна автентифікація та авторизація.

Принцип: забезпечити, щоб лише авторизовані користувачі мали доступ до системи доповненої реальності та могли взаємодіяти з нею.

Реалізація: впровадити багатофакторну автентифікацію, контроль доступу на основі ролей та механізми безперервної автентифікації [9].

Безпека даних.

Принцип: Завжди захищати цілісність і конфіденційність даних.

Реалізація: використовувати шифрування даних у стані спокою та під час передачі, застосовувати

безпечні методи зберігання даних та забезпечити належне управління ключами.

Перевірка датчиків і вхідних даних.

Принцип: забезпечити цілісність та автентичність даних з датчиків та даних, введених користувачем.

Реалізація: впровадження перевірок для підтвердження та обробки даних з камер, GPS та інших датчиків, щоб запобігти підробці або ін'єкційним атакам.

3. Операційні стратегії.

Регулярні оновлення та управління патчами.

Принцип: постійно оновлювати систему доповненої реальності найновішими виправленнями та оновленнями безпеки.

Реалізація: встановлення регулярного графіку оновлень, відстежування нових вразливостей та оперативне застосовування патчей.

Реагування на інциденти та відновлення.

Принцип: підготуватись до потенційних інцидентів безпеки та забезпечити швидке відновлення.

Реалізація: розробити та регулярно оновлювати план реагування на інциденти, проводити навчання, мати резервні копії та процедури відновлення.

Навчання та обізнаність користувачів.

Принцип: інформувати користувачів про потенційні ризики та найкращі практики безпеки.

Реалізація: провести навчання та надати ресурси, щоб допомогти користувачам розпізнавати такі загрози, як фішинг, розуміти важливість оновлень та знати, як ефективно використовувати функції безпеки [10].

4. Розширені рекомендації.

Адаптивна політика безпеки.

Принцип: адаптуватися до нових загроз і змін у середовищі доповненої реальності.

Реалізація: використовувати машинне навчання та штучний інтелект для аналізу поведінки, виявлення аномалій і прогнозування загроз, щоб передбачати нові ризики та реагувати на них.

Спільні зусилля з безпеки.

Принцип: співпрацювати з галузевими партнерами, дослідниками безпеки та регуляторними органами для посилення безпеки доповненої реальності.

Реалізація: брати участь у спільних платформах збору інформації про загрози, долучатись до громадських ініціатив у сфері безпеки та дотримуватись галузевих стандартів і правил.

Етичні міркування.

Принцип: враховувати етичні наслідки технології доповненої реальності, зокрема, пов'язані з конфіденційністю та згодою користувачів.

Реалізація: розробити чітку політику та керівні принципи етичного використання даних, забезпечити прозорість збору та обробки даних, а також надати користувачам можливість контролювати свої дані.

Захист додатків доповненої реальності вимагає багатогранного підходу, який охоплює розробку, впровадження та операційні стратегії. Важливо розуміти, що в міру того, як технологія доповненої реальності продовжує розвиватися, буде розвиватися і сфера кібербезпеки.

З урахуванням застосування контрзаходів матриця критичності має наступний вигляд (табл. 3):

Таблиця 3

Матриця критичності

Ймовірність виникнення \ Серйозність	Низька	Середня	Висока
Низька	1, 3, 4, 6		
Середня		2, 5	
Висока			

Друга матриця (табл. 3) ілюструє ефективність контрзаходів у зниженні критичності різних кіберризиків, пов'язаних з додатками доповненої реальності. Завдяки впровадженню цілеспрямованих стратегій безпеки ймовірність і серйозність загроз були значно знижені, що дозволило перевести більшість ризиків з категорії високої критичності в категорію середньої або низької.

5. Обговорення

Динамічна природа кіберзагроз, особливо у сфері штучного інтелекту, що швидко розвивається, вимагає постійного моніторингу та оновлення матриці критичності. Те, що сьогодні може бути загрозою з низьким рівнем критичності, може швидко зрости з технологічним прогресом або змінами в тактиці зловмисників.

Результати підкреслюють важливість проактивного підходу до кібербезпеки. Очікування атаки, перш ніж реагувати на неї, більше не є життєздатним. Замість цього організації повинні передбачати потенційні загрози і відповідно впроваджувати превентивні заходи. Хоча контрзаходи є ефективними, їх реалізація не позбавлена викликів. Вони можуть включати технічні труднощі, фінансові обмеження та опір змінам. Організації повинні збалансувати ці фактори при плануванні своїх стратегій кібербезпеки.

Взаємопов'язана природа систем доповненої реальності означає, що безпека не є виключною відповідальністю окремих користувачів або організацій. Замість цього вона вимагає спільних зусиль всієї екосистеми, включаючи розробників, виробників, постачальників послуг і регуляторні органи.

Висновки

Ця стаття зосереджена на важливості аналізу кібербезпеки у контексті доповненої реальності (AR), освітлюючи необхідність виявлення та нейтралізації потенційних загроз та вразливостей.

Використання матриці критичності, як до, так і після реалізації контрзаходів, дозволяє глибше зрозуміти специфіку кібербезпеки в AR3і зростаючим впровадженням AR в різних аспектах життя та діяльності, зростає і значимість зміцнення заходів безпеки для забезпечення стабільності цієї технології.

Екосистема доповненої реальності, що складається з обладнання, програмного забезпечення та мережевих комунікацій, являє собою складний контекст для потенційних кіберзагроз. Кожен компонент, сприяючи створенню ефекту занурення в атмосферу доповненої реальності, водночас створює певні вразливості, які необхідно усунути.

Додатки доповненої реальності вразливі до різноманітних кібератак, включаючи фішинг, шкідливе програмне забезпечення, атаки типу "людина посередині", підміну, відмову в обслуговуванні та введення коду. Ці атаки можуть призвести до серйозних наслідків, таких як крадіжка даних, несанкціонований доступ, дезінформація та перебої в роботі сервісів.

Вразливості у системах доповненої реальності охоплюють широкий спектр проблем, включаючи незахищеність даних, слабкі методи автентифікації, уразливості датчиків та небезпеки пов'язані з незахищеними мережевими з'єднаннями.

Матриця критичності з контрзаходами демонструє, що хоча ризики можна значно зменшити, їх неможливо повністю усунути.

Ефективне освітлення користувачів щодо ризиків і заходів безпеки є важливим для підвищення захисту систем доповненої реальності. Користувачі, обізнані з потенційними загрозами та методами їхнього усунення, можуть істотно зміцнити загальну безпеку.

Постійні дослідження та інновації в галузі кібербезпеки необхідні для вирішення проблем, пов'язаних з доповненою реальністю. Це включає розробку вдосконалених протоколів безпеки, технологій, що підвищують конфіденційність, і адаптивних механізмів безпеки, здатних реагувати на загрози, що еволюціонують.

Розуміючи загрози та вразливості, використовуючи структуровані фреймворки, такі як IMECA, і постійно адаптуючись до нових викликів, розробники можуть грантувати безпечність та надійність додатків доповненої реальності.

Майбутні дослідження мають бути зосереджені на розробці адаптивних моделей безпеки, здатних швидко реагувати на нові загрози в міру їх появи. Це включає використання штучного інтелекту і машинного навчання для виявлення загроз і реагування на них у режимі реального часу.

Внесок авторів: аналіз загроз, вразливості та типології атак у додатках доповненої реальності – **В. В. Нарожний**; верифікація дослідницького аналізу, аналіз результатів верифікації – **В. С. Харченко.**

Усі автори прочитали та погодилися з опублікованою версією рукопису.

Література

1. In-Depth Review of Augmented Reality: Tracking Technologies, Development Tools, AR Displays, Collaborative AR, and Security Concerns [Text] / T. Ali Syed, M. Shoaib Siddiqui, H. Binte Abdullah, S. Jan, Abdallah Namoun, A. Alzahrani, A. Nadeem, & A. B.

Alkhodre // Sensors. – 2023. – Vol. 23, Iss. 1. – Article No. 146. DOI: 10.3390/s23010146.

2. An Overview of Augmented Reality [Text] / F. Arena, M. Collotta, G. Pau, & F. Termine // Computers. – 2022. – Vol. 11, Iss. 2. – Article No. 28. DOI: 10.3390/computers11020028.

3. Easttom, W. C. Computer Security Fundamentals, 5th edition [Text] / W. C. Easttom. – Pearson IT Certification, 2023. – 576. ISBN: 9780137984756.

4. Schreiner, S. Security and Privacy in User Modeling: Human–Computer Interaction Series [Text] / S. Schreiner. – Springer Dordrecht, 2011. – 210 p. DOI: 10.1007/978-94-017-0377-2.

5. Peddie, J. Augmented Reality: Where We Will All Live [Text] / J. Peddie. – Springer Cham, 2017. – 323 p. DOI: 10.1007/978-3-319-54502-8.

6. User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review [Text] / I. Anastasaki, G. Drosatos, G. Pavlidis, & K. Rantos // Information. – 2023. – Vol. 14, Iss. 10. – Article No. 538. DOI: 10.3390/info14100538.

7. Впровадження технологій доповненої реальності у навчальному процесі з конструювання авіаційної техніки [Текст] / О. В. Каратанов, А. М. Биков, М. В. Сергієнко, Д. М. Мірошниченко // Радіоелектронні і комп'ютерні системи. – 2021. – № 1. – С. 110-118. DOI: 10.32620/reks.2021.1.10.

8. Vacca, J. R. Computer and Information Security Handbook [Text] / J. R. Vacca. – 3rd edition. – Morgan Kaufmann, 2017. – 1280 p. ISBN: 978-0128038437.

9. Jung, T. Augmented Reality and Virtual Reality: Empowering Human, Place and Business [Text] / T. Jung, & M. C. T. Dieck. – Springer Cham, 2018. – P. 319-350. DOI: 10.1007/978-3-319-64027-3.

10. Brooks, T. T. Cyber-Assurance for the Internet of Things [Text] / T. T. Brooks. – Wiley-IEEE Press, 2016. – 525 p. ISBN: 978-1119193869.

References

1. Ali Syed, T., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. In-Depth Review of Augmented Reality: Tracking Technologies, Development Tools, AR Displays, Collaborative AR, and Security Concerns. *Sensors*, 2023, vol. 23, iss. 1, article no. 146. DOI: 10.3390/s23010146.

2. Arena, F., Collotta, M., Pau, G., & Termine, F. An Overview of Augmented Reality. *Computers*, 2022, vol. 11, iss. 2, article no. 28. DOI: 10.3390/computers11020028.

3. Easttom, W. C. *Computer Security Fundamentals*, 5th edition, Pearson IT Certification Publ., 2023. 576. ISBN: 9780137984756.

4. Schreiner, S. *Security and Privacy in User Modeling: Human–Computer Interaction Serie*s. Springer Dordrecht Publ., 2011. 210 p. DOI: 10.1007/978-94-017-0377-2.

5. Peddie, J. *Augmented Reality: Where We Will All Live*. Springer Cham Publ., 2017. 323 p. DOI: 10.1007/978-3-319-54502-8.

6. Anastasaki, I., Drosatos, G., Pavlidis, G., & Rantos, K. User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review. *Information*, 2023, vol. 14, iss. 10, article no. 538. DOI: 10.3390/info14100538.

7. Karatanov, O., Bykov, A., Sergienko, M., & Miroshnychenko, D. Vprovadzhennya tekhnolohiy dopovnenoyi real′nosti u navchal′nomu protsesi z konstruyuvannya aviatsiynoyi tekhniky [Implementation of Augmented Reality Technologies in the Training Process with the Design of Aircraft Equipment]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, no. 1, pp. 110-118. DOI: 10.32620/reks.2021.1.10.

8. Vacca, J. R. *Computer and Information Security Handbook*, 3rd edition. Morgan Kaufmann Publ., 2017. 1280 p. ISBN: 978-0128038437.

9. Jung, T., & Dieck, M. C. T. *Augmented Reality and Virtual Reality: Empowering Human, Place and Business*. Springer Cham Publ., 2018, pp. 319-350. DOI: 10.1007/978-3-319-64027-3.

10. Brooks, T. T. *Cyber-Assurance for the Internet of Things*. Wiley-IEEE Press Publ., 2017. 525 p. ISBN: 978-1119193869.

Надійшла до редакції 10.08.2023, розглянута на редколегії 20.11.2023

RISK-BASED CYBERSECURITY ASSESSMENT OF AUGMENTED REALITY APPLICATIONS USING IMECA ANALYSIS

Volodymyr Narozhnyi, Vyacheslav Kharchenko

The subject of this study is a method for analyzing threats and vulnerabilities and selecting countermeasures to ensure cybersecurity in augmented reality (AR) applications. The **goal** of this study is to increase the completeness of cybersecurity assessment of AR applications by using a formalized procedure for identifying and analyzing the risks of common threats, vulnerabilities, and types of attacks. This study is based on the well-known IMESA method

(analysis of types, consequences and criticality of interventions), which structures the procedure for analyzing and minimizing risks by introducing appropriate countermeasures to ensure acceptable cybersecurity risks. Objectives: to substantiate the set of major cybersecurity threats specific to AR applications; to identify and describe download vulnerabilities in AR systems; to provide a detailed classification of various cyberattacks aimed at AR platforms, considering the results of a study of recent incidents; to use the IMECA method to describe and analyze cybersecurity issues in a structured manner and to propose reliable countermeasures. According to the tasks, the following **results** were obtained: 1) a classification of threats with a detailed description of how each of them can affect AR applications, namely threats such as software interference, unauthorized access, and malicious hardware embedding; 2) a critical analysis of weaknesses in AR systems, in particular, insecure data storage and insufficient authentication before using sensors, which provides an understanding of possible attack vectors; 3) a detailed description of various attack methodologies, including AR phishing, AR malware, and man-in-the-middle attacks, each illustrated with real-world examples or hypothetical scenarios. A systematic approach using the IMECA framework was used to identify, assess, and ensure the cybersecurity of AR applications using a set of proposed countermeasures. **Conclusions.** AR technology, despite its revolutionary nature and great potential, poses a unique set of cybersecurity challenges. These challenges are related to the immersive nature of the technology, dependence on real-time data, and integration with the physical world. The study emphasizes that an understanding of the threat landscape, combined with an IMESA-structured approach to risk management, is crucial for the secure development of AR applications. Developers, users, and managers responsible for security policies need to be proactive, innovative, and aligned in their approach to cybersecurity in AR systems.

Keywords: augmented reality (AR); cybersecurity; IMECA; data privacy; vulnerability assessment.

Нарожний Володимир Вікторович – асп. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, проф., зав. каф. комп'ютерних систем, мереж кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Volodymyr Narozhnyi – PhD Student of the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: v.narozhniy@csn.khai.edu, ORCID: 0009-0004-3492-2094.

Vyacheslav Kharchenko – Doctor of Technical Sciences, Professor, Head of the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu, ORCID: 0000-0001-5352-077X, Scopus Author ID: 22034616000.