Технічні науки

УДК 004.9

Батюк Анатолій Євгенович

кандидат технічних наук, доцент

Національний університет "Львівська політехніка"

Batiuk Anatolii

Candidate of Engineering Sciences, Associate Professor

Lviv Polytechnic National University

Кулик Юрій-Марко Романович

аспірант

Національного університету "Львівська політехніка"

Kulyk Yurii-Marko

PhD Student of the

Lviv Polytechnic National University

ФІЗИЧНА БЕЗПЕКА ТА КІБЕРЗАГРОЗИ В СИСТЕМАХ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ: ЗАБЕЗПЕЧЕННЯ НАЙКРАЩОГО ДОСВІДУ ВИКОРИСТАННЯ

PHYSICAL SECURITY AND CYBER THREATS IN VIRTUAL REALITY SYSTEMS: ENSURING THE BEST USER EXPERIENCE

Анотація. *Стрімкий розвиток технологій віртуальної реальності (ВР) відкриває широкі можливості для їх застосування в різноманітних сферах діяльності людини. ВР-системи активно впроваджуються в індустрії розваг, професійній підготовці, охороні здоров'я, освіті та багатьох інших галузях. Занурення користувача у віртуальне середовище дозволяє отримати унікальний досвід, недосяжний за допомогою традиційних технологій.*

Разом із безсумнівними перевагами ВР, такими як можливість імітації небезпечних ситуацій, тренування навичок у безпечному середовищі, дистанційне навчання тощо, існують і певні проблеми, які потребують ретельного вивчення та вирішення. Одними з ключових аспектів, що викликають занепокоєння при використанні таких систем, є забезпечення фізичної безпеки користувачів, використовуваного обладнання та програмних рішень.

Мета дослідження полягає у формулюванні комплексного підходу до забезпечення безпеки систем віртуальної реальності з метою максимізації користувацького досвіду. Вона передбачає вирішення таких завдань як аналіз існуючих досліджень у сфері фізичної безпеки ВР-систем, виявлення основних кіберзагроз, розроблення рекомендацій з комплексного забезпечення їх безпеки та оцінка ефективності запропонованих заходів для покращення досвіду користувача.

Об'єктом дослідження є системи віртуальної реальності, а предметом – заходи з фізичної та програмної безпеки даних систем.

Завдання даної наукової робити полягають в аналізі існуючих досліджень фізичної та програмної безпеки ВР-систем, визначенню її основних кіберзагроз, розробленню рекомендацій та рішень з комплексного забезпечення фізичної та кібербезпеки, оцінки та аналізу ефективності запропонованих заходів для засобів та рішень віртуальної реальності.

Наукова новизна отриманих результатів полягає у розробці комплексного підходу до забезпечення фізичної та програмної безпеки ВР-рішень.

Дослідження ґрунтується на застосуванні комплексу загальнонаукових та спеціалізованих методів, у тому числі аналізу літературних джерел для виявлення тенденцій та проблем у сфері безпеки ВР-систем, систематизації та узагальнення для розробки комплексного підходу до забезпечення безпеки, а також моделювання сценарію

програмних загроз та аналіз їх можливих наслідків для оцінки ефективності застосованих заходів.

Практична значущість роботи полягає в тому, що розроблені рекомендації можуть бути використані при проектуванні, встановленні та експлуатації систем та засобів віртуальної реальності у різних сферах застосування, адже впровадження запропонованих заходів дозволить забезпечити високий рівень безпеки та комфорту для будь-яких користувачів таких рішень.

Представлена наукова робота спрямована на розроблення комплексного підходу до забезпечення фізичної та програмної безпеки ВР-систем, що дозволить мінімізувати ризики їх використання та створити найкращий досвід для користувачів. Отримані результати мають важливе теоретичне та практичне значення для розвитку сучасних технологій у сфері віртуальної реальності.

Ключові слова: *віртуальна реальність, безпека застосування, кібербезпека, безпека даних, захист користувачів, захищеність систем.*

Summary. *The rapid development of virtual reality (VR) technologies opens up wide opportunities for their application in various areas of human activity. VR systems are being actively implemented in the entertainment industry, professional training, healthcare, education and many other sectors. Immersing users in a virtual environment allows them to gain a unique experience that is unattainable with traditional technologies.*

Along with the undoubted advantages of VR, such as the ability to simulate dangerous situations, training skills in a safe environment, distance learning, etc., there are also certain problems that need to be carefully studied and addressed. One of the key aspects of concern when using such systems is ensuring the physical security of users, equipment and software solutions.

The purpose of the study is to formulate a comprehensive approach to ensuring the security of virtual reality systems in order to maximize the user experience. It involves solving such tasks as analyzing existing research in the field of physical security of VR systems, identifying the main cyber threats faced by these systems, developing recommendations for comprehensive security, and evaluating the effectiveness of the proposed measures to improve the user experience.

The object of the study is virtual reality systems, and the subject is measures for the physical and software security of these systems.

The objectives of this research are to analyze existing studies of physical and software security of VR systems, identify its main cyber threats, develop recommendations and solutions for comprehensive physical and cyber security, evaluate and analyze the effectiveness of the proposed measures for virtual reality tools and solutions.

The scientific novelty of the results is the development of an integrated approach to ensuring physical and software security of VR solutions.

The study is based on the application of a set of general scientific and specialized methods, including the analysis of literature sources to identify trends and problems in the field of VR systems security, systematization and generalization to develop an integrated approach to security, as well as modelling scenario of software threats and analyzing their possible consequences to assess the effectiveness of the measures taken.

The practical significance of the work lies in the fact that the developed recommendations can be used in the design, installation and operation of virtual reality systems and tools in various fields of application, since the implementation of the proposed measures will ensure a high level of safety and comfort for any users of such solutions.

Thus, the presented research work is aimed at developing an integrated approach to ensuring the physical and software security of VR systems, which will

minimize the risks of their use and create the best experience for users. The results obtained are of great theoretical and practical importance for the development of modern technologies in the field of virtual reality.

Key words: *virtual reality, application security, cybersecurity, data security, user protection, system safety.*

Аналіз літературних джерел. Технології віртуальної реальності швидко розвиваються, а сфера їх застосування невпинно розширюється. Проте, разом із численними перевагами та можливостями, що відкриваються завдяки ВР-системам, виникають нові виклики та ризики, пов'язані з фізичною безпекою користувачів та захистом від кіберзагроз. Дослідники та розробники активно працюють над вирішенням цих питань, пропонуючи різноманітні підходи та рішення.

"Security Considerations for Virtual Reality Systems" за авторством Karthik Viswanathan та Abbas Yazdinejad [1] описує і досліджує потреби та варіанти застосування методів аутентифікації в рішеннях віртуальної реальності. Поточні системи передбачають, що технологія іммерсивного досвіду це комплекс периферійних пристроїв, підключених до персонального комп'ютера або мобільного пристрою. Існує повна залежність від обчислювального пристрою з традиційними механізмами аутентифікації для управління аутентифікацією та прийняттям рішень щодо авторизації. А застосування контролерів та шоломів віртуальної реальності створює додаткові виклики, оскільки надіслані ними дані (наприклад, дії людини с середовищі ВР) можна перехоплювати без відомості користувача.

У статті аналізується кілька запропонованих систем аутентифікації. Дослідники порівняли пропоновані механізми аутентифікації та прийшли до висновку, що жодна з них не відповідає вимогам, ідентифікованим ними. Тому для комерційного застосування ВР потрібний високий рівень

деталізації, аутентифікація повинна бути більш ніж просто перевіркою ідентичності користувача.

Автори розглядають різні механізми аутентифікації, такі як: RubikBiom, RubikAuth, OcuLock, BioMove. Кожен з них має власні переваги та недоліки застосування, наприклад, RubikBiom використовує складні алгоритми, які вимірюють поведінкові шаблони користувача, RubikAuth дозволяє застосовувати механізми аутентифікації за допомогою рухів руки користувача, OcuLock використовує складний алгоритм, який враховує різні аспекти роботи зорових системи людини (поведінка та рух очного яблука, очних м'язів), а BioMove використовує біометричну ідентифікацію на основі унікальних патернів руху рук та тіла користувача.

У роботі "Security of virtual reality authentication methods in metaverse: An overview" автори Pınar Kurtunluoglu, Beste Akdik та Enis Karaarslan [2] детально розглядають потенційні проблеми безпеки та конфіденційності у метавсевіті (віртуальному просторі, в якому люди можуть взаємодіяти між собою), з якими можуть зіткнутися користувачі ВР-систем.

Головними пристроями, які використовуються для доступу до метавсесвіту, є гарнітури віртуальної реальності. Стаття порівнює безпеку основних методів аутентифікації, які використовуються в середовищі віртуальної реальності, обговорює питання приватності (зазначається, що метавсесвіт може збирати значно більше даних, ніж соціальні мережі, включаючи особисту інформацію, поведінку та комунікаційні патерни), розглядає проблеми безпеки у метавсевіті, зокрема цілісність даних і відрізнення програмних агентів від людей.

Zhihan Lv, Dongliang Chen, Ranran Lou і Houbing Song в роботі під назвою "Industrial Security Solution for Virtual Reality" [3] обговорюють важливість захисту промислових системи ВР від зовнішніх атак та виокремлюють декілька проблем з забезпечення безпеки, у зв'язку з їх постійним підключенням до мережі Інтернет та Інтернету речей.

Зазначається, що традиційні методи захисту, такі як застосування патчів (внесення певних змін в частини коду для виправлення існуючих помилок), брандмауерів та антивірусного програмного забезпечення, не завжди ефективні у випадку промислових систем керування через їх унікальні характеристики.

У роботі пропонується використання алгоритму C-Support Vector Machine (CSVM) для побудови моделі виявлення вторгнень в мережі промислового контролю на основі зразків та класифікації. Дослідники використовують дані для симуляційних експериментів у віртуальному середовищі реальності. Результати показують, що вказаний алгоритм демонструє високу точність класифікації та здатність виявлення вторгнень при використанні різних ядерних функцій та змінних значень параметрів.

Рішення пропонує новий підхід до виявлення вторгнень у промислових системах керування в умовах віртуального середовища. Використання алгоритму CSWC-SVM дозволяє ефективно виявляти потенційні загрози безпеці в промислових мережах, що використовуються у віртуальному середовищі. А знання та техніки, надані в даній праці, можуть допомогти розробникам програмного забезпечення та адміністраторам мереж забезпечити безпеку віртуальної реальності в промисловому контексті.

Aniket Gulhane, Akhil Vyas, Reshmi Mitra, Roland Oruche, Gabriela Hoefer, Samaikya Valluripally, Prasad Calyam та Khaza Anuarul Hoque у науковій праці під назвою "Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications" [4] описують та досліджують проблеми забезпечення безпеки, конфіденційності та безпеки людей у середовищах навчання на основі віртуальної реальності (VRLE) на прикладі рішення vSocial.

Для оцінки рівня та якості навчання та залучення людей до навчального процесу використовуються методи відстеження емоцій та

аналізу голосу, тобто зберігає дані, отримані під час процесу навчання, на хмарній платформі. Це створює потенційні загрози для безпеки та конфіденційності.

У статті пропонуються нові методи оцінки ризиків, які використовують "дерева атак" для розрахунку оцінки ризику для різних загроз VRLE з використанням частоти та тривалості загроз як вхідних даних. Використовується тестова платформа vSocial для демонстрації ефективності методів оцінок та демонстрації того, як відповідна формалізація дерев атак може допомогти в створенні більш безпечної VRLE.

Автори зазначають, що існують обмежені дослідження у сфері безпеки і приватності в технології віртуальної реальності, тому потрібні систематичні рамки для квантифікації ризиків, пов'язаних з загрозами безпеки, конфіденційності та безпеці.

Maria Korolov у дослідницькій статті "The real risks of virtual reality" [5] описує важливі ризики для здоров'я, поведінкові аспекти та проблеми конфіденційності при застосуванні рішень віртуальної реальності. Детально вказує на фізичні ризики для людини, що включають можливість виникнення різноманітних фізичних симптомів та захворювань, таких як епілептичні напади та нудота, при частому та довготривалому користуванню системи ВР.

Також, вказує і на те, що поведінкові ризики включають можливість виникнення неприйнятних поведінкових моделей, таких як стеження та деанонімазація (розкривання та розповсюдження персональних даних), у віртуальних середовищах. Вони потребують уваги з боку компаній, які використовують віртуальну реальність для навчання або комунікації з клієнтами.

Важливо заздалегідь визначили рівень моніторингу і сповістили про цю політику співробітників або клієнтів. Порушення конфіденційності

може мати серйозні правові наслідки для компаній, тому вони повинні звернутися до юридичних консультантів, щоб уникнути можливих судових питань.

Автор вважає, що у сфері інформаційної безпеки, віртуальна реальність може створювати загрози для конфіденційності даних та комунікацій, оскільки відкриті, публічно доступні, віртуальні середовища можуть бути причиною масштабних витоків персональних даних, через потенційні проблеми з існуючими недоліками та програмними вразливостями систем.

Результати дослідження та їх обговорення. Віртуальна реальність (ВР) є однією з найбільш захоплюючих і стрімко зростаючих технологій нашого часу, оскільки занурення у різноманітні, хоть і нереальні, світи, здатні повністю поглинути увагу користувача та залишити незабутні враження та, навіть, нові знання у як сферах відпочинку та розваг, так і освіти, медицини та й інших галузях.

Однак, поряд з незаперечними перевагами, системи ВР також несуть певні ризики для фізичної безпеки користувачів та їхніх конфіденційних даних.

Через високий рівень занурення у віртуальне середовище, існує ризик фізичних травм для людини та пошкоджень для застосованих технічних засобів, внаслідок невдалих рухів або зіткнень з предметами [5]. Необхідно ретельно продумати захист користувачів від таких ситуацій за допомогою відповідного розташування обладнання, інструкцій, попереджень, а також примінення додаткових засобів для забезпечення захисту від потенційних ушкоджень.

Одним із ключових аспектів забезпечення фізичної безпеки користувачів віртуальної реальності є правильна організація фізичного простору, в якому буде використовуватися дана система. Ретельна підготовка приміщення має вирішальне значення для створення безпечного

та комфортного середовища для занурення користувача у віртуальну реальність.

Для безпечного використання рішень ВР необхідно виділяти достатній вільний простір навколо користувача. Рекомендована мінімальна площа повинна становити не менше ніж 3х3 метри, даний простір повинен бути звільнений від меблів, декоративних елементів, кутів або інших предметів, об які користувач може травмуватися під час переміщень у віртуальному середовищі [6] (рис. 1).

Важливо, щоб розміри приміщення дозволяли користувачу вільно рухатися, не наражаючись на небезпеку зіткнення з фізичними перешкодами.

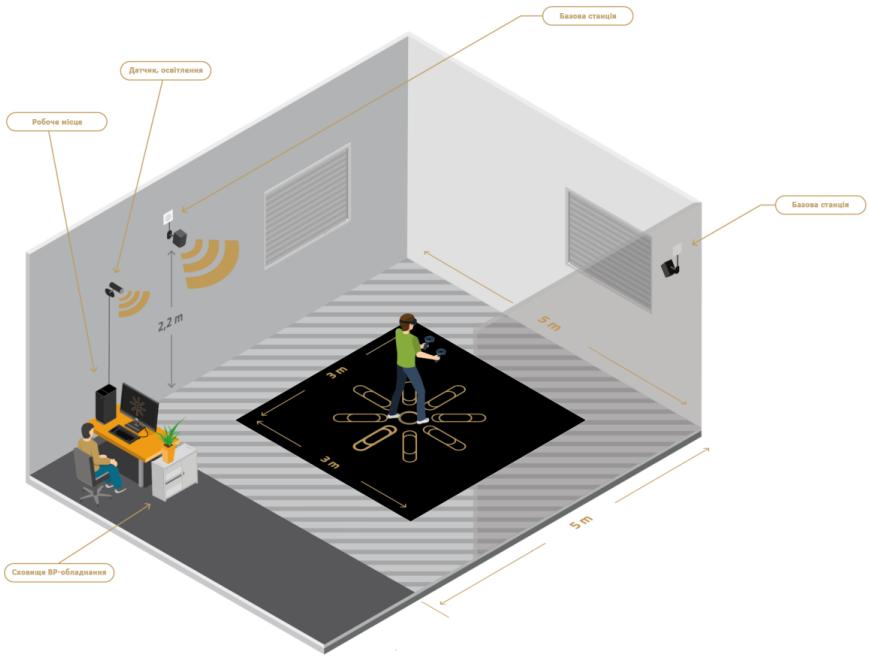

Рис. 1. Приклад планування кімнати для безпечного застосування ВР-систем [6]

Джерело: відредаговано автором

Крім виділення достатнього простору, необхідно ретельно дослідити приміщення та усунути будь-які предмети, що можуть становити потенційну небезпеку для користувача. До таких об'єктів належать:

- гострі кути меблів, виступи на стінах, декоративні елементи, оскільки вони можуть стати причиною травмування при випадковому зіткненні;.

- сходи, перепади висоти підлоги, нерівності поверхні, що можуть збільшувати ризик спотикання та падіння користувача;

- нестійкі, рухомі або легкі предмети, які можуть бути зрушені або перекинуті під час рухів у віртуальному середовищі.

Усунення або належне екранування таких потенційно небезпечних предметів є необхідним для забезпечення безпеки користувачів.

Ще одним важливим аспектом підготовки приміщення є забезпечення достатнього та рівномірного освітлення, що дозволить краще орієнтуватися у фізичному просторі навіть під час повного занурення у віртуальну реальність.

Надмірна темрява чи різка зміна освітленості можуть викликати дискомфорт та збільшити ризик травмування, тому приміщення повинно бути рівномірно освітлене природним або штучним світлом, без темних кутів або різких світлотіней.

Використання додаткових джерел світла, наприклад, спрямованих прожекторів або світлодіодних стрічок, може допомогти створити оптимальні умови освітлення для безпечного використання ВР-систем.

Додатковим аспектом забезпечення фізичної безпеки користувачів у системах віртуальної реальності є чітке визначення та контроль меж безпечної віртуальної зони. Це дозволяє запобігти ситуаціям, коли користувач випадково виходить за межі встановленого простору і наражається на небезпеку зіткнення.

Застосовуючи популярне, наявне, рішення гарнітури віртуальної реальності Oculus Quest 2 можна навести приклад реалізації контролю меж безпечної зони. Дане обладнання (шолом та контролери) оснащене високоточною системою відстеження положення (трекінгу) у фізичному

просторі, воно використовує вбудовані камери, які постійно аналізують навколишнє середовище, щоб визначити оптимальну безпечну зону для користувача [7].

Спочатку, під час першого налаштування системи, Oculus Quest 2 пропонує окреслити межі безпечної віртуальної зони. Це можна зробити за допомогою контролерів, обводячи по підлозі периметр, в якому планується застосовувати дану гарнітуру (рис. 2). Система аналізує отриману інформацію та визначає розмір і форму безпечної зони з урахуванням особливостей приміщення. Цікавою особливістю даного методу є відображення зображення з камер шолому для створення віртуальної зони самим користувачем в режимі змішаної реальності (віртуальні об'єкти накладаються на проекцію реального світу).

Рис. 2. Застосування режиму безпечної зони

Джерело: створено автором

Вбудовані камери шолома відстежують положення людини та її наближення до встановлених меж. Якщо користувач починає наближатися до кордонів безпечної зони, тоді система подає йому відповідне попередження. Це може бути у вигляді напівпрозорих віртуальних стін на периферії зору, що вказують на наближення до меж, або спеціальних звукових сигналів. Воно дає змогу користувачеві вчасно скоригувати своє переміщення і не вийти за межі безпечної зони.

Варто зазначити, що крім Oculus Quest 2, аналогічні механізми контролю безпечної зони застосовуються і в інших сучасних ВР-системах, наприклад Oculus Rift, HTC Vive, Valve Index та PlayStation VR/VR2. Незалежно від виробника, ця функціональність є ключовою для забезпечення комфортного та безпечного досвіду використання технологій віртуальної реальності.

Ще одним важливим аспектом фізичної безпеки є підготовка поверхні підлоги. Вона має бути рівною та нековзною, щоб запобігти спотиканню та падінню користувача під час переміщень у віртуальному середовищі.

Нерівності, вибоїни або слизькі ділянки на підлозі становлять потенційну небезпеку для користувача. Тому перед використанням приміщення необхідно усунути всі нерівності, наклеїти протиковзкі покриття або килимки.

За можливості, доцільно використовувати спеціальні м'які підлогові покриття, такі як татамі або гумові мати. Вони не тільки запобігають травмуванню, але й додають комфорту під час переміщень у віртуальному середовищі.

Необхідно завжди відокремлювати зону використання ВР, від інших частин приміщення, застосовуючи, наприклад, фізичні бар'єри. Це можуть бути, предмети з м'яких матеріалів, таких як килимки або гумові бортики, оскільки, такі бар'єри допомагають чітко визначити безпечні межі простору, в якому дозволено переміщатися користувачу.

Усі вищезазначені заходи щодо підготовки приміщення необхідно розглядати в комплексі. Лише комбінація правильно організованого фізичного простору, усунення потенційно небезпечних предметів, забезпечення належного освітлення та нековзної підлоги, а також виокремлення безпечної зони використання ВР дозволить створити максимально безпечне середовище для занурення користувачів у віртуальну реальність.

Інші важливі заходи, такі як правильний менеджмент кабелів та застосовування захисних спеціальних аксесуарів, також необхідно впроваджувати в комплексі для максимальної ефективності.

Ретельний контроль за прокладеними кабелями є дуже важливим, адже неправильне розміщення або їх переплетення, може становити серйозну небезпеку, спричинити спотикання, падіння або інші травми.

Необхідно враховувати довжину та тип кабелів, що використовуються для підключення різноманітних компонентів, наприклад шолому до робочої станції чи комп'ютера.

Найкращим рішенням є використання універсального кабелю (рис. 3), довжиною від 5 метрів, з можливістю передавати необхідне, для роботи гарнітури, живлення (хорошим показником вважається напруга 5В (вольт) (з допустимою похибкою 0.25В), та сила струму 2, і більше, А (ампер), тобто опором менше рівному 2.5Ом) та швидким стандартом обміном інформацією, наприклад, стандарту USB (Universal Serial Bus, універсальна послідовна шина) 3.1 Gen 1 (гарантує швидкість провідної передачі 5Гбіт/с, гігабіт на секунду, мільярдів біт в секунду).

Рис. 3. Приклад закріпленого кабелю, що використовується для підключення до ВР-гарнітури, довжиною 5 метрів, з можливістю передачі даних зі швидкістю 10Гбіт/с (стандарту USB 3.1 Gen 2) та потужністю живлення 10.5W (ват, тобто силою стуму заряджання 2.1А, при напрузі 5В)

Джерело: створено автором

Необхідно ретельно планувати положення всіх проводів та фіксувати їх місця будь-яких підключень. Доцільно використовувати спеціальні кабельні канали або кріплення, які дозволяють надійно зафіксувати кабелі та приховати їх з-під ніг користувача. Це допомагає уникнути заплутування кабелів і мінімізує ризик того, що користувач може спіткнутися об них під час переміщення у віртуальному просторі.

Ще одним важливим аспектом забезпечення фізичної безпеки в системах віртуальної реальності є застосування спеціальних аксесуарів, які підвищують комфорт та захищеність користувачів.

М'який силіконовий чохол, який можна встановити на корпус шолома, дозволяє покращувати ергономіку та комфорт носіння (рис. 4). Його матеріал має амортизуючі властивості, що дозволяє пом'якшувати можливі удари, захищає конструкцію від подряпин, потертостей та інших пошкоджень, які можуть виникнути під час активного використання ВР-системи.

Додатковим аксесуаром для забезпечення безпеки користувачів є спеціальні м'які накладки або чохли для контролерів (рис. 4). Вони виконують кілька важливих функцій: пом'якшують удари у разі випадкового зіткнення контролерів з навколишніми предметами, захищаючи руки користувача від травм, , зменшують ризик появи подряпин або інших пошкоджень на самих контролерах, подовжуючи їх термін служби.

Крім того, більшість контролерів надають можливість для кріплення та застосування зап'ястних ремінців (рис. 4), що дозволяють надійно фіксувати контролери на руках користувача, виключаючи можливість їх випадкового випадання або вислизання з рук під час активних сесій.

Рис. 4. Захисні аксесуари для шолому та контролерів гарнітури ВР

Джерело: створено автором

Використання спеціальних аксесуарів суттєво підвищує рівень фізичної безпеки для користувачів, адже вони забезпечують захист найбільш вразливих частин тіла (голова, руки, ноги людини) від травм, одночасно покращуючи зручність та комфорт використання.

Забезпечення програмної безпеки, також, відіграє критичну роль при розробці та експлуатації систем віртуальної реальності. Адже ці системи оперують значними обсягами конфіденційної інформації, пов'язаної з користувачами, що робить їх привабливою ціллю для зловмисників.

Одним із важливих аспектів кібербезпеки ВР-систем є організація надійних підключень між компонентами. Тут можна виділити два основні типи з'єднань: провідне та бездротове.

Провідне підключення, засноване на використанні фізичних кабелів, як правило, забезпечує більш стабільний та надійний зв'язок між шоломом, контролерами та іншими пристроями ВР. Завдяки своїй фізичній природі, такі підключення є менш вразливими до перехоплення даних порівняно з бездротовими каналами. Однак, наявність кабелів накладає додаткові вимоги на організацію кабельного простору, що було описано раніше.

Необхідно приділяти увагу акуратному прокладенню та фіксації кабелів, щоб уникнути ризиків спотикання або пошкодження обладнання.

Бездротове підключення, яке активно використовується в сучасних ВР-системах, забезпечує більшу мобільність та свободу переміщення користувача у віртуальному просторі. Відсутність фізичних кабелів робить систему більш зручною та зменшує ризик фізичних ушкоджень. Однак, бездротові канали передачі даних, такі як Wi-Fi або Bluetooth, не здатні на передачу живлення до гарнітури ВР, а також є потенційно більш вразливими до перехоплення трафіку зловмисниками.

Для забезпечення належного рівня програмної безпеки в системах віртуальної реальності необхідно реалізувати надійні механізми шифрування даних. Це стосується як передачі інформації між компонентами ВР-системи, так і зберігання даних на серверах.

Оскільки забезпечення належного рівня шифрування даних є критично важливим аспектом кібербезпеки, дані, що генеруються та обробляються в таких системах, можуть містити конфіденційну інформацію користувачів [2; 3; 4].

Для забезпечення максимального рівня безпеки, шифрування даних необхідно реалізувати на двох ключових рівнях: під час передачі між компонентами системи ВР та під час зберігання на серверах.

На етапі передачі даних доцільно використовувати сучасні криптографічні протоколи, такі як TLS (Transport Layer Security) або SSL (Secure Sockets Layer). Ці рішення дозволяють забезпечити конфіденційність та цілісність інформації, яка циркулює між шоломом, контролерами, робочою станцією чи іншими пристроями, що взаємодіють у межах ВР-системи. Застосування TLS/SSL-шифрування є особливо критичним для бездротових ВР-систем, де дані передаються через Wi-Fi (Wireless Fidelity, загальновживана назва для стандарту IEEE 802.11,

застосовується для безпровідної передачі інформації) або Bluetooth-канали, які потенційно можуть бути перехоплені зловмисниками [8].

Крім того, необхідно подбати про надійне шифрування даних, що зберігаються на серверах, задіяних у функціонуванні систем. Це стосується як локального обладнання, встановленого безпосередньо в приміщенні, так і можливих хмарних сховищ, куди може передаватися певна частина інформації.

Для шифрування даних на серверах доцільно використовувати сучасні криптографічні алгоритми, такі як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) або DES (Data Encryption Standard). Ці рішення забезпечують надійний захист даних, гарантуючи, що навіть у разі компрометації серверів, зловмисники не зможуть отримати доступ до конфіденційної інформації [9].

Особливу увагу необхідно приділити безпеці шифрувальних ключів, які використовуються для криптографічного захисту даних. Ключі повинні зберігатися в надійному сховищі, мати обмеження доступу та регулярно оновлюватися. Це дозволяє виключити можливість їх компрометації зловмисниками, що могло б поставити під загрозу безпеку всієї системи.

Забезпечення належного контролю та управління доступом до серверів, на яких розгортаються системи віртуальної реальності є, також, важливим елементом кібербезпеки. Для ефективного контролю доступу до серверів, необхідно впровадити надійну систему ідентифікації та авторизації користувачів [1]. Це може включати в себе використання багатофакторної автентифікації, поєднуючи традиційні паролі з біометричними даними (наприклад, відбитки пальців) або одноразовими кодами. Таким чином, доступ до критичних компонентів системи буде обмежений лише для авторизованих осіб, що значно підвищує рівень захисту.

Часто ВР-додатки вимагають швидкого та безперебійного доступу до хмарних або віддалених серверів для забезпечення плавного та реалістичного досвіду. Однак, під час атак, наприклад, таких, що спрямовані на відмову в обслуговуванні, DDoS (Denial-of-Service, Distributed), система може бути перевантажена великою кількістю фіктивного трафіку, що може призвести до уповільнення роботи або повної відмови роботи її компонентів [4].

Зловмисники можуть використовувати різноманітні методи для здійснення DDoS-атак, наприклад, викрадені або зараженні пристрої, які утворюють ботнет – мережу скомпрометованих пристроїв, які керуються централізовано та використовуються для відправки великої кількості запитів на цільову систему. Поширеним методом є атаки з використанням підроблених IP-адрес або техніки відбиття, коли запити надсилаються через треті сторони, ускладнюючи відстеження джерела атаки [10].

Хмарні провайдери, такі, як AWS (Amazon Web Services), GCP (Google Cloud Platform), Microsoft Azure та DigitalOcean, пропонують власні рішення та інструмент для захисту від DDoS-атак.

Існує доволі популярне рішення від Amazon під назвою AWS Shield, що забезпечує постійний моніторинг трафіку та автоматичне виявлення й ліквідацію найпоширеніших типів атак, таких як атаки на рівні мережі та транспортного рівня, використовує глобальну мережу для розподілу трафіку та запобігання перевантаженню [11].

Хоча хмарні провайдери пропонують потужні інструменти для боротьби з DDoS-атаками (приклад роботи сервісу AWS Shield з запобігання та захисту від шкідливого трафіку зображений на рисунку 5), їх ефективність значною мірою залежить від правильної конфігурації та налаштування. Розробники та адміністратори систем віртуальної реальності повинні ретельно вивчати рекомендації, слідкувати за оновленнями безпеки та своєчасно впроваджувати необхідні заходи захисту.

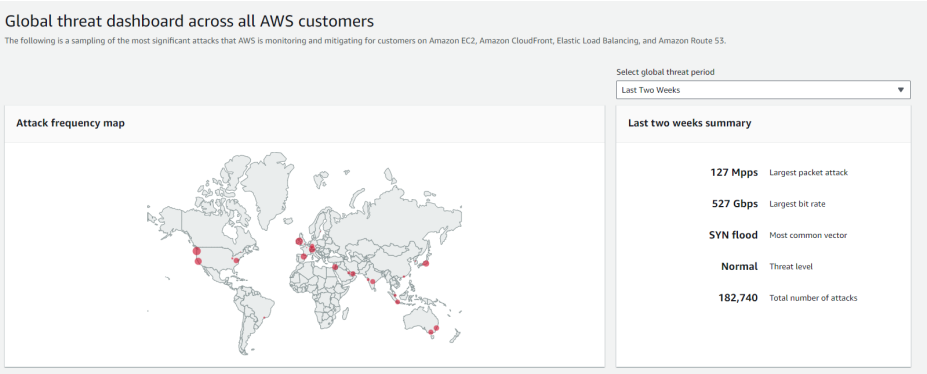

Рис. 5. Статистика атак та їх запобігання системою AWS Shield [12]

Ще одним елементом запобіганню атак є встановлення брандмауерів та налаштування мережевих портів на серверах. Вони дозволяють обмежити можливості зловмисників, виявляючи та блокуючи підозрілу активність, оскільки ретельне налаштування та контроль мережевих портів допомагає мінімізувати ризик несанкціонованого доступу.

Для кращої наглядності та підтвердження ефективності використання інструментів кіберзахисту, було проведено невеликий експеримент, використовуючи рішення хмарного провайдера AWS.

Створено віртуальну машину (рис. 6) зі встановленим рішенням Lighttpd (доволі популярне програмне забезпечення, що використовується для взаємодії та відображення мережевого контенту), налаштованим на очікування, обробку та надсилання HTTP (HyperText Transfer Protocol, протокол передачі гіпертекстових документів) та HTTPS (HyperText Transfer Protocol Secure, протокол передачі гіпертекстових документів з використанням додаткового шару шифрування та автентифікації) запитів.

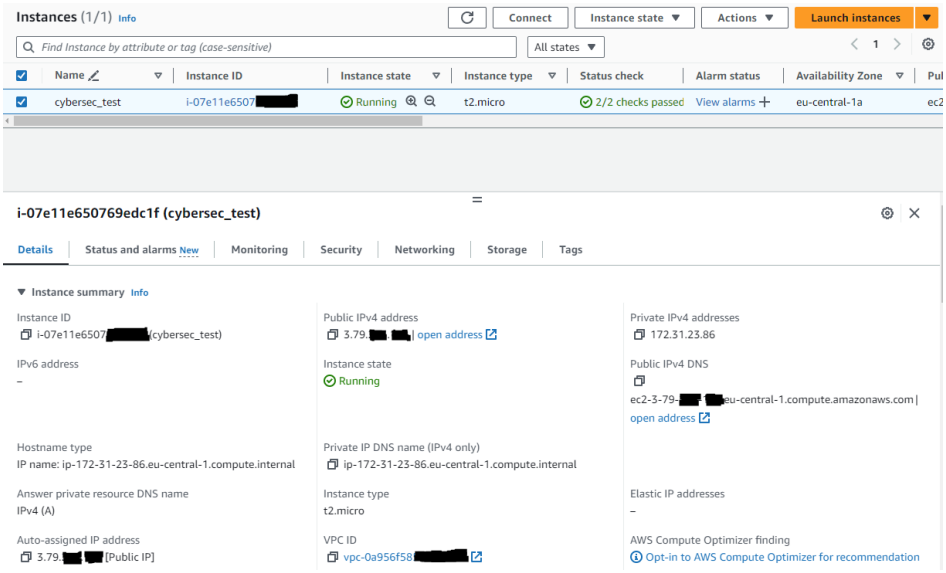

Рис. 6. Запущена віртуальна машина

Джерело: створено автором

На комп'ютері, що виконував роль атакуючого, завантажено та інстальоване популярне рішення Zenmap, що дозволяє виконувати сканування всіх викритих портів та отримувати інформацію про віддалений сервер.

В результаті сканування (рис. 7), Zenmap не тільки повідомив про відкриті порти (22, 8080), через які можна виконувати з'єднання та атаки, а й тип та версію операційної системи (Linux-based, Ubuntu), встановленого програмного забезпечення Lighttpd (жодних, вказаних раніше, заходів додаткової програмної безпеки використано не було).

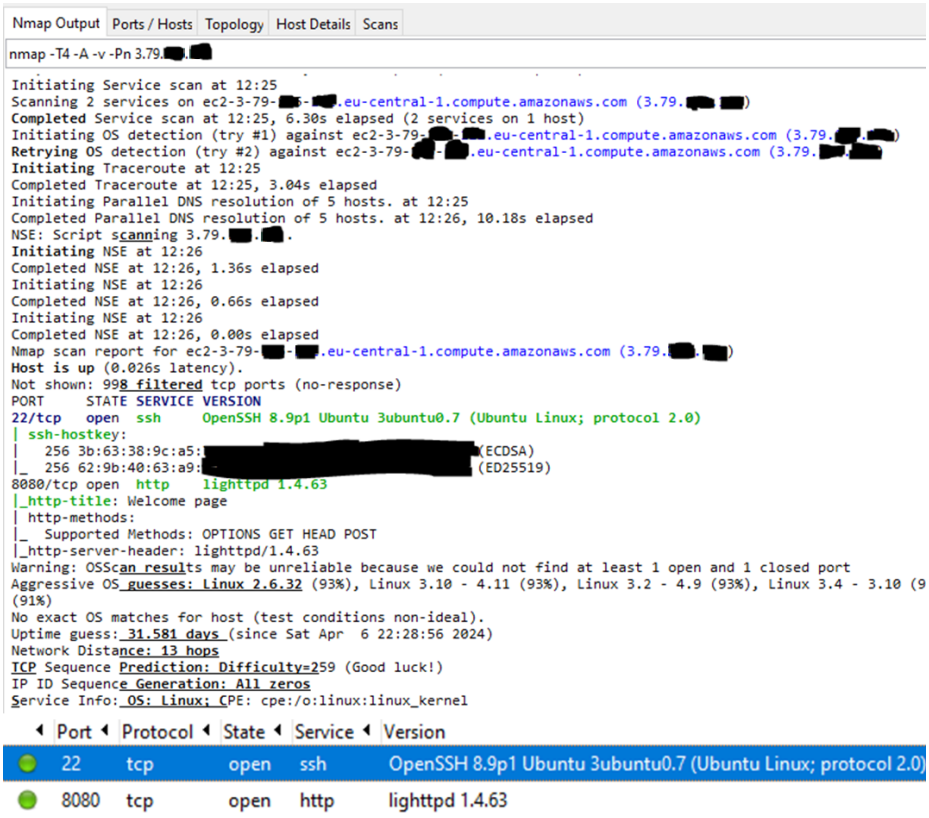

Рис. 7. Результати сканування віддаленого сервера

Джерело: створено автором

Отриманий результат показав, що вдалося знайти версію встановлених програмних компонентів рішення, в яких були виявлені недосконалі частини програмного коду, вразливості CVE-2022-41556 (Common Vulnerabilities and Exposures, ідентифікатор запису в базі даних загальновідомих проблем інформаційної безпеки), CVE-2022-30780, CVE-2022-22707, які дозволяли зловмисникам викликати відмову в обслуговуванні всієї системи [13].

Продовжуючи експеримент, використовуючи засоби платформи AWS та сервісу Security Group було створено правила безпеки для вбудованого брандмауера, обмежено доступ до мережевих портів (рис. 8) та запущено повторене сканування на комп'ютері, що виконує роль атакуючого.

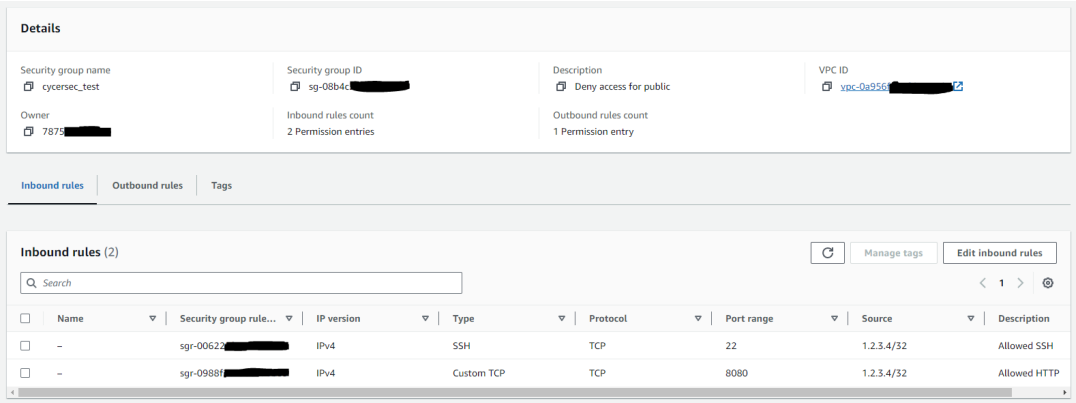

Рис. 8. Примінені правила брандмауера

Джерело: створено автором

Після застосування нових правил брандмауера, що дозволяють виконувати підключення тільки для вказаних джерел та мережевих адрес, Zenmap не зміг виконати аналіз та відобразити потенційно небезпечну інформацію (рис. 9).

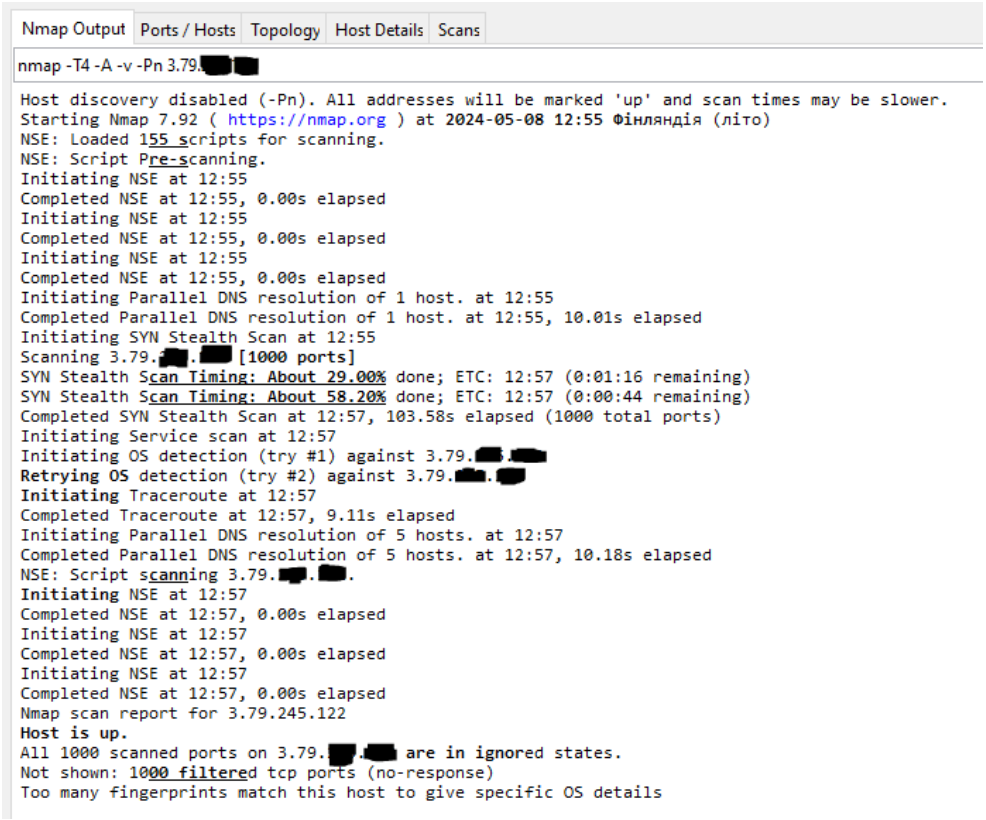

Рис. 9. Результат повторного сканування, після додаткового засобу програмної безпеки

Джерело: створено автором

Отже, проведений експеримент наочно демонструє важливість застосування належних засобів кібербезпеки для захисту інформаційних систем та ресурсів. Спочатку, без додаткових захисних заходів, сканування віддаленого сервера дозволило отримати чутливу інформацію про операційну систему, відкриті порти та версії встановленого програмного забезпечення, що може бути використано зловмисниками для виявлення та експлуатації вразливостей. Однак, після застосування брандмауера з відповідними правилами доступу, повторне сканування не змогло виявити жодної корисної інформації про систему. Це підтверджує, що належне налаштування та використання засобів кіберзахисту, таких як брандмауери, є критично важливим для забезпечення безпеки інформаційних ресурсів та систем, оскільки ефективно перешкоджає зловмисникам у збиранні розвідувальних даних та потенційних спробах атак.

Висновок. Забезпечення фізичної та програмної безпеки є невід'ємною складовою успішного впровадження та використання систем віртуальної реальності.

Передусім, під час роботи з ВР-системами необхідно ретельно підготувати фізичне середовище, у якому буде використовуватися обладнання. Це включає виділення достатньої вільної площі, усунення перешкод, забезпечення належного освітлення та наявності додаткових орієнтирів для полегшення орієнтації користувача у реальному просторі.

Додаткову увагу слід приділяти питанню правильного розташування та менеджменту кабелів, які можуть становити загрозу для користувачів, створюючи ризики спотикання чи заплутування. Доцільно використовувати спеціальні кабельні канали, кріплення та інші пристрої для організації та захисту кабелів. Також, використовувати рішення, що дозволяють відстежувати положення користувача, для визначення меж безпечної зони та попередження про потенційні загрози у реальному часі.

Важливим аспектом є використання спеціальних аксесуарів та пристосувань, призначених для роботи з ВР-системами. Зокрема, рекомендується застосовувати м'які силіконові чохли та накладки для шоломів і контролерів, а також зап'ясні ремінці для запобігання випадковому випусканню контролерів з рук.

Забезпечення належного рівня кібербезпеки системи є одним з головних факторів при проектуванні та застосування рішень віртуальної реальності, необхідно вживати заходів для захисту конфіденційності та цілісності інформації.

Передусім, застосовувати надійне шифрування даних, як під час їх передачі через мережі, так і в стані спокою на серверах. Це дозволить запобігти несанкціонованому доступу та перехопленню конфіденційної інформації, використовувати брандмауери та забезпечити можливість віддаленого контролю для оперативного реагування на інциденти та загрози.

У випадку використання хмарних сервісів для зберігання даних, слід ретельно проаналізувати рівень захисту, який вони забезпечують, та розглянути можливість додаткового шифрування даних перед їх передачею до хмарного сховища. Альтернативним рішенням може бути використання власних захищених серверів.

Загалом, питання фізичної безпеки та кібербезпеки у системах віртуальної реальності перебувають у постійному розвитку, оскільки самі технології ВР швидко вдосконалюються, а методи атак і загрози стають все більш складними. Тому розробники та дослідники повинні постійно відстежувати нові тенденції, вивчати передовий досвід і впроваджувати передові рішення для забезпечення максимально безпечного та комфортного досвіду використання.

Література

1. Viswanathan, K., Yazdinejad, A. (2022). Security considerations for virtual reality systems. arXiv preprint arXiv:2201.02563.

2. Kurtunluoglu, P., Akdik, B., Karaarslan, E. (2022). Security of virtual reality authentication methods in metaverse: An overview. arXiv preprint arXiv:2209.06447.

3. Lv, Z., Chen, D., Lou, R., Song, H. (2020). Industrial security solution for virtual reality. *IEEE Internet of Things Journal, 8*(8), 6273-6281.

4. Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., Hoque, K. A. (2019). Security, privacy and safety risk assessment for virtual reality learning environment applications. *16th IEEE Annual Consumer Communications & Networking Conf.* (pp. 1-9). 2019.

5. Korolov, M. (2014). The real risks of virtual reality. *Risk Management, 61*(8), 20-24.

6. ROOM REQUIREMENTS. (2024). *Innerspace*. URL: https://www.innerspace.eu/requirements/room-requirements/ (date of access: 10.05.2024).

7. Oscillada, J. M, (2017). Oculus Introduces Guardian, A Boundary System For Touch. URL: https://virtualrealitytimes.com/2017/02/18/oculus-guardian-boundary-system (date of access: 10.05.2024).

8. Sirohi, P., Agarwal, A., Tyagi, S. (2016). A comprehensive study on security attacks on SSL/TLS protocol. *2nd International Conf. on next generation computing technologies* (pp. 893-898). 2016.

9. Hamza, A., Kumar, B. (2020). A review paper on DES, AES, RSA encryption standards. *9th International Conf. System Modeling and Advancement in Research Trends* (pp. 333-338). 2020.

10. Mirkovic, J., Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.

11. Routavaara, I. (2020). Security monitoring in AWS public cloud.

12 Global threat dashboard. (2024). *AWS.* URL: https://console.aws.amazon.com/wafv2/shieldv2/global_threat_dashboard (date of access: 10.05.2024).

13. Lighttpd: Security Vulnerabilities, CVEs. (2024). *CVEdetails.* URL: https://www.cvedetails.com/vulnerability-list/vendor_id-2713/Lighttpd.html (date of access: 10.05.2024).