Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В.о. завідувача кафедри БІСТ

Мелкозьорова О.М.

_____

« » 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

за спеціальністю: 125 - Кібербезпека

на тему: «Аналіз розвитку та дослідження ризиків безпеки VR та AR технологій»

оцінка « » Керівник: к.т.н. Малахов С.В._____

Голова ЕК

Лемешко О.В._____ Рецензент: Гостєв О.Л._____

Виконавець: студентка групи КБ-42

Рибалкіна А.А._____

Харків – 2024

РЕФЕРАТ

Пояснювальна записка містить: 48 сторінок, 5 рисунків, 2 таблиці, 29 використаних джерела.

Мета роботи полягає в аналізі основних етапів розвитку технологій віртуальної і доповненої реальності (VR і AR технологій) та визначенні ризиків безпеки, які зумовлені їх використанням.

Об’єкт дослідження: - технології віртуальної та доповненої реальності, як окремі напрями в розвитку сучасних інформаційних технологій (ІТ).

Предмет дослідження: - ризики інформаційної безпеки (ІБ), що пов'язані з використанням VR і AR технологій та стратегії їх парирування.

Основними методами досліджень є аналіз та порівняння.

Відповідно до декларованої мети, у межах роботи вирішувалися наступні завдання: - стислий огляд сучасного стану розвитку VR і AR технологій; - аналіз розвитку обох напрямів, як складової загальної еволюції сучасних ІТ технологій; - ідентифікація потенційних загроз і ризиків для VR та AR; - узагальнення специфічних вразливостей, що притаманні для VR та AR систем; - визначення потенційних стратегій захисту та запобігання загрозам безпеки при впровадженні VR та AR рішень.

У першому розділі роботи розглянуто основні засади VR та AR технологій, особливості їх роботи, переваги і недоліки. У другому розділі проведено ретроспективний огляд розвитку VR і AR технологій та визначена специфіка їх практичного застосування в різних галузях сучасного суспільства. У третьому розділі запропоновано аналіз основних ризиків безпеки при використанні VR і AR технологій. Також надано огляд можливих стратегій захисту для забезпечення належного рівня ІБ при впровадженні відповідних технологій в різні галузі сучасного суспільства.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ВІРТУАЛЬНА РЕАЛЬНІСТЬ, ДОПОВНЕНА РЕАЛЬНІСТЬ, ЗАГРОЗИ ІБ, СТРАТЕГІЇ ЗАХИСТУ.

ABSTRACT

Contains: 48 pages, 5 figures, 2 tables, 29 references.

Purpose of the Work: the objective of this work is to analyze the main stages in the development of virtual and augmented reality technologies (VR and AR technologies) and to identify the security risks associated with their use.

Object of Study: virtual and augmented reality technologies as distinct directions in the development of modern information technologies (IT).

Subject of Study: information security (IS) risks associated with the use of VR and AR technologies and strategies for mitigating them.

Main Research Methods: Analysis and comparison.

In line with the declared purpose, the following tasks were addressed within the work: - a brief review of the current state of development of VR and AR technologies; - analysis of the development of both directions as components of the overall evolution of modern IT technologies; - identification of potential threats and risks for VR and AR; - summarization of specific vulnerabilities inherent in VR and AR systems; - determination of potential protection strategies and threat prevention measures when implementing VR and AR solutions.

In the first section of the work, the main principles of VR and AR technologies, their features, advantages, and disadvantages are considered. In the second section, a retrospective review of the development of VR and AR technologies is conducted, and the specifics of their practical application in various sectors of modern society are determined. In the third section, an analysis of the main security risks associated with the use of VR and AR technologies is proposed. An overview of possible protection strategies to ensure an appropriate level of IS when implementing these technologies in various sectors of modern society is also provided.

Keywords: INFORMATION SECURITY, VIRTUAL REALITY, AUGMENTED REALITY, IS THREATS, PROTECTION STRATEGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ – інформаційна безпека;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ТБ – технічна безпека;

САПР – система автоматизованого проектування (CAD - Computer-Aided Design);

AES – стандарт шифрування даних (Advanced Encryption Standard);

AR – доповнена реальність (augmented reality);

CCD – пристрій із зарядовим зв’язком (Charge-Coupled Device);

CDN – мережа доставки контенту (Content Delivery Network);

DDoS – розподілена атака на відмову в обслуговуванні (Distributed Denial of Service);

DLP – технології запобігання витоку конфіденційної інформації (Data Leak Prevention);

DOI – цифровий ідентифікатор об'єкта (Digital Object Identifier);

HMD – шоломи віртуальної реальності (Head-Mounted Displays);

IDS – система виявлення вторгнень (Intrusion Detection System);

IP – інтернет протокол (Internet Protocol);

IDS – система виявлення вторгнень (Intrusion Detection System);

IPS – система запобігання вторгнень (Intrusion Prevention System);

IT – інформаційні технології (Information Technology);

OSI – абстрактна мережева модель для комунікацій і розробки мережевих протоколів (Open Systems Interconnection);

OTP – пароль, дійсний тільки для одного сеансу автентифікації (One Time Password);

RSA – алгоритм шифрування даних (Rivest-Shamir-Adleman);

VR – віртуальна реальність (virtual reality);

VRML – мова моделювання віртуальної реальності (Virtual Reality Modeling Language);

WPA – протокол безпеки для безпровідних мереж (Wi-Fi Protected Access).

ВСТУП

У сучасному світі технології віртуальної (VR) та доповненої реальності (AR) відіграють ключову роль у всіх сферах життя, від розваг до бізнесу та медицини. Безумовно, що вони є одними з найбільш перспективних і швидко зростаючих напрямів діяльності сучасної науки, та відкривають нові горизонти для взаємодії з цифровим світом, надаючи користувачам можливість «занурення» у віртуальні середовища та/або додавання цифрових елементів до «реального» - звичного для нас (користувачів) світу відносин, явищ та сутностей.

VR та AR технології мають величезний потенціал для подальшої трансформації різних галузей сучасного електронного суспільства, таких як освіта, медицина, промисловість та роздрібна торгівля. Вони дозволяють створювати нові методи навчання, покращувати процеси виробництва, підвищувати ефективність маркетингу та забезпечувати більш захоплюючі ігрові досвіди, та розширювати нові прикладні горизонти інформаційних технологій (ІТ). Водночас, розвиток цих технологій зумовлює появу нових викликів у сфері інформаційної безпеки (ІБ). Недостатня увага до питань ІБ призводе до серйозних наслідків, таких як крадіжка особистих даних, злом пристроїв, несанкціонований доступ (НСД) до конфіденційної інформації та навіть фізичні ушкодження користувачів відповідних пристроїв та/чи сервісів. Враховуючи темпи поширення VR та AR, необхідність у розробці та впровадженні нових принципів й стандартів ІБ стає все більш актуальним.

Метою роботи є аналіз розвитку VR/AR технологій, а також дослідження ризиків безпеки, котрі є наслідком їх впровадження та використання: - основні принципи роботи цих технологій, історичний розвиток та сучасний стан, практичне застосування у різних галузях; специфічні методи уразливостей та потенційні стратегії захисту.

В роботі зроблена спроба ідентифікації потенційних загроз та ризиків безпеки, що притаманні для випадків використання VR/AR технологій. Проведено аналіз методів уразливостей та надані пропозиції, стосовно деяких принципових аспектів при розробці відповідних стратегій захисту для забезпечення безпечного використання цих технологій у різних прикладних контекстах. В цілому, за своїм задумом, робота спрямована на систематизацію та покращення розуміння сутності ризиків безпеки, що обумовлені наслідками впровадження VR/AR технологій, а також на надання базових рекомендацій, стосовно їх (*ризиків*) можливої мінімізації.

1 ОСНОВНІ ЗАСАДИ VR/AR ТЕХНОЛОГІЙ ТА ОСОБЛИВОСТІ ЇХ РОБОТИ

1.1 Основи принципи і методологія використання VR/AR технологій

Технології AR (доповнена реальність) і VR (віртуальна реальність) – це технології, які забезпечують інтерактивний та «занурюючий» досвід, створюючи або змішуючи цифровий контент із реальним чи віртуальним середовищем. Хоча ці технології і мають спільні риси, вони відрізняються своїми характеристиками та областями використання.

Віртуальна реальність (ВР, virtual reality - VR) надає можливість умовного пересування у повністю віртуальному *(тобто, програмно емульованому (відтвореному))* цифровому просторі - створеному штучному середовищі, яке існує лише у вигляді уявних фізичних імітацій (візуальних, тактильних та ін.), та не є частиною «традиційного», фізичного світу. Інши кажучи, віртуальна реальність – ілюзія дійсності, створювана за допомогою комп'ютерних систем, які забезпечують зорові, звукові та інші відчуття.

Сьогодні процес «занурення» у віртуальну реальність стає дедалі складнішим. Фахівці з ІТ, створюють реалістичні послідовності реагування, які активуються кожним фізичним рухом учасників цифрових мандрівок через уявні світи, до яких можна отримати доступ, не покидаючи своєї фізичної реальності . VR вже не є новинкою, а інноваційним інструментом, який широко застосовується у різних професійних сферах. У VR ключову роль відіграють висока роздільна здатність дисплеїв і точність трекінгу рухів, що забезпечують реалістичність і точність відтворення віртуального середовища.

Найпоширенішим апаратним засобом занурення (або взаємодії) у віртуальну реальність є спеціальні шоломи/окуляри (наприклад, Oculus Rift, HTC Vive, PlayStation VR, Valve Index, Samsung Gear VR). Пристрій розташований перед очима користувача дисплей виводиться відео в форматі

3D. Прикріплені до корпусу гіроскоп й акселерометр відстежують повороти голови і передають дані в обчислювальну систему, яка змінює зображення на дисплеї в залежності від показань датчиків. У результаті користувач має можливість «озирнутися» всередині віртуальної реальності і відчути себе в ній, як у реальному світі. Також є додаткові пристрої, такі як контролери та рукавички з тактильним зворотним зв'язком, дозволяють більш реалістично взаємодіяти з віртуальними об'єктами. На рис. 1.1 зображено характерна конструкція VR окулярів.

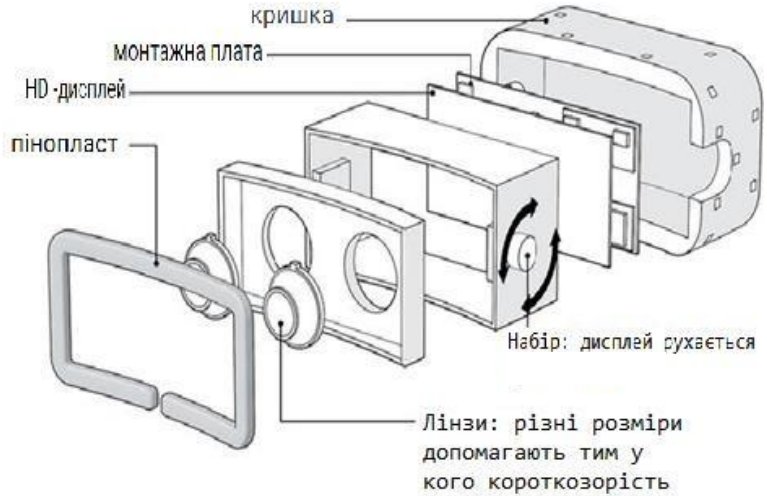

Рис 1.1 – Будова VR окулярів [1]

Системи віртуальної реальності дозволяють користувачам повністю зануритися у віртуальний світ, створений цифровими інформаційними технологіями. Системи доповненої реальності накладають комп'ютерні дані на реальний світ, який бачить користувач.

Доповнена реальність (ДР, *Augmented Reality - AR*)- це система, яка поєднує картину реального світу з об'єктами, створеними комп'ютером. Накладення додаткових елементів на зображення з камери повинно здійснюватися в режимі реального часу, бути інтерактивним та забезпечувати вільний рух користувача у трьох вимірах. Для цього використовуються пристрої, такі як смартфони, планшети, смарт-окуляри та інші гаджети, що оснащені камерами та сенсорами. У результаті те, що бачать на екрані *(або в*

окулярах), частково є фізичною реальністю, а частково цифровою. Однак важливо враховувати та мінімізувати ризики безпеки, пов'язані з її використанням, щоб забезпечити безпечне та ефективне впровадження AR у різні сфери діяльності. Доповнена реальність (AR) і віртуальна реальність (VR) є двома основними типами технологій занурення. Обидві технології мають багато схожих характеристик, але й відмінностей.

Доповнена реальність (AR), на відміну від VR, не заміщує реальний світ, а додає до нього певні (*потрібні для виконання деяких задач*) цифрові елементи. AR інтегрує віртуальні об’єкти в реальне оточення користувача, забезпечуючи змішану реальність. Це означає, що користувач бачить як реальні, так і віртуальні об’єкти одночасно, що дозволяє інтерактивна взаємодіяти з ними. Технічно загальна система доповненої реальності складається з програмного забезпечення, побудованого на вибір із чотирьох основних апаратних компонентів: процесора, пристрою відстеження, пристрою відображення та пристрою введення. Блок обробки створює моделі доповнення, контролює з’єднання пристроїв і регулює положення накладеної інформації в реальному світі щодо пози та положення користувача, використовуючи інформацію, що надходить із пристрою відстеження. Пристрій відстеження використовується для відстеження точного положення та орієнтації користувача, щоб точно вирівняти/зареєструвати збільшення до бажаних положень. [3] Цей пристрій зазвичай складається принаймні з одного елемента захоплення зображення (пристрою із зарядовим зв’язком CCD, стереокамери або камери Kinect з датчиком глибини).

Тривимірна цифрова модель створюється або за допомогою САПР (зазвичай ще на етапі розробки об'єкта), або шляхом оцифрування даної одиниці обладнання. Цей цифровий двійник збирає інформацію про стан об'єкта, що отримується від нього самого, з інформаційних систем та із зовнішніх джерел. З його допомогою ПО доповненої реальності масштабує і точно розміщує на зображенні об'єкта або навколо нього актуальні дані.

1.2 Основні принципи роботи технологій

Основні компоненти системи VR:

- Шоломи віртуальної реальності (HMD): Це основний пристрій для візуалізації віртуального світу. Він складається з дисплея високої роздільної здатності, який розміщений перед очима користувача, та лінз, що забезпечують правильне фокусування та створення тривимірного ефекту. Деякі шоломи також оснащені вбудованими навушниками для аудіозанурення [2].
- Контролери: пристрої дозволяють користувачам взаємодіяти з віртуальним середовищем. Вони відстежують рухи рук і передають цю інформацію в систему, забезпечуючи точну маніпуляцію віртуальними об'єктами [2].
- Трекінгові системи: використовуються для відстеження положення голови та тіла користувача. Це може бути здійснено за допомогою камер, сенсорів або інфрачервоних маячків, які встановлені в кімнаті або на шоломі [3].

Принципи роботи VR:

1) Тривимірне моделювання: віртуальні об'єкти і середовища створюються за допомогою програмного забезпечення для 3D-моделювання. Ці моделі повинні бути максимально реалістичними для досягнення ефекту повного занурення [4].
2) Відстеження рухів: Трекінгові системи відстежують рухи голови і тіла користувача в реальному часі і передають цю інформацію в комп'ютер. Це дозволяє системі змінювати зображення на дисплеї відповідно до рухів користувача, створюючи ефект присутності у віртуальному світі .
3) Рендеринг в реальному часі: Комп'ютер обробляє і відображає графіку у режимі реального часу, забезпечуючи плавний і

реалістичний досвід для користувача. Цей процес включає обчислення освітлення, тіней, текстур і інших аспектів зображення.

4) Аудіо занурення: Багато VR систем використовують просторове аудіо, яке відтворюється через навушники, вбудовані в шолом. Це дозволяє користувачам чути звуки з різних напрямків, що підсилює ефект присутності.

Доповнена реальність (AR). Основні компоненти системи AR:

- Окуляри доповненої реальності: пристрої включають прозорі дисплеї, які накладають віртуальні об'єкти та інформацію на реальний світ. Окуляри можуть мати вбудовані камери, сенсори та процесори для обробки зображень і взаємодії з навколишнім середовищем.
- Смартфони та планшети: мобільні пристрої також використовуються для AR за допомогою вбудованих камер і дисплеїв. Спеціальні додатки обробляють зображення з камери і накладають на них віртуальні елементи .
- Програмне забезпечення: включає алгоритми для розпізнавання об'єктів, обробки зображень та інтеграції віртуальних елементів у реальне середовище. Це може бути платформа ARKit від Apple, ARCore від Google або інші інструменти для розробки AR додатків .

Принципи роботи AR:

1) Розпізнавання образів: камери пристрою захоплюють зображення реального світу. Спеціальні алгоритми аналізують ці зображення для виявлення об'єктів, орієнтирів та поверхонь, на які будуть накладені віртуальні елементи.
2) Накладання віртуальних елементів: після розпізнавання об'єктів програмне забезпечення накладає віртуальні елементи на реальне зображення. Це може бути текст, графіка, анімація або тривимірні

моделі, які інтегруються в реальне середовище з урахуванням просторових координат [5].

3) Взаємодія у реальному часі: користувачі можуть взаємодіяти з віртуальними елементами за допомогою жестів, дотиків або голосових команд. Камери і сенсори відстежують рухи користувача і дозволяють системі реагувати на них у реальному часі [6].
4) Інтеграція з реальним світом: доповнена реальність не ізолює користувача від реального світу, а навпаки, покращує його сприйняття, надаючи додаткову інформацію та функціональність. Це може бути корисним у навчанні, медицині, ремонті, маркетингу та багатьох інших галузях.

Таким чином, VR/AR технології реалізують різні підходи до взаємодії з віртуальним і реальним світом. VR забезпечує відчуття повного (психоемоціонального чи психофізіологічного) занурення у програмно емульоване віртуальне середовище/процес, тоді як AR лише інтегрує певні віртуальні елементи у реальні середовище та/чи процеси, доповнюючи його новими інформаційними вимірами. Кожна з цих технологій має свої унікальні принципи роботи та області застосування, що робить їх корисними у різних практичних контекстах (інженерне проектування, довідкові системи, навігація, неогеографія, військові симулятори, медицина тощо).

1.3 Переваги та недоліки VR та AR

Практичне використання VR надає достатньо багато переваг, зокрема забезпечує користувачам повне «занурення» у синтетичний - віртуальний світ, створюючи потрібні емульовані середовища. Це дозволяє досягти високого рівня взаємодії з імітуемими сутностями, процесами і явищами, оскільки користувачі можуть активно взаємодіяти з віртуальними об'єктами та оточенням. VR також має широке застосування в різних галузях, включаючи ігри, освіту, медицину, архітектуру та військову справу. Проте, VR має й свої

недоліки. Використання VR-систем може бути дорогим, оскільки вони потребують спеціального обладнання, такого як шоломи та потужні комп'ютери. Крім того, VR вимагає багато місця для безпечного використання та може викликати проблеми зі здоров'ям, такі як нудота та запаморочення при тривалому використанні.

Доповнена реальність (AR) надає користувачам можливість бачити та взаємодіяти з віртуальними елементами, накладеними на реальне середовище. Це дозволяє користувачам залишатися в реальному світі, одночасно отримуючи додаткову інформацію та можливості для взаємодії. AR є більш доступною та мобільною, оскільки вона може використовуватися на смартфонах та планшетах, не потребуючи спеціального обладнання. Крім того, AR має широкий спектр застосувань, включаючи освіту, медицину, архітектуру, ремонт, маркетинг та розваги. Проте, AR також має свої обмеження. Ефективність AR залежить від умов реального середовища, таких як освітлення та розпізнавання об'єктів. Інтерактивність з віртуальними елементами може бути менш природною, ніж у VR, і існують потенційні ризики для конфіденційності, оскільки AR-системи можуть збирати та обробляти дані про навколишнє середовище та користувачів.

У кожній технології можна виділити недоліки, які наведено у табл. 1.1. Відповідно, у таблиці 1.2, наведено переваги цих технологій.

За результатами аналізу отриманих відомостей (табл. 1.1-1.2) можна стверджувати, що технології VR та AR мають свої унікальні переваги і недоліки, вони мають різні підходи та вимоги до технологічної реалізації. AR накладає тривимірний віртуальний вміст на реальний світ, покращуючи його за допомогою додаткової інформації, і потребує високої пропускної здатності для забезпечення якісної роботи. Вона надає користувачам більше свободи та можливостей для маркетологів, не потребуючи проекційних дисплеїв.

Крім того, AR демонструє кращий ринковий потенціал і зростає швидшими темпами завдяки використанню великими брендами, і менш

залежить від обмежень пристроїв, що робить її більш гнучкою у використанні. Натомість VR замінює реальний світ на повністю віртуальне середовище, не вимагає використання маркерів або визначення місцезнаходження користувача і має нижчі вимоги до пропускної здатності для потокового відео на 360 градусів, Retina відео та відео з роздільною здатністю 4K. VR забезпечує більш інтерактивний досвід, і краще підходить для додатків, що потребують повного занурення в альтернативний тривимірний світ. Хоча VR є більш інтерактивною, AR має кращий потенціал для інтеграції з реальним світом і маркетингових додатків.

Таблиця 1.1 – Недоліки VR та AR

Доповнена реальність	**Віртуальна реальність**
Накладання тривимірного віртуального цифрового вмісту на реальний світ для збільшення останнього.	Заміна реального світу на віртуальний3D-світ.
Система AR виявляє маркери та розташування користувачів, а також системні дзвінки за попередньо визначеним вмістом, що накладається.	VRML створює інтерактивну послідовність аудіо, анімації, відео та URL-адрес
Вміст AR накладений на виявлений маркер або розташування користувачів.	Немає необхідності в маркерах та виявленні місцеположення користувача для представлення 3D-вмісту.
Вища пропускна здатність для вищої якості роботи - до 100 Мбіт / с для потокової передачі	Нижня вимога допропускної здатності - щонайменше 25 Мбіт/с для потокової передачі.
Найкраще підходить, коли додаток повинен охоплювати середовище користувача.	Найкраще підходить, коли додатокповинен повністю зануритись.

Також хотіла б зазначити, що слід виділити важливий недолік для обох технологій: - що доповнена та віртуальна реальність створює проблеми із психологічною залежністю (зі всіма наслідками) у користувачів, які інтенсивно використовують відповідні платформи. Крім залежності, необхідно враховувати різні інші медичні проблеми, такі як: - проблеми з очима, підвищений рівень ожиріння, хронічний біль *(відторгненні інплантів інтерфейсу, у разі їх використання),*і психологічні та нервові розлади та ін.

Таблиця 1.2 – Переваги VR та AR

Доповнена реальність	**Віртуальна реальність**
Доповнена реальність надає більше свободи для користувача та більше можливостей для маркетологів, оскільки немає необхідності мати проекційний дисплей.	Віртуальна реальність є більш інтерактивною, ніж доповнена.
Доповнена реальність має кращий ринковий потенціал, ніж віртуальна, і останнім часом зростає швидшими темпами, оскільки великі бренди починають його використовувати.	Віртуальна реальність має більшу кількість додатків.
На доповнену реальність менше впливають обмеження пристрою.	Нижча вимога до пропускної здатності, ніж у доповненої реальності, для потокового відео на 360° (*відео якості Retina та роздільної здатності 4K*).

2 РЕТРОСПЕКТИВНИЙ ОГЛЯД РОЗВИТКУ VR/AR ТЕХНОЛОГІЙ ТА СПЕЦИФІКА ЇХ ПРАКТИЧНОГО ЗАСТОСУВАННЯ

2.1 Історичний розвиток технологій

Історія технологій віртуальної реальності (VR) та доповненої реальності (AR) налічує кілька десятиліть і включає багато значущих етапів розвитку.

Початок розвитку та перші експерименти був у ранні роки (1960-ті – 1980-ті роки). Перші кроки в напрямку VR були зроблені в 1960-х роках. Іван Сазерленд, професор Гарвардського університету, створив систему "Меч Демоклеса" (1968), яка використовувала шолом з дисплеями для обох очей і забезпечувала первинний досвід віртуальної реальності. У 1980-х роках компанія VPL Research, заснована Джароном Ланьє, розробила перші комерційні системи VR, такі як DataGlove та EyePhone, що забезпечували користувачам можливість взаємодії з віртуальними об'єктами через трекінгові рукавички та шоломи [7].

1990-ті роки – цей час є розширення можливостей. У 1990-х роках розвиток VR вдосконалюється з акцентом на створення інтерактивних ігрових середовищ та тренажерів. Системи, такі як Sega VR та Nintendo Virtual Boy, були спробами комерціалізації VR-технологій для масового ринку, проте через технічні обмеження та високі витрати ці проекти не стали комерційно успішними [7]. У той же час дослідження у галузі доповненої реальності почали набирати обертів. Льюїс Розенберг у 1992 році створив систему AR для ВПС США, що дозволяла технікам бачити віртуальні інструкції та схеми накладені на реальні об'єкти.

Наступним етапом були 2000-ті роки – новий підйом. З початком нового тисячоліття VR та AR технології зробили великий крок у розвитку завдяки покращенню комп'ютерних потужностей та зниженню вартості апаратного забезпечення. Так у 2012 році Oculus Rift представив перший сучасний шолом

віртуальної реальності, що забезпечував високу роздільну здатність і точний трекінг рухів голови [2]. Це стало початком нової ери віртуальної реальності. Тим часом, AR технології отримали підтримку від великих технологічних компаній. У 2013 році Google представила Google Glass – окуляри доповненої реальності, що надавали користувачам можливість переглядати інформацію, накладену на реальне оточення [7].

2.2 Сучасний стан VR та AR технологій

На сьогоднішній день VR та AR технології продовжують активно розвиватися, інтегруючись у різні сфери життя та бізнесу.

Сучасні системи VR використовуються у багатьох сферах життя, таких як ігрова індустрія, освіта, медицина, архітектура, банківська сфера та інші. В наступному підрозділі більш детально розглянемо окремо кожну сферу використання. Компанії, як Facebook (з брендом Oculus), HTC (Vive) та Sony (PlayStation VR), пропонують високоякісні VR пристрої для споживчого ринку. Також у розвитку великим поштовхом був час пандемії Covid-19 тоді VR стала популярною в індустрії роздрібної торгівлі. Наприклад, John Lewis створив віртуальний різдвяний магазин у 2020 році. Клієнти могли віртуально відвідати магазин на Оксфорд-стріт, оглянути різні товари, включаючи прикраси та предмети домашнього вжитку. Після цього вони могли придбати обрані товари через веб-сайт John Lewis або у фізичному магазині. Системи VR дозволяють створювати реалістичні симуляції, що використовуються для тренування пілотів, хірургів та інших фахівців. В освітніх установах VR використовується для створення інтерактивних навчальних середовищ, що дозволяють студентам досліджувати тривимірні моделі та симуляції [7].

AR почала проникати в роздрібну торгівлю, створюючи нові та захоплюючі враження для покупців по всьому світу. Доповнена реальність технології знайшли широке застосування у навігації, дизайні, ремонті та обслуговуванні техніки, розвагах та маркетингу. AR використовується для

створення інтерактивних інструкцій, що накладаються на реальні об'єкти, що полегшує виконання завдань [6]. Наприклад, у дизайні AR використовується для візуалізації проектів у реальному середовищі, що дозволяє архітекторам та дизайнерам краще уявити, як виглядатиме їхній проект після завершення. Популярні AR платформи, такі як ARKit від Apple та ARCore від Google, дозволяють розробникам створювати додатки для смартфонів та планшетів, які інтегрують віртуальні елементи в реальний світ. Відомі бренди, такі як Sephora, створили додатки, що дозволяють клієнтам віртуально приміряти макіяж перед покупкою. Останніми роками (у зв’язку з пандемією) популярність віртуальних примірочних зросла, оскільки покупці мали обмежений доступ до фізичних магазинів. Зараз більш популярною є можливість приміряти одяг за допомогою мобільних пристроїв. У період закриття шкіл через COVID-19 вчителі взаємодіяли з учнями та організовували віртуальні екскурсії, щоб зменшити їхню ізольованість. Університети та навчальні програми використовували доповнену реальність, щоб допомогти студентам зрозуміти та побачити різні ситуації. Прикладом в наш час є студенти-медики могли віртуально побувати в операційній, а пілоти - пережити надзвичайну ситуацію з пасажирського сидіння. Віртуальна реальність також була інтегрована в різні навчальні симуляції.

Інвестиції та перспективи відіграють досить важливу роль у розвитку даних технологій. Саме гравцями на ринку VR та AR є такі компанії, як Facebook, Microsoft, Epic Games та Apple, які інвестують мільярди доларів у розвиток цих технологій. Facebook придбала Oculus у 2014 році за 2 мільярди доларів, що стало одним з найбільших угод у сфері VR. Microsoft розробила HoloLens – окуляри доповненої реальності, що використовуються для промислових та бізнес-застосувань. Epic Games активно інтегрує AR технології у свою ігрову платформу Unreal Engine, що дозволяє створювати віртуальні та доповнені світи з високою деталізацією та реалістичністю. [8]

Система технологій доповненої та віртуальної реальності стрімко набирає попит, тож ринок доповненої та віртуальної реальності (AR/VR) очікує значне зростання: середньорічний темп зростання прогнозується на рівні 11,8% з 2024 по 2033 рік. До 2033 року обсяг ринку може досягти приблизно 106,2 мільярда доларів США, що є суттєвим збільшенням порівняно з 34,8 мільярда доларів США у 2023 році [9], дана тенденція зображена на рисунку 2.1.

Рисунок 2.1 — Графік зростання ринку VR та AR

VR та AR технології пройшли довгий шлях від перших експериментів до сучасних високотехнологічних систем. Вони продовжують активно розвиватися, інтегруючись у різні сфери життя та бізнесу. Інвестиції великих компаній у розвиток цих технологій свідчать про їхні перспективи та значення у майбутньому. Важливою складовою успішного розвитку VR та AR є забезпечення безпеки користувачів та даних, що вимагає постійної уваги та вдосконалення методів захисту [2]. Звичайно і технологічний прогрес значно впливає на розвиток ринку доповненої та віртуальної реальності. Вдосконалення обладнання, такого як сучасні гарнітури та тактильні пристрої,

покращує взаємодію з користувачем. Крім того, прогрес у програмному забезпеченні, включаючи реалістичні симуляції та доповнені накладання, сприяє технологічній еволюції цих ринків.

2.3 Практичне застосування та основні галузі використання

Спочатку проаналізуємо кожну технологію окремо та сфери життя, де вона має попит на використання. Віртуальна реальність (VR) відкриває нові можливості у багатьох сферах життя завдяки здатності створювати повністю імерсивні середовища, що забезпечують високий рівень взаємодії та інтерактивності. Тож якщо розглядати віртуальну реальність, то можна виділити декілька основних галузей, де VR вже знайшла своє застосування, та її практичні переваги.

- Ігрова індустрія: є однією з найбільших та найпопулярніших галузей, що активно використовує VR. Віртуальна реальність дозволяє геймерам занурюватися у повністю віртуальні світи, де вони можуть взаємодіяти з об'єктами та персонажами на новому рівні. Популярні VR-платформи, такі як Oculus Rift, HTC Vive та PlayStation VR, надають можливість розробникам створювати реалістичні та захоплюючі ігри. Відомі ігри з підтримкою VR, такі як Beat Saber, Half-Life: Alyx та VRChat, стали справжніми хітами, завдяки своїм інноваційним ігровим механікам та інтерактивності [5].
- Освіта: VR використовується для створення інтерактивних навчальних середовищ. Студенти можуть проводити експерименти у віртуальних лабораторіях, досліджувати будову клітин або подорожувати у минуле, вивчаючи історичні події у форматі 3D. VR дозволяє створювати симуляції, які допомагають студентам краще розуміти складні концепції та процеси, роблячи навчання більш цікавим та ефективним.
- Медицина: VR знайшла широке застосування для тренування хірургів, реабілітації пацієнтів та лікування фобій. Хірурги можуть

використовувати VR для відпрацювання складних операційних технік у безпечному віртуальному середовищі, що підвищує їхню професійну підготовку без ризику для пацієнтів. Пацієнти, які проходять реабілітацію після травм, можуть використовувати VR-тренажери для відновлення рухових навичок. VR також використовується у психотерапії для лікування тривожних розладів та фобій, забезпечуючи поступове та контрольоване зіткнення з об'єктами страху [10].

- Архітектура та дизайн: VR дозволяє створювати тривимірні моделі будівель та інтер'єрів, які можна досліджувати у віртуальному просторі. Це дає можливість клієнтам отримати більш чітке уявлення про кінцевий результат проекту, робити корективи на ранніх етапах та забезпечує ефективну комунікацію між архітекторами, дизайнерами та замовниками. VR-технології використовуються для віртуальних турів по майбутніх будівлях, що допомагає залучити інвесторів та покупців.
- Банківська сфера: технологія розпочинає розвиток для створення віртуальних відділень банків, де клієнти можуть взаємодіяти з банківськими продуктами та послугами у віртуальному просторі. Також VR використовується для навчання співробітників, моделювання різних сценаріїв розвитку ринків та управління ризиками. Наприклад, за допомогою VR можна проводити тренінги з управління фінансовими кризами, де співробітники можуть практикувати свої навички у віртуальному середовищі, що максимально наближене до реальних умов.
- Військова справа: є досить популярною для тренування солдатів у різних бойових сценаріях. Віртуальні симуляції дозволяють відпрацьовувати тактичні маневри та взаємодію в команді без ризику для життя та здоров'я. VR-технології допомагають створювати реалістичні бойові ситуації, що покращує підготовку військових і дозволяє адаптуватися до різних умов.

- Нерухомість: VR дозволяє потенційним покупцям здійснювати віртуальні огляди по будинках та квартирах. Перевагою є можливість краще ознайомитися з об'єктами нерухомості, не виходячи з дому.
- Туризм: саме технологія віртуальної реальності додає можливість віртуальних подорожей до різних країн та визначних місць. Це особливо актуально, якщо клієнт не може вирішити де зацікавить його більше, в такому випадку віртуальні тури дозволяють користувачам ознайомитися з визначними місцями, музеями та іншими туристичними атракціями у форматі 360 градусів, що створює ефект присутності.
- Розваги: набула значний попит саме у даній галузі, де використовується для створення інтерактивних кінотеатрів та парків розваг, де відвідувачі можуть зануритися у різні фантастичні світи та історії. VR-атракціони, такі як віртуальні американські гірки чи симулятори польоту, стають дедалі популярнішими, надаючи новий рівень розваг та вражень.

У листопаді 2020 року, у м. Сідней була проведена конференція з питання розвитку інноваційних технологій в туристичній сфері, де доповідачами було надано ряд статистичних даних стосовно розвитку напряму віртуального туризму. На рис 2.2 відображена статистика інтернет-запитів. Завдяки дослідженню яких, можна побачити, які види стали найбільш популярними у сфері віртуальних мандрівок [11]

Отже, сучасні системи VR знаходять широке застосування у багатьох сферах життя, забезпечуючи нові можливості для навчання, тренувань, роботи та розваг. З розвитком технологій можна очікувати подальшого розширення сфер їх використання та появи нових інноваційних рішень.

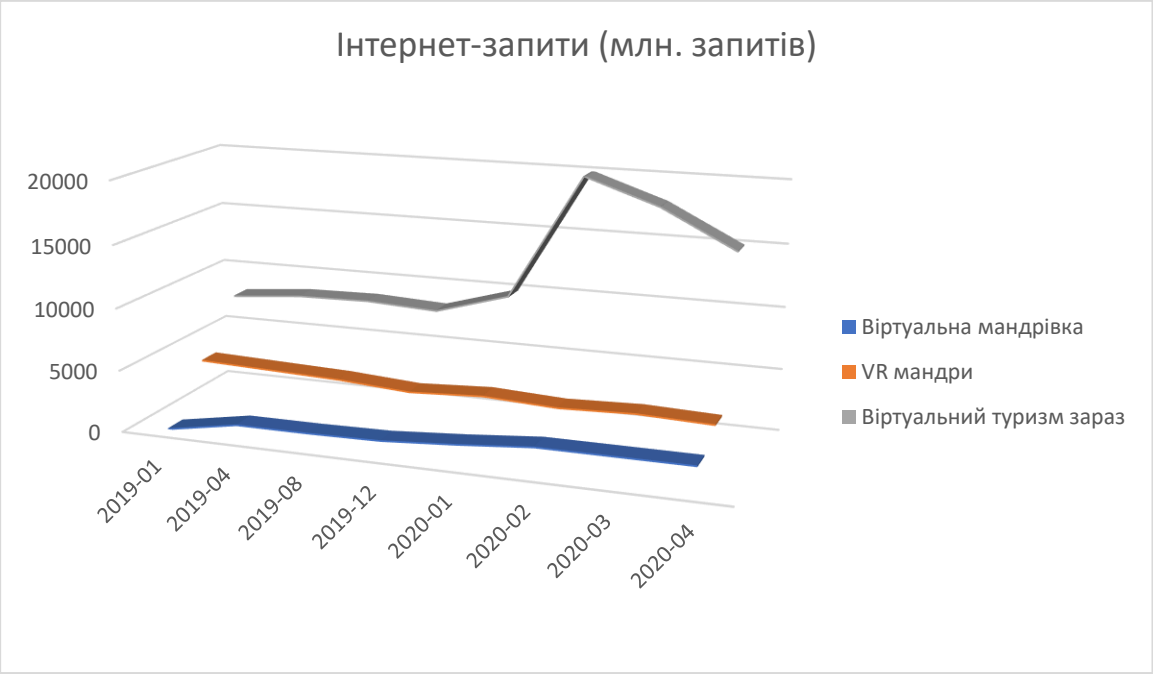

Рисунок 2.2 – Тенденції запитів стосовно віртуального туризму

Якщо ж розглядати доповнену реальність, то практичне застосування та галузі використання AR будуть відрізнятись. Доповнена реальність надає можливість інтегрувати віртуальні елементи у реальне середовище, створюючи нові способи взаємодії з інформацією та оточенням. Ця технологія знаходить широке застосування у різних галузях, забезпечуючи підвищення ефективності та зручності роботи. Нижче розглянемо основні сфери застосування AR та її практичні переваги:

- Освіта: там доповнена реальність використовується для покращення навчального процесу шляхом інтеграції віртуальних елементів у реальні підручники, лабораторні роботи та навчальні матеріали. Наприклад, за допомогою AR-аплікацій студенти можуть взаємодіяти з тривимірними моделями молекул, анатомічними структурами чи історичними артефактами, що сприяє глибшому розумінню складних тем. Це робить навчання більш захоплюючим і ефективним.
- Медицина: знаходить широке застосування для навчання медичного персоналу, планування операцій та реабілітації пацієнтів. Лікарі можуть

використовувати AR для накладання віртуальних зображень на реальні тіла пацієнтів, що допомагає більш точно проводити діагностику та операції. AR також використовується для навчання студентів-медиків, дозволяючи їм вивчати анатомію та хірургічні техніки у віртуальному середовищі.

- Архітектура та дизайн: тут AR дозволяє архітекторам та дизайнерам створювати віртуальні моделі будівель та інтер'єрів, які можуть бути накладені на реальні середовища. Це дає можливість клієнтам побачити, як виглядатимуть майбутні будівлі чи інтер'єри у реальному масштабі, що значно полегшує прийняття рішень та внесення коректив на ранніх етапах проектування .
- Ремонт та обслуговування: саме тут головна мета полягає в тому, що AR допомагає технікам отримувати віртуальні інструкції та схеми, накладені на реальні об'єкти, що спрощує процес ремонту та технічного обслуговування. Наприклад, під час ремонту складного обладнання технік може бачити віртуальні інструкції та поради, що накладаються на реальні компоненти, що дозволяє швидше та точніше виконувати роботу.
- Маркетинг та роздрібна торгівля: AR для створення інтерактивних рекламних кампаній та покращення досвіду покупців. За допомогою AR-каталогів та мобільних додатків покупці можуть віртуально "приміряти" одяг, аксесуари чи меблі перед покупкою. Це дозволяє краще уявити, як товар виглядатиме у реальному житті, що сприяє підвищенню задоволеності клієнтів та збільшенню продажів. Можливість протестувати продукт перед покупкою є важливою для багатьох споживачів. Доповнена реальність все частіше використовується для надання споживачам можливості "спробувати перед покупкою". Приблизно 40% споживачів зазначають, що готові заплатити більше за продукт, який можна попередньо протестувати за

допомогою доповненої реальності. AR також має значний вплив на автомобільну промисловість, дозволяючи брендам вдосконалити процес покупки та навчання водінню. Так клієнти можуть віртуально переглядати різні моделі BMW у різних кольорах прямо на своїх під'їзних доріжках. [5]

- Навігація та туризм: використовується для покращення орієнтації у просторі та створення інтерактивних туристичних гідів. За допомогою AR-додатків користувачі можуть отримувати інформацію про визначні місця, маршрути та навігаційні підказки, накладені на реальне середовище. Це робить подорожі більш зручними та інформативними, дозволяючи туристам краще орієнтуватися у нових місцях та отримувати більше інформації про культурні об'єкти.
- Промисловість та виробництво: доповнену реальність можна розглядати для підвищення ефективності виробничих процесів та навчання персоналу. Робітники можуть отримувати віртуальні інструкції та поради безпосередньо на робочому місці, що дозволяє зменшити кількість помилок та підвищити продуктивність. AR також використовується для моделювання та планування виробничих ліній, що допомагає оптимізувати процеси та знижувати витрати, що є великою перевагою для власників.
- Розваги та медіа: попит має в даній галузі завдяки створенню інтерактивного контенту, що дозволяє глядачам взаємодіяти з віртуальними елементами у реальному часі. AR-додатки дозволяють створювати захоплюючі ігри, інтерактивні книги та фільми, де глядачі можуть взаємодіяти з персонажами та об'єктами. Це створює нові можливості для творчості та розваг, роблячи контент більш динамічним та інтерактивним.

Сучасні системи AR знаходять широке застосування у багатьох сферах життя, забезпечуючи нові можливості для навчання, роботи, ремонту та

розваг. З розвитком технологій можна очікувати подальшого розширення сфер їх використання та появи нових інноваційних рішень.

Загалом, віртуальна і доповнена реальність відкривають нові можливості в різних сферах життя, забезпечуючи високий рівень взаємодії та інтерактивності. З розвитком IT технологій можна очікувати подальшого розширення сфер використання VR/AR технологій, що приведе до появи нових інноваційних рішень та підвищення якості життя. Однак, нажаль, поява та практичне впровадження кожної нової технології, зумовлює і появу нових загроз для суспільства, що їх використовує. В цьому сенсі VR/AR технологій теж не сталі виключенням... - Про це, більш предметно, зупинимося у наступному розділі.

3 ДОСЛІДЖЕННЯ ПИТАНЬ РИЗИКІВ БЕЗПЕКИ В VR ТА AR

3.1 Ідентифікація основних ризиків

Використання VR та AR технологій супроводжується новими та різноманітними ризиками, які можуть суттєво вплинути на стан ІБ (*безвідносно типу кінцевих користувачів*). Ризики можна класифікувати на фізичні, психологічні, а також загрози для ІБ відповідних систем та конфіденційності і стану здоров'я їх користувачів.

Фізичні ризики є одними з найпоширеніших при використанні VR та AR технологій. Одним із таких ризиків є травми, що можуть виникнути через зіткнення з реальними об'єктами. Користувач, занурений у віртуальний світ, часто втрачає орієнтацію у фізичному просторі, що може призвести до випадкових зіткнень з меблями чи іншими перешкодами. Такі інциденти можуть спричинити не лише незначні ушкодження, але й серйозні травми.

Ще одним важливим аспектом є напруга на очі, що виникає внаслідок тривалого використання VR шоломів. Концентрація на близько розташованих екранах може спричинити перенапруження очей, головний біль та зорове виснаження. Також варто згадати про порушення рівноваги та запаморочення, які часто виникають через конфлікт між візуальною інформацією та сигналами, що надходять від внутрішнього вуха. Це явище, відоме як кібер-синдром, може призводити до дезорієнтації, нудоти та навіть падінь. Лише 13% споживачів кажуть, що готові провести більше години у VR-шоломі без перерви [13].

Психологічні ризики також заслуговують на особливу увагу. Тривале використання VR може негативно впливати на психічний стан користувачів, спричиняючи кібер-синдром, що проявляється у вигляді депресії, тривоги та соціальної ізоляції. Перебування у віртуальних середовищах може викликати втрату зв'язку з реальністю, що у свою чергу може призвести до проблем у міжособистісних стосунках та соціальній взаємодії.

Крім того, інтенсивні візуальні та аудіо ефекти, характерні для VR та AR технологій, можуть впливати на підсвідомість користувачів, викликаючи психологічний стрес. Деякі віртуальні досвіди можуть бути настільки реалістичними, що користувачі можуть відчувати сильні емоційні реакції, такі як страх або тривога, що може мати тривалі наслідки для їхнього психічного здоров'я.

Інформаційна безпека та приватність є ще однією важливою сферою ризиків, пов'язаних з використанням VR та AR. Збирання, зберігання та обробка даних, зокрема біометричних, можуть стати мішенню для зловмисників. Неналежний доступ до цих даних може призвести до серйозних наслідків, таких як крадіжка особистої інформації, фінансові втрати та порушення приватності користувачів.

Особливої уваги потребують ризики, пов'язані з відстеженням рухів та збором біометричних даних. Багато сучасних VR та AR пристроїв використовують датчики для відстеження рухів голови, рук та очей, що дозволяє створювати більш реалістичні та інтерактивні віртуальні середовища. Однак, ці дані можуть бути використані зловмисниками для створення детальних профілів користувачів, що становить серйозну загрозу для приватності.

Таким чином, використання VR та AR технологій пов'язане з низкою ризиків, які охоплюють фізичні, психологічні аспекти, а також питання інформаційної безпеки та приватності. Виявлення та розуміння цих ризиків є важливим етапом для розробки ефективних заходів щодо їх мінімізації та забезпечення безпеки користувачів [14].

3.2 Технічні ризики

Технічні ризики, пов'язані з використанням VR та AR технологій, охоплюють різноманітні аспекти, починаючи від програмного забезпечення і закінчуючи апаратними компонентами. Ці ризики можуть призводити до збоїв

у роботі систем, порушень безпеки та зниження якості користувацького досвіду.

Одним з основних технічних ризиків є вразливості в програмному забезпеченні. Віртуальна та доповнена реальності залежать від складного програмного забезпечення, яке часто має баги та недоліки, що можуть бути використані зловмисниками. Такі вразливості можуть призвести до експлойтів, через які зловмисники отримують контроль над системами або доступ до конфіденційних даних користувачів. Наприклад, атака на VR/AR програму може дозволити зловмисникам маніпулювати візуальними даними або отримувати доступ до особистих даних користувача, таких як місцезнаходження або біометричні дані. Безпека та конфіденційність 1 з 5 людей «помірно» або «надзвичайно» стурбований безпекою та конфіденційністю VR. Питання захисту особистих даних та безпеки є важливими для багатьох користувачів, враховуючи обсяг інформації, що збирається VR-системами. Майже 1 із 2 користувачів зазнає переслідувань у соціальних мережах VR, причому типовими цілями стають жіночі аватари. Віртуальні соціальні платформи стикаються з проблемами кібербулінгу та переслідувань, особливо серед жінок [15].

Ще один значний ризик пов'язаний з надмірною залежністю від оновлень програмного забезпечення. Багато виробників VR/AR пристроїв регулярно випускають оновлення для своїх продуктів, щоб покращити функціональність і виправити виявленні вразливості. Однак, відсутність регулярних оновлень або затримки в їх випуску можуть залишити системи вразливими до нових загроз. Це створює ризик, що зловмисники можуть користуватися не оновленим програмним забезпеченням для реалізації атак.

Апаратні недоліки також можуть становити суттєву загрозу для безпеки та функціональності VR/AR систем. Наприклад, несправності в роботі сенсорів, які використовуються для відстеження рухів та позиціонування користувача, можуть призвести до дезорієнтації та навіть фізичних травм.

Якщо датчики неправильно визначають положення користувача або об'єктів у віртуальному просторі, це може спричинити втрату рівноваги та падіння.

Перегрів пристроїв є ще одним серйозним апаратним ризиком. VR/AR гарнітури, особливо ті, що мають високу продуктивність і використовують потужні графічні процесори, можуть перегріватися при інтенсивному використанні. Перегрів може не лише вплинути на роботу пристрою, знижуючи його продуктивність, але й становити небезпеку для користувача, викликаючи дискомфорт або навіть опіки. Виробники повинні передбачити ефективні системи охолодження та захисту від перегріву, щоб мінімізувати ці ризики.

Конфіденційність даних користувачів є ще однією важливою складовою технічних ризиків. Оскільки VR та AR пристрої збирають велику кількість особистих даних, включаючи рухи, вирази обличчя та голосові записи, існує ризик недостатньої захищеності цих даних від несанкціонованого доступу. Зловмисники можуть спробувати отримати доступ до цих даних для крадіжки особистої інформації користувачів або використання її у шахрайських схемах. Наприклад, відстеження рухів очей, що покращує користувацький досвід, також може використовуватися рекламодавцями для відстеження уваги та уподобань користувачів, що потенційно призводить до порушень приватності.

VR та AR пристрої можуть бути піддатливі до різних видів кібератак, таких як віруси, шкідливі програми та зловмисні застосунки (Віруси можуть інфікувати VR та AR пристрої через завантажені файли або підключення до інфікованих мереж, викликаючи збої системи або крадіжку даних. Шкідливі програми маскуються під легітимні додатки, викрадаючи інформацію, записуючи дії користувача або надаючи доступ зловмисникам. Атаки типу "людина посередині" перехоплюють дані між пристроєм та сервером, викрадаючи або змінюючи інформацію. DDoS атаки спричиняють збої серверів та недоступність сервісів. Викрадення даних включає збір особистої інформації, а відстеження дозволяє сенсорам пристроїв стежити за

місцезнаходженням та діями користувача без його відома.). Це може призвести до компрометації особистих даних користувачів, втрати конфіденційної інформації або навіть втрати контролю над пристроєм. Злом VR/AR гаджетів також відкриває можливості для кіберзлочинців змінювати реальність користувачів або використовувати їхні дані для створення глибоких фейків, що становить серйозну загрозу [16].

Недостатня захищеність мереж є ще одним важливим технічним ризиком. Використання VR та AR вимагає підключення до Інтернету або локальних мереж, що створює потенційні ризики для безпеки. Недостатньо захищені мережі можуть бути схильні до зловмисних атак, які можуть стати загрозою для даних користувачів та пристроїв.

Оскільки VR/AR технології перебувають на етапі свого стрімкого розвитку, то вочевидь ,що вимог діючих стандартів безпеки, які регулюють захист особистих даних та безпеку пристроїв, може бути недостатньо. Це може призвести до вразливостей в захисту користувачів від нових (потенційних), що зумовлені впровадженням VR/AR технології. Наприклад, різні виробники можуть використовувати власні підходи до безпеки, що може створювати розбіжності у рівні захисту та ускладнювати сумісність відповідних систем [17].

3.3 Соціальні та етичні ризики

Соціальні та етичні ризики використання технологій віртуальної (VR) та доповненої реальності (AR) є однією з найважливіших та найскладніших категорій ризиків, оскільки вони впливають не тільки на окремих користувачів, але й на суспільство в цілому. Ці ризики охоплюють різноманітні аспекти, включаючи питання приватності, етичних стандартів, соціальної взаємодії та психологічного впливу.

Одним з ключових соціальних ризиків є зниження якості соціальної взаємодії. Використання VR та AR може сприяти соціальній ізоляції, оскільки

користувачі можуть витрачати більше часу у віртуальних світах, ніж у реальному спілкуванні з іншими людьми. Це може призвести до ослаблення міжособистісних зв'язків та розвитку соціальних навичок, що є критично важливими для здорового суспільства. Наприклад, молодь, яка виростає, проводячи більшу частину свого часу у віртуальних середовищах, може відчувати труднощі у встановленні та підтримці реальних соціальних контактів.

Етичні питання також відіграють важливу роль у використанні VR та AR технологій. Відстеження рухів очей, емоцій та інших біометричних даних піднімає серйозні етичні питання щодо приватності та згоди користувачів. Використання цих даних для комерційних цілей або їх передача третім сторонам без чіткої згоди користувача може вважатися порушенням прав на приватність. Це питання стає ще більш актуальним у контексті розробки нових технологій, де користувачі можуть бути не повністю обізнані про те, які дані збираються та як вони використовуються.

Ще одним важливим етичним аспектом є контент, доступний у VR та AR середовищах. Деякі віртуальні простори можуть містити насильницький або шкідливий контент, який може мати негативний вплив на користувачів, особливо на дітей та підлітків. Відсутність належного контролю та регулювання контенту може призвести до ситуацій, коли користувачі піддаються впливу неприпустимих матеріалів, що може мати серйозні психологічні та етичні наслідки.

Соціальні та етичні ризики також включають питання доступності та нерівності. Не всі люди мають рівний доступ до новітніх технологій, що може призвести до розширення цифрової нерівності. Люди з низьким рівнем доходу або ті, хто живе у віддалених районах, можуть бути виключені з переваг, які надають VR та AR, що ще більше поглиблює соціальні та економічні розриви.

Технології VR та AR також можуть мати вплив на зайнятість та ринок праці. З розвитком автоматизації та впровадженням VR/AR у різні галузі існує

ризик втрати робочих місць у традиційних секторах. Це може призвести до соціальної нестабільності, особливо якщо не будуть вжиті заходи для перекваліфікації працівників та створення нових можливостей зайнятості у нових галузях.

Етичні питання щодо маніпуляцій та зловживань VR/AR технологіями також потребують особливої уваги. Наприклад, можливість створення реалістичних deepfake-відео за допомогою VR технологій може бути використана для обману та маніпуляцій, що має серйозні наслідки для довіри у суспільстві. Такі технології можуть використовуватися для політичних маніпуляцій, шантажу або розповсюдження дезінформації, що ставить під загрозу суспільні інститути та демократію.

Таким чином, соціальні та етичні ризики VR та AR технологій є багатогранними та вимагають ретельного аналізу та регулювання. Виробники та розробники повинні враховувати ці ризики при створенні нових продуктів та технологій, забезпечуючи захист прав користувачів, етичне використання даних та підтримку соціальної справедливості. Для зменшення негативного впливу необхідно розробляти чіткі етичні стандарти, проводити освітні кампанії та залучати широку громадськість до обговорення та вирішення цих проблем [18].

3.4 Стратегії захисту та запобігання загрозам

Один із ключових аспектів забезпечення безпеки в AR та VR - це реалізація технічних заходів, спрямованих на захист користувачів та їх даних. Для досягнення цієї мети, важливо впроваджувати наступні заходи:

1) Шифрування даних: Шифрування даних в AR та VR системах використовується для захисту конфіденційної інформації, такої як особисті дані користувачів, банківська інформація тощо. Використання сучасних алгоритмів шифрування (наприклад, AES, RSA) дозволяє забезпечити надійний захист від несанкціонованого доступу.

2) Захист мережі: Забезпечення безпеки мережевих з'єднань включає в себе застосування захисту від DDoS атак, використання безпровідних мереж з ефективними протоколами шифрування (наприклад, WPA2/WPA3), а також регулярне оновлення програмного забезпечення мережевого обладнання.
3) Виявлення та виправлення вразливостей: Аудити безпеки допомагають виявити потенційні вразливості в системі та розробити стратегії для їх виправлення. Це може включати в себе встановлення оновлень безпеки, виправлення програмних помилок, а також використання інструментів виявлення вразливостей, таких як сканери портів та веб-додатків.
4) Механізми автентифікації та авторизації: Використання сильних механізмів автентифікації, таких як біометричні дані, двофакторна аутентифікація або використання токенів, дозволяє перевіряти ідентичність користувачів та забезпечувати доступ тільки авторизованим особам.
5) Захист від шкідливих додатків: Встановлення програмного забезпечення для виявлення та блокування шкідливих програм (антивіруси, фаєрволи) допомагає запобігти інфікуванню системи шкідливими кодами або програмами-викрадачами даних.
6) Фізична безпека: Заходи фізичної безпеки включають в себе захист пристроїв AR та VR від крадіжок або несанкціонованого доступу. Це може включати встановлення систем відеоспостереження, захищених зон доступу або використання систем слідкування за обладнанням.
7) Резервне копіювання та відновлення: Регулярне створення резервних копій даних дозволяє відновлювати систему у випадку втрати даних внаслідок аварій, атак або інших непередбачених ситуацій. Це може бути здійснено за допомогою спеціалізованих програмних засобів або хмарних послуг зберігання даних.

Впровадження цих технічних заходів забезпечує належний рівень безпеки в системах AR та VR, дозволяючи користувачам насолоджуватися їхніми перевагами без зайвих ризиків.

Ринок AR і VR зараз генерує приблизно 32,1 мільярда доларів США щороку. Прогнозується, що до 2028 року дохід зростатиме із середньорічним темпом зростання 10,77% [9], з кожним роком даний показник лише набирає оберти, а саме це і спонукає шахраїв зацікавитись. Якщо проаналізувати ринок технологій доповненої та віртуальної реальності, то розширення ринку VR та AR призводить до збільшення кількості пристроїв і користувачів, які щодня або щомісяця використовують дані технології їх зображено на рисунку 3.1, що підвищує ризик безпеки, якщо не будуть впроваджені чіткі стандарти чи регламенти дій.

Рисунок 3.1 — Графік частоти використання технологіями серед користувачів *(за даними* [19]*)*

Впровадження доповненої та віртуальної реальностей породжує ряд викликів, пов'язаних з безпекою та конфіденційністю. Немає універсального методу, щоб абсолютно захистити користувачів від потенційних загроз. Однак існують кілька рекомендацій, які можуть спрямувати на правильний шлях:

- Ознайомлення з політикою конфіденційності: Перед вибором платформи варто детально вивчити її політику конфіденційності.

Важливо з'ясувати, які дані збираються, як вони обробляються та чи передаються третім сторонам.

- Обмежити передачу особистої інформації: Уникайте розголошення конфіденційних даних у віртуальних середовищах, якщо це необхідно. Використовуйте псевдоніми та уникайте надання фінансових даних, якщо вони не є обов'язковими. Варто користуватися послугами з видалення особистої інформації для контролю за своїм онлайн-слідом.
- Дотримання правил безпеки в Інтернеті: Використовуйте VPN для захисту особистих даних та обмежити свою діяльність у онлайн-спільнотах з дотриманням обережності. Переконайтеся, що використовується надійне програмне забезпечення для безпеки в Інтернеті.
- Керування дозволами: Обмежити права доступу до додатків або сервісів на мінімальний рівень. Вимкніть непотрібні дозволи, які не є обов'язковими для основної функціональності.
- Використання надійної автентифікації: Встановлення надійних та унікальних паролей для облікових записів. Використання двофакторної автентифікації для забезпечення додаткового рівня безпеки.
- Перевірка наявності сертифікатів безпеки: Придбаючи обладнання, переконайтесь, що воно відповідає стандартам безпеки та має всі необхідні сертифікати.

Впровадження технологій доповненої та віртуальної реальностей вимагає ретельного врахування аспектів безпеки та конфіденційності. Хоча не існує єдиного універсального рішення для захисту користувачів, важливо дотримуватися кількох ключових вище зазначених принципів.

Розквіт віртуальних та доповнених реальностей відкриває нові можливості для розваг, навчання та спілкування. Однак, разом із зростанням популярності цих технологій, з'являються й нові загрози. Зловмисники

використовують різноманітні тактики, щоб експлуатувати вразливості в цих середовищах для своєї особистої вигоди.

У 2020 та 2021 роках стали свідками кількох значних інцидентів, що підкреслюють загрози, пов'язані з віртуальними та доповненими реальностями. Так наприклад, хакерська група під назвою «Lizard Squad» здійснила розподілену атаку типу «відмова в обслуговуванні» (DDoS) на популярну платформу віртуальної реальності VRChat. Внаслідок атаки платформа була недоступною протягом кількох годин, що спричинило перебої в роботі для тисяч користувачів. Ця атака нарушила досвід користувачів та спричинила серйозні технічні труднощі для платформи. [20]

Використання захисних рішень для мережі, таких як брандмауери та системи виявлення і запобігання вторгненням (IPS/IDS), допомагає виявляти та блокувати підозрілу активність. Спеціалізовані сервіси захисту від DDoS атак, такі як Cloudflare, Akamai або AWS Shield, здатні відслідковувати трафік та автоматично блокувати атаки, зменшуючи їхній вплив на систему.

Розподіл навантаження є ще одним ефективним методом захисту. Використання балансувальників навантаження для розподілу трафіку між декількома серверами допомагає уникнути перевантаження одного сервера. Мережі доставки контенту (CDN) також можуть розподіляти трафік і зменшувати навантаження на центральні сервери, підвищуючи стійкість системи до DDoS атак. Моніторинг та аналітика відіграють ключову роль у забезпеченні безпеки. Постійний моніторинг трафіку дозволяє виявляти аномалії, які можуть свідчити про початок атаки, а збір та аналіз логів сервера допомагають ідентифікувати підозрілу активність і підготуватися до майбутніх атак.

Окрім технічних заходів, важливо мати план дій на випадок атаки. Розробка інцидентних планів, які включають дії для швидкого відновлення роботи платформи у разі атаки, і регулярне тестування системи на стійкість до DDoS атак забезпечують готовність до непередбачених ситуацій.

Забезпечення безпеки платформ VR та AR вимагає комплексного підходу, який включає використання сучасних технологій захисту, постійний моніторинг, аналітику та планування дій на випадок інцидентів. Це дозволяє знизити ризик успішних атак та забезпечити безперебійну роботу платформ, що є критично важливим для користувачів та бізнесу.

У 2021 році дослідники виявили вразливість на платформі Decentraland, яка могла дозволити хакерам взяти під контроль віртуальний світ і викрасти активи у користувачів. Ця уразливість була пов'язана з системою управління платформою, що дозволяє користувачам голосувати за зміни в правилах і політиках віртуального світу. Недоліки в цій системі могли бути використані для отримання несанкціонованого доступу та маніпуляцій з активами користувачів [21].

Ріст, у свій час, популярності гри Pokémon GO також привернуло увагу кіберзлочинців, що створили шкідливі версії гри для Android-пристроїв. Ці "підроблені" версії містять шпигунське програмне забезпечення, яке може стежити за онлайн-діями користувачів та загрожувати їхній безпеці. Шпигунське ПЗ може виконувати різноманітні дії, включаючи перехоплення особистої інформації та відстеження активності користувача без їхнього відома. Для захисту від шкідливих версій гри та шпигунського програмного забезпечення, користувачам слід дотримуватися кількох ключових рекомендацій. Перш за все, потрібно завантажувати додатки тільки з офіційних магазинів, таких як Google Play, щоб уникнути інфікованих програм. Завжди потрібно перевіряти розробника та відгуки про додаток перед завантаженням. Встановити надійне антивірусне програмне забезпечення на свій пристрій, яке здатне виявляти та блокувати шпигунські програми. Регулярно оновлювати свої додатки та операційну систему, щоб захиститися від відомих вразливостей. Потрібно бути обережними з дозволами, які запитують додатки, і не надавати доступ до даних, якщо це не є необхідним для роботи програми. Дотримуючись цих рекомендацій, можна значно

знизити ризик ураження шпигунським ПЗ та забезпечити безпеку свого пристрою [22].

Дослідники з Університету Нью-Гейвен розробили метод, який дозволяє втручатися в те, що ви бачите у віртуальній реальності за допомогою вірусів. Віртуальні системи, такі як HTC Vive та Oculus Rift, настільки захопливі, що необхідні спеціальні заходи, щоб уникнути травм під час їх використання. Проте, це не заважає зловмиснику змінити ваше сприйняття віртуальної реальності. У контрольованому експерименті дослідники продемонстрували, що можуть змінити візуальний вміст у віртуальних середовищах на пристроях, таких як Oculus Rift та Vive. Їх дослідження висвітлює потенційні ризики, пов'язані з віртуальною реальністю, яка, хоча колись була популярною, тепер стикається з обмеженнями через складність обладнання та відсутність значного досвіду. Крім того, вони довели вразливість систем віртуальної реальності, які використовуються, оскільки їхній фокус був спрямований на перевірку цілісності системи, а не на виявлення потенційних загроз від вірусів. Це означає, що атакувач може маніпулювати віртуальними об'єктами на екрані, що може призвести до нещасних випадків під час гри [21].

Якщо розглянути відомості від *"Regional Distribution"* (2022 р.), що наведені на рис. 3.2, то добре видно, що різні країни беруть участь у дослідженнях безпеки VR та AR [9]. З аналізу наведених відомостей можна зробити декілька висновків:

Провідні країни:

- Японія займає перше місце за кількістю проведених досліджень у галузі безпеки VR та AR, що складає 17% від загальної кількості досліджень. Це вказує на високий рівень зацікавленості в забезпеченні безпеки цих технологій та значні інвестиції в дослідження.
- На другому місці знаходяться Сполучені Штати Америки з 13%. Це свідчить про значну активність у сфері досліджень безпеки VR та AR,

що може бути пов'язано з високим рівнем технологічного розвитку та великою кількістю технологічних компаній, які працюють у цій галузі.

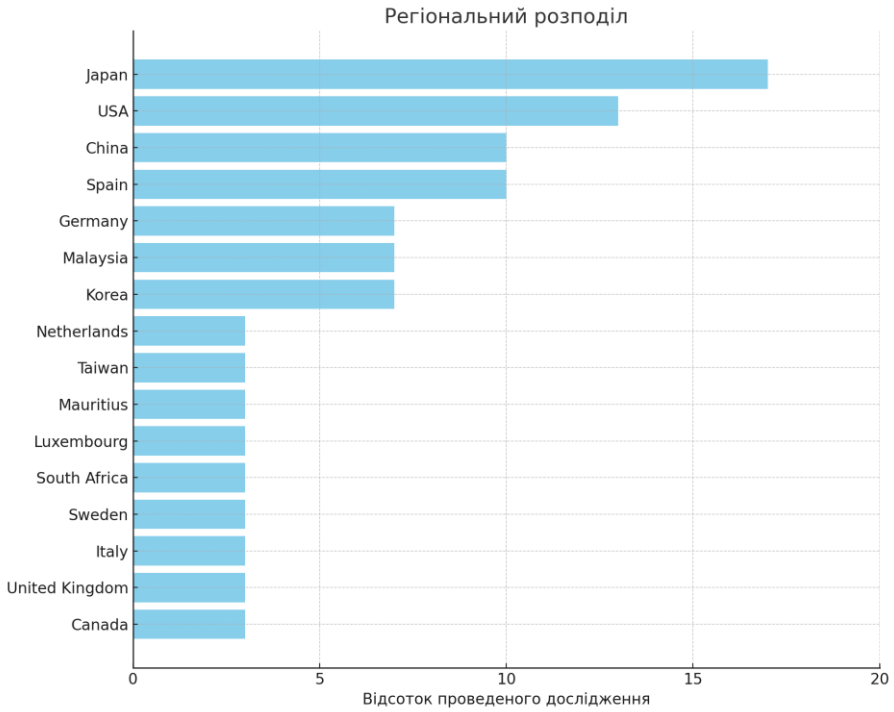

Рисунок 3.2 — Відсоток досліджень з тематики VR/AR за країнами.

Середній рівень участі:

- Китай та Іспанія мають значну частку досліджень, по 10% кожна. Китай демонструє високі темпи розвитку технологій та безпеки, включаючи VR та AR. Іспанія також показує значну активність у цій галузі.
- Корея, Малайзія та Німеччина по 7%. Ці країни також мають значний внесок у дослідження безпеки VR та AR. Корея відома своїм технологічним прогресом, а Німеччина — своїми інженерними досягненнями та увагою до безпеки технологій.

Країни з меншою участю:

Канада, Великобританія, Італія, Швеція, Південна Африка, Люксембург, Маврикій, Тайвань, Нідерланди по 3%. Ці країни також

проводять дослідження у сфері безпеки VR та AR, але їхня частка менша порівняно з лідерами. Це може бути пов'язано з різними рівнями інвестицій, технологічного розвитку та пріоритетів у дослідженнях безпеки [11].

ВИСНОВКИ

Розвиток VR та AR технологій відкриває нові можливості, але і приносить нові загрози для кібербезпеки. Безпека користувачів відповідних послуг, сервісів та гаджетів підпадає під вплив принципово нових загроз через непрямі – опосередковані і часто, взагалі непомітні дії зловмисників, що використовують різноманітні техніки для експлуатації нових специфічних вразливостей. Наприклад, можуть здійснюватися відділені атаки на мережі, втручання у конфіденційність даних, а також маніпуляції з віртуальними середовищами *(бот-фермами віртуальних користувачів – VR юнітів та/чи бот системами)* та поведінкою користувачів відповідних послуг та гаджетів, яки призводять до фінансових втрат, потері функціональності реальних систем та засобів, і навіть до серйозних психологічних дисфункцій користувачів.

Для захисту у цих емульованих кіберсередовищах важливо дотримуватися кращих з вже відомих практик кібербезпеки. Перш за все, це використання сучасних механізмів автентифікації, таких як багатофакторна автентифікація, яка значно знижує ризик НСД. Регулярне оновлення використовуваного програмного забезпечення є, також, критично важливим, оскільки виробники постійно виправляють вразливості, які можуть бути використані атакуючою стороною. Шифрування даних забезпечує захист конфіденційної інформації під час передачі та зберігання, зменшуючи ризик її перехоплення та несанкціонованого використання. А залучення сучасних напрацювань в галузі AI і LM [23-25], додатково розширює можливості, стосовно завчасного виявлення перших ознак, навіть ще невідомих загроз, та посилює оперативність реагування і локалізації можливих наслідків, в разі виникнення відповідних інцидентів ІБ.

Слід підкреслити, що процес підвищення загального рівня професійних компетенцій користувачів (відповідних послуг та гаджетів), стосовно питань

безпеки та безперервного навчання персоналу відповідним прийомам роботи, поряд з усвідомленням всієї повноти здійснюваних мережевих маніпуляцій, є вкрай важливим, саме при використанні VR та AR технологій. Ігнорування цих процедурних аспектів, може дуже швидко призвести до вкрай масштабних наслідків.

Навчання користувачів має критичне значення для забезпечення безпеки. Користувачі повинні бути обізнані про потенційні загрози та методи їх запобігання, включаючи розпізнавання різних типів атак, належне управління паролями та уникнення підозрілих програмних додатків [26-27]. При цьому, окрім запровадження різних технічних заходів, необхідно враховувати соціальні та етичні аспекти [28-29], щоб забезпечити безпечне та етичне використання VR/AR технологій. Це включає захист прав користувачів, забезпечення їх конфіденційності та запобігання використанню технологій для незаконних або шкідливих цілей [29].

Ефективні стратегії захисту (наприклад, впровадження поведінкової фільтрації мережевих подій за рахунок залучення AI та LM [23-25] та комплексна інтеграція біометричних систем захисту від НСД) допоможуть мінімізувати ризики та забезпечити безпечне впровадження VR/AR у різні сфери життя. При цьому, безумовно, що всі технічні аспекти заходів мають підкріплюватися переосмисленням суті та порядку реалізації, у т.ч. організаційної складової, у межах всього реалізованого спектра заходів протидії та профілактики характерних загроз. Це включає розробку нових нормативних актів і стандартів безпеки, впровадження передових технологій захисту та постійний моніторинг VR/AR систем на предмет появи нових загроз. Співпраця між урядами, бізнесом і науковцями є ключовою для розробки та оперативного впровадження відповідних комплексних рішень де фактор часу та масштабованість наслідків, відіграють ключову роль. Тільки в такої парадигмі спільних дій, можна повною мірою скористатися

потенційними перевагами VR/AR технологій, мінімізуючи при цьому ризики для користувачів та суспільства в цілому.

На рівні приватних користувачів окремих виробів та/чи апаратних VR/AR симуляторів важливо дотримуватися надійних механізмів автентифікації та захисту від НСД, підтримувати актуальний стан останніх «прошивок» апаратних засобів та застосовувати стійки алгоритми шифрування для підтримки каналів обміну інформацією між ядром емульованого середовища (процесу) та консольним обладнанням користувачів. У цьому сенсі особливу роль починають грати гарантії безпеки, які анонсують основні провайдери послуг зв'язку..., т.к. саме їх високошвидкісні канали передачі, стають однією з "слабких" елементів у загальному ланцюжку (сукупності) задіяних ресурсів. Питання консолідації та узгодження політик безпеки між провайдерами умовного "середовища передачі" та провайдерами платформ "умовної реальності" стають першочерговими завданнями. Очевидно, що взаємозв'язок таких питань, як: персоніфікація, анонімізація і кластеризація, стосовно емульованих форм і сутностей процесів і явищ, є завданням, що складно формалізується. – Принаймні зараз... Однак, незважаючи на це, та враховуючи швидкий розвиток IT технологій, слід неперервно підтримувати високий рівень поінформованості персоналу з питань VR/AR загроз *(тренінги, навчання та регулярний внутрішній аудит ІБ)* та методів їх запобігання. Така робота, безумовно, повинна бути в фундаменті всіх наступних дій...

.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 WHAT IS INDUSTRIAL AUTOMATION? A COMPREHENSIVE OVERVIEW [Електронний ресурс] / Fiberroad. – 2024. – Режим доступу: https://fiberroad.com/en/resources/new-trends/what-is-industrial-automation-a-comprehensive-overview/ (дата звернення: 10.05.2024)

2 Cipresso, P., Giglioli, I. A. C., Raya, M. A., & Riva, G. (2018). The past, present, and future of Virtual and Augmented Reality research: A network and cluster analysis of the literature. Frontiers in Psychology, 9, 2086. DOI: 10.3389/fpsyg.2018.02086

3 Jerald, J. (2015). The VR Book: Human-Centered Design for Virtual Reality. Morgan & Claypool Publishers. DOI: 10.1145/2792790

4 Azuma, R. T. (1997). A survey of augmented reality. Presence: Teleoperators and Virtual Environments, 6(4), 355-385. DOI: 10.1162/pres.1997.6.4.355

5 Sampangi, R. K., Kosta, S., & Mukhopadhyay, S. (2019). Security and Privacy in Virtual Reality: A Survey. Proceedings of the 2019 ACM Symposium on Virtual Reality Software and Technology (VRST '19). DOI: 10.1145/3359996.3364267

6 Lee, J., Kim, K., & Park, Y. (2020). Threats and Countermeasures in Augmented Reality: A Survey. Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) DOI: 10.1109/PerComWorkshops48775.2020.9156154

7 An Update on European Union General Data Protection Regulation 2016 [Електронний ресурс]. – The Verge. – Режим доступу: https://www.theverge.com/2013/2/20/4006762/google-glass-explained (дата звернення: 21.05.2024)

8 NYU Tandon School of Engineering. Why they dox: First large-scale study reveals top motivations and targets for cyber bullying [Електронний ресурс] / NYU Tandon School of Engineering. – Режим доступу: https://engineering.nyu.edu/news/why-they-dox-first-large-scale-study-reveals-top-motivations-and-targets-form-cyber-bullying (дата звернення: 19.05.2024)

9 24+ Augmented Reality Stats (2024-2028) [Електронний ресурс] / Exploding Topics. – Режим доступу: https://explodingtopics.com/blog/augmented-reality-stats (дата звернення: 24.05.2024)

10 Document 02002L0058-20091219 [Електронний ресурс] / Cases Media. – Режим доступу: https://cases.media/en/article/virtualna-i-dopovnena-realnist-u-medicini-yak-ci-tekhnologiyi-dopomagayut-paciyentam (дата звернення: 20.05.2024)

11 Occupancy rate of the hotel industry worldwide from 2008 to 2018, by region [Електронний ресурс] / Statista. – Режим доступу: https://www.statista.com/statistics/266741/occupancy-rate-of-hotels-worldwide-by-region (дата звернення 19.05.2024)

12 Effects of AR and VR on the Automobile Industry [Електронний ресурс] / ReadWrite. – Режим доступу: https://readwrite.com/effects-of-ar-and-vr-on-the-automobile-industry (дата звернення: 26.05.2024)

13 Kourtesis P. Cybersickness, Cognition, & Motor Skills: The Effects of Music, Gender, and Gaming Experience [Електронний ресурс] / Panagiotis Kourtesis, Rayaan Amir, Josie Linnell, Ferran Argelaguet, Sarah MacPherson // IEEE VR 2023. – 2023. – Режим доступу: https://ieeevr.org (дата звернення: 24.05.2024)

14 Kaspersky Lab. Security and Privacy Risks of AR and VR [Електронний ресурс] // Kaspersky Resource Center. – 2023. – Режим доступу:

https://usa.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr (дата звернення: 23.05.2024)

15 Risks of AR and VR [Електронний ресурс] // Resource Center. – 2023. – Режим доступу: https://usa.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr (дата звернення: 13.05.2024)

16 VR and AR Data Privacy Risks [Електронний ресурс] // InfoSecTrain Blog. – 2023. – Режим доступу: https://www.infosectrain.com/blog/vr-and-ar-data-privacy-risks/ (дата звернення: 19.05.2024)

17 The ethical challenges of AR/VR [Електронний ресурс] // Medium. – Режим доступу: https://medium.com/@alex24dutertre/the-ethical-challenges-of-ar-vr-a5333594f909 (дата звернення: 20.05.2024)

18 Potential security risks to be prepared for [Електронний ресурс] // AT&T Cybersecurity. – Режим доступу: https://cybersecurity.att.com/blogs/security-essentials/vr-and-ar-potential-security-risks-to-be-prepared-for (дата звернення: 13.05.2024)

19 Training and Education [Електронний ресурс] / Virtualspeech // Virtualspeech. – 2024. – Режим доступу: https://virtualspeech.com/blog/vr-stats-training-education (дата звернення: 13.05.2024)

20 Cyber Security Risks of the Metaverse [Електронний ресурс] // WhiteBlueOcean. – 2023. – Режим доступу: https://www.whiteblueocean.com/newsroom/cyber-security-risks-of-the-metaverse/ (дата звернення: 19.05.2024).

21 Goswami, R. Hack a VR system, lead a player astray? Yes, say researchers [Електронний ресурс] / Ruchika Goswami // CNET. – Режим доступу: https://www.cnet.com/tech/mobile/hack-a-vr-system-lead-a-player-astray-yes-say-researchers/ (дата звернення: 18.05.2024).

22 Fake Pokémon GO app watches you, tracks you, listens to your calls [Електронний ресурс] // Sophos News. – Режим доступу: https://news.sophos.com/en-us/2016/07/12/fake-pokemon-go-app-watches-you-tracks-you-listens-to-your-calls/ (дата звернення: 13.05.2024).

23 Азаров, С., Нємцев, М., & Малахов, С. Огляд аналогій та обгрунтування принципів створення демон юнітів відстеження мережевої активності користувачів. Proceedings of the XX International Scientific and Practical Conference. Graz, Austria. 2023. Pp. 447-453. Available at: DOI: 10.46299/ISG.2023.1.20

24 Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. Proceedings of the XXI International Scientific and Practical Conference. Melbourne, Australia. 2023. Pp. 483-487. Available at: DOI: 10.46299/ISG.2023.1.21

25 Михайленко, Д., Чорна, Т. & Малахов, С. Використання можливостей AI при реалізації Static та Dynamic Honeypot для покращення параметрів захисту інформаційних ресурсів. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, (с. 54-57). 7.10.2022 р. Суми, Україна: МЦНД. DOI 10.36074/mcnd-07.10.2022

26 Богданова, Є., Чорна, Т., & Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. *Комп'ютерні науки та кібербезпека*, (2), 35-40. – Режим доступу: https://periodicals.karazin.ua/cscs/article/view/21039/19745 (дата звернення: 24.05.2024).

27 Яремчук, К., Воскобойников, Д., & Мелкозьорова, О. (2022). Сучасні загрози та способи забезпечення безпеки веб-застосунків. *Комп'ютерні науки та кібербезпека*, (2), 28-34. – Режим доступу:

https://periodicals.karazin.ua/cscs/article/view/21038/19744 (дата звернення: 25.05.2024).

28 Лєсная, Ю., Малахов, С. Узагальнення основних передумов реалізації фішингових атак. Proceedings of the XVII International Scientific and Practical Conference. Ankara, Turkey. 2023. Pp.453-457 – Режим доступу: https://isg-konf.com/system-analysis-and-intelligent-systems-for-management/ (дата звернення: 20.05.2024).

29 Гайкова, В., & Малахов, С. (2021). Аналіз факторів і умов реалізації кібербулінгу з урахуванням можливостей сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*, (1), 50-59. DOI: 10.26565/2519-2310-2021-1-04.