Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кібербезпека
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Моделювання загроз безпеки навчальної системи з використанням доповненої реальності на основі Mitre Attack

Виконав: студент 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Ревура Д.С (прізвище та ініціали)

Керівник (підпис) Козак Р.О (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«___» _____ 2023 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Ревурі Дмитру Степановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Моделювання загроз безпеки навчальної системи з використанням доповненої реальності на основі Mitre Attack

Керівник роботи Козак Р.О., к.т.н., доцент каф. КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «3» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

АННОТАЦІЯ

Моделювання загроз безпеки навчальної системи з використанням доповненої реальності на основі Mitre Attack // Кваліфікаційна робота ОР «Бакалавр» // Ревура Дмитро Степанович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 69, рис. – 18, табл. – 3, бібліогр. – 25.

Ключові слова: ДОПОВНЕНА РЕАЛЬНІСТЬ, НАВЧАЛЬНА СИСТЕМА, АРХІТЕКТУРА, АТАКА, ЗАГРОЗА, ВЕКТОР АТАК, БЕЗПЕКА, MITRE ATT&CK.

Метою даної роботи є моделювання загроз безпеки для навчальної системи з використанням доповненої реальності на основі Mitre Attack.

Об'єкт дослідження – навчальна система з використанням технології доповненої реальності.

Предмет дослідження – загрози безпеки для навчальної системи з використанням доповненої реальності та методи їх моделювання на основі Mitre Attack.

В кваліфікаційній роботі проведено огляд доповненої реальності, побудовано узагальнену архітектуру навчальної системи з використанням доповненої реальності, проведено аналіз її компонентів, побудовано вектори атак на важливі компоненти системи, змодельовано загрози безпеки для цієї системи основі Mitre Attack, а також розроблено рекомендації щодо заходів і засобів забезпечення безпеки навчальної системи від ідентифікованих загроз.

Результатом роботи є побудована модель загроз для навчальної системи з використанням доповненої реальності на основі Mitre Attack.

Для реалізації даної роботи були використані такі програмні продукти: MITRE ATT&CK Navigator, Draw.io.

ABSTRACT

Modeling security threats to an educational system using augmented reality based on Mitre Attack // Qualification work for a Bachelor's degree // Revura Dmytro Stepanovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer and Information Systems and Software Engineering, Department of Cybersecurity, SB-41 group // Ternopil, 2023 // p. 69, fig. - 18, tab. - 3, bibl. - 25.

Keywords: AUGMENTED REALITY, EDUCATIONAL SYSTEM, ARCHITECTURE, ATTACK, THREAT, ATTACK VECTOR, SECURITY, MITRE ATT&CK.

The purpose of this work is to model security threats to an educational system using augmented reality based on Mitre Attack.

The object of research is an educational system that utilizes augmented reality technology.

The subject of research is security threats to an educational system using augmented reality and methods of modeling these threats based on Mitre Attack.

In the qualification work, an overview of augmented reality is conducted, a generalized architecture of an educational system using augmented reality is constructed, an analysis of its components is carried out, attack vectors on important system components are constructed, security threats to this system are modeled based on Mitre Attack, and recommendations for security measures and means for the educational system against identified threats are developed.

The result of the work is a constructed threat model for an educational system using augmented reality based on Mitre Attack.

The following software products were used for the implementation of this work: MITRE ATT&CK Navigator, Draw.io.

ЗМІСТ

ВСТУП

Сучасний швидкий розвиток технологій приводить до впровадження нових інноваційних рішень у різних сферах життя, включаючи освіту. Однією з таких технологій є розширена реальність (Augmented Reality - AR), яка володіє значним потенціалом для вдосконалення навчальних процесів. Системи доповненої реальності поєднують в собі віртуальні об'єкти з реальним оточенням, надаючи унікальні можливості для інтерактивного навчання та сприяючи залученню студентів до активного процесу освоєння матеріалу.

Актуальність теми даної дипломної роботи обумовлена широким впровадженням систем доповненої реальності в освітній процес. З одного боку, ця технологія надає можливості для покращення ефективності навчання та залучення студентів до активної діяльності. З іншого боку, використання систем доповненої реальності вимагає врахування аспектів безпеки, оскільки вони можуть стати об'єктом атак з боку зловмисників, загрожуючи конфіденційності, цілісності та доступності навчальної інформації.

Метою даної дипломної роботи є моделювання загроз безпеки навчальної системи з використанням доповненої реальності на основі фреймворку MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge). MITRE ATT&CK надає комплексний опис методів, тактик та прийомів, які використовуються зловмисниками для здійснення атак. Цей фреймворк дозволяє ідентифікувати потенційні загрози безпеки та розробляти відповідні заходи для їх запобігання.

Об'єктом дослідження дипломної роботи є навчальна система з використанням доповненої реальності. Предметом дослідження є моделювання загроз безпеки в цій системі на основі фреймворку MITRE ATT&CK. Аналізуючи підходи до моделювання загроз та застосовуючи фреймворк MITRE ATT&CK, робота включає розробку заходів та засобів забезпечення безпеки, які допоможуть запобігти можливим атакам у системі доповненої реальності.

Наукове значення даної роботи полягає у вдосконаленні методів забезпечення безпеки навчальних систем з використанням доповненої реальності. Результати дослідження сприятимуть створенню більш надійних та захищених

систем, які можуть бути успішно використані в освітніх установах. Практичне значення полягає у можливості використання розроблених заходів та засобів забезпечення безпеки для запобігання потенційним атакам та зловживанням у навчальних системах з використанням доповненої реальності.

Робота складається з трьох розділів. У розділі 1 досліджується технологія доповненої реальності, її визначення та характеристики, а також розглядається використання систем доповненої реальності в освітніх цілях. Розділ 2 присвячений архітектурі навчальної системи з використанням доповненої реальності, проводиться аналіз існуючих навчальних систем і надається узагальнена архітектура такої системи. У розділі 2.3 обговорюється важливість забезпечення безпеки навчальних систем з використанням технології доповненої реальності. У розділі 3 розглядається застосування фреймворку MITRE ATT&CK для моделювання загроз безпеки в системі доповненої реальності. Проводиться аналіз підходів для моделювання загроз безпеки, досліджується фреймворк MITRE ATT&CK та описується його застосування для моделювання загроз. Крім того, розділ 3.4 пропонує розробку заходів та засобів забезпечення безпеки, які допоможуть у попередженні та нейтралізації потенційних атак у системі доповненої реальності.

Робота вирішує актуальну проблематику забезпечення безпеки навчальних систем з використанням доповненої реальності, пропонує нові підходи до моделювання загроз та розробку заходів забезпечення безпеки. Розв'язані задачі галузі сприятимуть підвищенню рівня безпеки та довіри до систем доповненої реальності, що використовуються в освітньому процесі.

РОЗДІЛ 1 СИСТЕМИ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

1.1 Технології розширеної реальності

У сучасному цифровому світі, де інформаційні технології прискорюють свій розвиток, однією з найперспективніших і революційних технологій є технології розширеної реальності. Розширена реальність (Augmented Reality, AR), віртуальна реальність (Virtual Reality, VR) та змішана реальність (Mixed Reality, MR) вже активно використовуються в багатьох сферах життя, включаючи освіту, медицину, розваги та промисловість (див. рисунок 1.1).

Рисунок 1.1 – Технології розширеної реальності

Віртуальна реальність (VR) – це технологія, що створює симульоване середовище, замінюючи реальний світ вигаданим. Ця технологія занурює користувача в повністю віртуальний світ, в якому він може взаємодіяти з віртуальними об'єктами і сценами. За допомогою VR, люди можуть відвідувати віртуальні музеї, переглядати тривимірні фільми, грати в ігри, навчатися і навіть проводити віртуальні зустрічі. Основним характеристиками VR є занурення у віртуальну навколишню реальність, сенсорний зворотний зв'язок, інтерактивність. Процес занурення забезпечується за допомогою спеціального обладнання, такого як шоломи віртуальної реальності (наприклад, Oculus Rift, HTC Vive) та рукавиці з трекерами руху. Основними сферами застосування VR є ігрова індустрія та

розваги, проте можливості VR набагато ширші. В освітніх цілях VR дозволяє створювати симуляції реальних ситуацій для навчання студентів. Також VR активно використовується у медицині, навчанні хірургів, психотерапії та реабілітації пацієнтів.

На відміну від віртуальної реальності, доповнена реальність (AR) накладає віртуальні об'єкти на реальне середовище користувача. Це означає, що користувач бачить реальний світ, який доповнено віртуальними елементами, що відображаються на екрані смартфона або спеціальних AR-окулярах. AR використовується в різних сферах, включаючи роздрібну торгівлю, освіту, медицину та ігрову індустрію. Наприклад, в роздрібній торгівлі AR може допомогти покупцям перевірити, як предмет меблів буде виглядати в їх домі, перш ніж вони здійснять покупку. У освіті, AR може допомогти студентам краще зрозуміти складні концепції, представивши їх у тривимірній перспективі. За допомогою AR, лікарі можуть отримати детальнішу інформацію про стан пацієнта, що може покращити якість медичного обслуговування.

Змішана реальність (MR) – це новітня технологія, яка поєднує елементи VR та AR, дозволяючи віртуальним та реальним об'єктам співіснувати та взаємодіяти в реальному часі. MR не просто накладає віртуальні об'єкти на реальний світ, але й дозволяє цим об'єктам взаємодіяти з реальним світом. Одним з прикладів застосування MR є Microsoft HoloLens, пристрій, що використовується для демонстрації віртуальних 3D-проектів у реальному світі. Ця технологія може бути використана в таких сферах, як освіта, медицина, архітектура, інженерія та ігрова індустрія.

Усі ці технології, VR, AR та MR, відкривають нові можливості для взаємодії з цифровим контентом і впливають на те, як ми сприймаємо та взаємодіємо з реальним світом. Вони продовжують розвиватися, створюючи нові способи використання та вдосконалення вже існуючих технологій.

1.2 Визначення та характеристики систем доповненої реальності

Системи доповненої реальності (AR) — це технології, що накладають комп'ютерно-генеровану інформацію (наприклад, зображення, звук, відео, GPS-дані тощо) на реальний світ, тим самим доповнюючи його та дозволяючи користувачам сприймати цією інформацію одночасно з відчуттям реальності.

Ці технології відрізняються від віртуальної реальності (VR), яка повністю занурює користувача в цифрове середовище, та від змішаної реальності (MR), що забезпечує ще більш тісну інтеграцію між реальним та віртуальним світами, дозволяючи віртуальним об'єктам взаємодіяти з реальним середовищем.

Системи доповненої реальності обов’язково містять такі складові:

– Сенсори та камери для збору інформації про навколишнє середовище.

– Обчислювальний блок для обробки даних з сенсорів та камер.

– Технології відображення для постання віртуальних об’єктів перед очима користувача, що інтегровані в реальний світ.

– Віртуальні об'єкти, які додаються до реального світу і можуть бути сприйняті за допомогою AR пристроїв.

Системи доповненої реальності (AR) використовують ряд алгоритмів для різних функцій та завдань. Деякі з цих алгоритмів включають:

– Відстеження руху – алгоритми, які дозволяють системі визначати положення та рухи користувача або об'єктів у просторі.

– Розпізнавання об'єктів – алгоритми, що дозволяють системі розпізнавати конкретні об'єкти або шаблони у реальному світі.

– Відслідковування поверхонь – алгоритми, які дозволяють системі розпізнавати та відстежувати поверхні, такі як стіни, столи або підлога, для розміщення віртуальних об'єктів.

– Комп'ютерний зір – алгоритми, що дозволяють системі аналізувати та розуміти візуальну інформацію, включаючи розпізнавання форм, кольорів та текстур.

– Розпізнавання образів – алгоритм для визначення місця віртуальних об'єктів у реальному світі.

Системи доповненої реальності (AR) відкривають широкі можливості, що значно перевищують просте накладання віртуальних об'єктів на реальне середовище:

– Додавання віртуальних об'єктів до реального світу, серед яких може бути текст, зображення, відео, 3D моделі та багато іншого.

– Візуалізація даних в реальному часі для відображення динамічних даних, інтегруючи їх безпосередньо з реальним середовищем.

– 3D-моделювання.

– Взаємодія з віртуальними об'єктами в реальному світі.

– Розпізнавання об'єктів для більш реалістичної взаємодії між віртуальними та реальними об'єктами.

Технічні вимоги до систем AR залежать від конкретної системи та її застосування. Однак, загалом, системи доповненої реальності вимагають потужного обчислювального апарату, щоб забезпечити гладкість та високу якість візуалізації. Вони також вимагають високоякісних сенсорів та камер для збору даних про реальний світ. Ці дані можуть включати відео, зображення, геопросторові дані, дані про рух, звук та інше. Важливими є також ефективні алгоритми обробки даних, які можуть обробляти ці дані в реальному часі та інтегрувати віртуальні об'єкти з реальним середовищем.

Системи доповненої реальності активно взаємодіють з реальним світом. Вони використовують камери та сенсори для збору даних про реальне середовище, включаючи форму та розташування реальних об'єктів. Ці дані потім обробляються, щоб визначити, де і як додати віртуальні об'єкти. Наприклад, система AR може використовувати дані з камери та геопросторові дані для розміщення віртуального об'єкта на реальному столі в реальному часі. Цей процес вимагає високої точності та швидкості обчислень, щоб забезпечити неперервну і переконливу взаємодію між віртуальними та реальними об'єктами.

В цілому, системи доповненої реальності (AR) – це комплексні технології, які інтегрують віртуальні об'єкти та інформацію в реальне середовище в реальному часі. Вони використовують широкий спектр сенсорів та алгоритмів для збору, аналізу та обробки даних про реальний світ. AR відрізняється від віртуальної

реальності (VR) та змішаної реальності (MR) за своєю здібністю забезпечувати взаємодію з реальним світом, а не лише створювати повністю віртуальне середовище або комбінувати реальні та віртуальні об'єкти. Вони відкривають широкі можливості, включаючи візуалізацію даних в реальному часі, 3D-моделювання, розпізнавання об'єктів та багато іншого, також можуть знайти застосування в різноманітних областях, від ігрової індустрії до медицини, науки, освіти, індустрії, архітектури та інших сферах, вимагаючи потужне обчислювальне забезпечення, високоякісні сенсори та камери, а також ефективні алгоритми обробки даних. Системи AR представляють собою перспективне поле для подальших досліджень та розробок, і заслуговують на більш детальне вивчення та розуміння.

1.3 Використання систем доповненої реальності в освітніх цілях

Системи доповненої реальності (AR) відкривають нові перспективи в освіті, поєднуючи реальний світ із віртуальними елементами, тим самим підвищуючи зацікавленість учнів і покращуючи процес навчання. Використання систем доповненої реальності (AR) в освіті вже давно перестало бути просто теоретичною концепцією. Завдяки розвитку технологій і все більшому їх доступу, AR стає важливим інструментом, який може революціонізувати традиційний освітній процес.

Наводячи конкретний приклад використання AR для освіти, варто згадати про такі додатки як Google Expeditions, Anatomy 4D, Elements 4D. Додаток Google Expeditions надає величезну кількість віртуальних екскурсій, що дозволяє учням відвідати місця, куди вони не могли б відвідати в реальному житті. Це може включати все від віртуальних турів історичними пам'ятками до подорожей в космос або в глибини океану. Anatomy 4D дозволяє учням вивчати людське тіло в тривимірному форматі. Вони можуть досліджувати різні системи тіла, такі як кровообіг, нервова система, м'язи та інше, що допомагає зробити вивчення анатомії більш цікавим та відчутним. Elements 4D – додаток AR, що використовує віртуальні "блоки" елементів, які можуть бути комбіновані для демонстрації

хімічних реакцій, учні можуть досліджувати, як різні елементи взаємодіють, що допомагає їм краще зрозуміти хімічні процеси.

Процес використання доповненої реальності (AR) в освіті передбачає детальне планування, розробку, впровадження та оцінювання. Наведена на рисунку 1.2 схема надає загальний огляд кроків, які потрібно виконати для успішної інтеграції AR в освітній процес.

На першому етапі – плануванні – визначаються навчальні цілі, які можуть бути досягнуті за допомогою AR. Завданнями цього етапу є конкретизація та формулювання цілей, а також вибір підходящих тем або предметів, де використання AR може найбільше сприяти навчанню. Додатково, на цьому етапі визначаються технічні вимоги та засоби, необхідні для успішного впровадження AR в освітній процес.

Другий етап – розробка – фокусується на створенні або виборі відповідних AR-додатків або програм для навчання. Це включає розробку або вибір контенту, який буде використовуватися в AR-середовищі. Контент може включати в себе візуальні елементи, текстові, аудіо та відеоматеріали, які допомагають студентам легше розуміти та запам'ятовувати матеріал. Під час цього етапу також проводиться забезпечення сумісності та оптимізація контенту для AR-платформ.

Третій етап – впровадження – передбачає підготовку студентів і вчителів до використання AR, а також проведення навчальних сесій з використання AR для учнів або студентів. На цьому етапі відбувається активне використання AR в навчальному процесі, де студенти мають можливість взаємодіяти з віртуальними об'єктами та сценаріями. Вчителі забезпечують підтримку та супровід студентів під час їхнього дослідження та навчання з використанням AR.

Останній етап – оцінювання – включає зібрання даних про продуктивність та результати навчання з використанням AR. Здійснюється аналіз отриманих даних для оцінки ефективності використання AR в освіті. Крім того, на цьому етапі враховується зворотний зв'язок від учнів або студентів щодо їхнього досвіду використання AR. Зворотній зв'язок допомагає виявити сильні сторони, а також можливі покращення та налаштування використання AR в навчанні.

Рисунок 1.2 – Процес впровадження AR в сфері освіти

Схема зображена на рисунку 1.2 відображає загальний процес впровадження AR в освіті, починаючи з планування та закінчуючи оцінюванням результатів. Вона показує, що успішна інтеграція AR в освітній процес вимагає ретельного підготування, розробки контенту та програм, а також систематичного оцінювання для постійного вдосконалення.

До можливостей та переваг застосування AR в освіті можна віднести такі:

– Інтерактивність та занурення. AR може впроваджувати новий рівень взаємодії в навчання, перетворюючи пасивне сприймання інформації на активне занурення. Учні можуть маніпулювати віртуальними об'єктами, вивчати їх з різних кутів і в масштабах, що сприяє кращому розумінню теми.

– Візуалізація складних концепцій. AR може допомогти учням краще зрозуміти складні абстрактні концепції, перетворивши їх на візуальні, тривимірні об'єкти. Це особливо корисно в таких науках, як фізика, хімія або біологія, де поняття можуть бути складними для візуалізації.

– Мотивація та зацікавленість. Використання AR може зробити процес навчання більш захоплюючим та мотивуючим, особливо для молодших вікових груп, які виростають в цифровий вік. Вона може перетворити навчання на гру, що в свою чергу може підвищити мотивацію та зацікавленість учнів.

– Доступ до недоступного. AR може дозволити учням вивчати предмети або сценарії, які зазвичай були б недоступними або небезпечними – від покрокового розібрання дорогого механічного пристрою до віртуальної екскурсії на Марс.

Зі всіма перевагами, використання AR в освіті має також і деякі обмеження у впровадженні:

– Технічні обмеження. На сьогоднішній день, AR все ще знаходиться на початковій стадії розвитку, і деякі технологічні обмеження можуть обмежувати її потенціал. Це може включати проблеми з точністю та стабільністю трекінгу, якість графіки, жорсткість апаратного забезпечення та обмежений рівень взаємодії.

– Обмежений доступ. Хоча технологія стає все більш доступною, не всі школи або учні можуть мати доступ до необхідного обладнання або ресурсів для використання AR в класі.

– Потреба в кваліфікованих вчителях. Щоб ефективно впроваджувати AR в навчання, вчителям потрібно мати відповідні навички та знання. Це може включати технічні знання для вирішення проблем, знання про те, як найкраще інтегрувати AR в уроки, і здатність креативно використовувати технологію для підвищення якості навчання.

Для кращого розуміння переваг та недоліків впровадження систем AR в освіті, створюю таблицю, описує переваги і недоліки використання доповненої реальності (AR) в освіті (див. таблицю 1.1).

Таблиця 1.1 – Переваги і недоліки використання AR в освіті

Переваги	Недоліки
Покращує залучення учнів до навчання	Потребує високої технічної підготовки та обладнання
Забезпечує інтерактивне навчання	Може бути витратним для освітніх установ та учнів
Стимулює сприйняття і запам'ятовування матеріалу	Може викликати відволікання та залежність від технології
Сприяє розвитку креативності та критичного мислення	Обмежує можливості спілкування обличчя в обличчя

Продовження таблиці 1.1

Переваги	Недоліки
Дозволяє візуалізувати абстрактні поняття	Вимагає налагодження та синхронізації засобів AR
Забезпечує індивідуалізований підхід до навчання	Може виникнути відчуття відсутності реального досвіду
Підвищує мотивацію та зацікавленість учнів	Можливі проблеми з конфіденційністю та безпекою даних
Сприяє взаємодії та співпраці між учнями	Потребує додаткового часу для підготовки та налагодження

У підсумку, системи доповненої реальності представляють значний потенціал для поліпшення якості та ефективності освітнього процесу. Вони можуть створювати більш іммерсивний та взаємодійний досвід навчання, сприяючи глибшому розумінню матеріалу. Використання AR в освіті вже продемонструвало свою ефективність через ряд застосунків, включаючи віртуальні екскурсії, інтерактивне вивчення анатомії та дослідження хімічних реакцій. Однак, важливо врахувати й обмеження та виклики, пов'язані з впровадженням AR в освітній процес. Технічні обмеження, обмежений доступ до технології та потреба в кваліфікованих вчителях є ключовими питаннями, які потрібно вирішити, щоб повноцінно використовувати можливості AR. З урахуванням цих викликів та потенціалу, системи доповненої реальності в освіті відкривають нові горизонти для навчання та заслуговують подальшого дослідження та розробки.

РОЗДІЛ 2 АРХІТЕКТУРА НАВЧАЛЬНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

2.1 Аналіз існуючих навчальних систем з використанням доповненої реальності

Застосування технології доповненої реальності (AR) в освітніх системах створило новий підхід до навчання, який зосереджений на активному залученні студентів. Цей підхід поєднує в собі цифровий контент з реальним світом, створюючи динамічне середовище, де студенти можуть взаємодіяти з об'єктами навчання в контексті реального світу. Для початку, проаналізуємо ключові компоненти, які використовуються в цих системах:

– Інтерфейс користувача, в основі якого лежать пристрої, які використовуються для інтеракції з AR середовищем. Це можуть бути мобільні пристрої, як-то смартфони і планшети, настільні комп'ютери з веб-камерами або спеціалізовані AR пристрої, як-то окуляри доповненої реальності або голографічні дисплеї. Інтерфейси користувача не тільки відображають доповнений контент, але і забезпечують взаємодію з цим контентом, часто використовуючи сенсори, контролери або технологію розпізнавання жестів.

– Системи відслідковування, що відіграють критично важливу роль, визначаючи положення і орієнтацію користувача в реальному світі. Це досягається за допомогою широкого спектра технологій, включаючи GPS, IMU сенсори (наприклад, акселерометр, гіроскоп, магнетометр), системи розпізнавання зображень або AR маркери, та технології, такі як SLAM (одночасна локалізація та картографування).

– Доповнений контент, а саме віртуальні об'єкти, що накладаються на реальний світ, створюючи ілюзію їх присутності в фізичному середовищі. Цей контент може бути текстом, зображеннями, відео, аудіо або 3D-моделями. Розробка доповненого контенту часто вимагає знань з 3D-моделювання та комп'ютерної графіки.

– Програмне забезпечення та апаратні засоби, що використовуються для обробки інформації, отриманої від систем відслідковування, та подання доповненого контенту через інтерфейс користувача. Вони можуть використовувати як місцеві обчислювальні ресурси (наприклад, процесор і графічний адаптер смартфона або комп'ютера), так і зовнішні обчислювальні ресурси, доступні через хмарні сервіси.

– Безпека та приватність необхідні компоненти системи, адже керуючи чутливими даними, такими як місцезнаходження користувача, його поведінка або навіть зображення його довкілля, AR системи повинні включати надійні заходи безпеки та приватності. Це може включати в себе різноманітні методи шифрування, аутентифікацію користувача, авторизацію, контроль доступу та анонімізацію даних.

AR системи можуть бути поділені на дві основні категорії: маркерні та не маркерні системи. Ця класифікація відноситься до способу, якими системи визначають та відслідковують віртуальні об'єкти в реальному світі.

– У маркерних системах використовуються спеціальні маркери або коди, які визначають положення та орієнтацію віртуальних об'єктів. Ці маркери можуть бути вигляду спеціальних друкованих зображень, QR-кодів або інших геометричних форм. Камера AR системи розпізнає ці маркери та використовує їх для позиціонування та відображення віртуального контенту. Маркерні системи зазвичай забезпечують високу точність відслідковування та стабільність позиціонування віртуальних об'єктів.

– У не маркерних системах для визначення положення віртуальних об'єктів використовуються природні ознаки або розпізнавання зображень. Вони не потребують спеціальних маркерів, але використовують алгоритми комп'ютерного зору, щоб визначити та відслідковувати ознаки в реальному світі. Не маркерні системи дають більшу свободу користувачам, оскільки вони можуть розміщувати віртуальні об'єкти на будь-якому підходящому поверхні без необхідності використання спеціальних маркерів.

Кожен тип AR системи має свої переваги та обмеження. Маркерні системи забезпечують більш точне відслідковування та стабільність, але вимагають

наявності маркерів для правильної роботи. Не маркерні системи дають більшу гнучкість та можливість використовувати різні поверхні для відображення віртуальних об'єктів, але можуть бути менш точними та стабільними у деяких умовах. Вибір між маркерною та не маркерною системою залежить від конкретних потреб та вимог проекту або застосування.

Проаналізуємо два основні типи навчальних систем, що використовують AR: мобільні та через окуляри.

Мобільні AR навчальні системи використовують смартфони або планшети як основний інтерфейс для користувача , на яких відображається AR контент, з елементами керування, такими як кнопки, жести або взаємодія на сенсорному екрані, що дозволяють користувачу взаємодіяти з AR контентом. Вони працюють, використовуючи вбудовану камеру пристрою для визначення положення та орієнтації у реальному світі. Ці дані потім використовуються для накладання віртуальних об'єктів на зображення з камери в реальному часі. Ці системи можуть використовувати GPS для геолокації та акселерометр і гіроскоп для визначення орієнтації пристрою. Програмне забезпечення AR, таке як ARKit (Apple) або ARCore (Android), використовуються для обробки зображень з камери, визначення положення AR об'єктів, та накладання цих об'єктів на зображення з камери. Оскільки ці системи працюють на пристроях користувача, вони використовують обчислювальні можливості цих пристроїв для обробки AR. Проте, для обробки важких обчислень, таких як 3D графіка або аналіз великого обсягу даних, можуть використовуватися хмарні сервіси. Щодо безпеки і приватності, вони мають використовувати шифрування для захисту даних користувача та механізми аутентифікації та авторизації для забезпечення безпечного доступу до системи.

Окуляри та голографічні AR навчальні системи використовують спеціалізовані пристрої, такі як Microsoft HoloLens, які дозволяють накладати віртуальні об'єкти безпосередньо на поле зору користувача. Вони використовують складні системи відслідковування, такі як слідкування за поглядом, SLAM (одночасна локалізація та картографування) та слідкування за рухом голови. Обробка даних може відбуватися безпосередньо на пристрої, але важкі обчислення, такі як обробка 3D-графіки або аналіз великих наборів даних, можуть бути

перенесені в хмару. Оскільки ці системи можуть збирати великі обсяги чутливих даних, таких як місцезнаходження користувача, їх поведінка, або навіть зображення їхнього середовища, безпека та приватність є важливими питаннями. Ці системи повинні використовувати сильні технології шифрування та авторизації користувача для захисту даних.

Детальніше розглянемо архітектуру кожного з типів системи AR:

1. Архітектура мобільних AR систем складається з наступних елементів:

– Інтерфейс користувача: Зазвичай це екран смартфона або планшета. Інтерфейс має зручні для користувача елементи керування, які дозволяють інтерактивно взаємодіяти з AR контентом.

– Система відслідковування: Для визначення положення і орієнтації пристрою в просторі використовуються камери, сенсори (акселерометри, гіроскопи) та, інколи, GPS.

– Графічний рушій: Для обробки інформації від системи відслідковування та відображення AR контенту на екрані пристрою.

– Доповнений контент: Це можуть бути текст, зображення, відео, аудіо та 3D моделі, які додаються до реального світу.

– Безпека і приватність: Використовуються механізми шифрування, авторизації та аутентифікації для забезпечення безпечного доступу до системи і захисту даних користувача.

2. Архітектура голографічних систем або окулярів складається з:

– Інтерфейс користувача: Спеціалізований пристрій для відображення доповненого контенту в полі зору користувача, наприклад, Microsoft HoloLens.

– Система відслідковування: Використовуються передові технології, такі як слідкування за рухом голови, слідкування за поглядом або SLAM (Simultaneous Localization and Mapping).

– Графічний рушій: Відповідає за відображення доповненого контенту в реальному середовищі відповідно до даних системи відслідковування.

– Доповнений контент: Може включати текст, зображення, відео, аудіо, 3D моделі та інтерактивні елементи.

– Безпека і приватність: Оскільки ці системи можуть збирати великі обсяги даних про користувача і його довкілля, вони вимагають особливих заходів забезпечення приватності та безпеки.

У таблиці 2.1 наведено порівняння між двома типами навчальних систем, що використовують AR, з урахуванням їхніх основних характеристик, таких як інтерфейс користувача, система відслідковування, графічний рушій, доповнений контент і безпека та приватність.

Таблиця 2.1 - Порівняння типів навчальних систем, що використовують технологію доповненої реальності

Тип системи	**Інтерфейс користувача**	**Система відслідковування**	**Графічний рушій**	**Доповнений контент**	**Безпека та приватність**
Мобільні	Смартфон або планшет	Камера, сенсори, GPS	ARKit, ARCore	Текст, зображення, відео, звук, 3D-моделі	Шифрування, автентифікація, аутентифікація
Окуляри	Спеціалізовані пристрої, такі як Microsoft HoloLens	Розпізнавання рухів голови, SLAM	HoloLens, Magic Leap	Текст, зображення, відео, звук, 3D-моделі	Шифрування, автентифікація, аутентифікація

Архітектури систем можуть варіюватися в залежності від специфічного використання AR системи, але в цілому дають уявлення про те, як може бути влаштована AR навчальна система. На основі цього аналізу можна створити узагальнену архітектуру навчальної системи з використанням технології доповненої реальності, яка би включала основні компоненти, що були описані вище, та враховувала специфіку різних типів систем.

2.2 Узагальнена архітектура навчальної системи з використанням доповненої реальності

Узагальнена архітектура AR для навчальних систем включає різноманітні компоненти та зв'язки, що дозволяють створювати інтерактивне та пізнавальне навчання, поєднуючи реальний світ з віртуальним контентом. Важливо зазначити, що доповнена реальність та навчальна система існують як окремі компоненти, але

вони мають взаємодіяти та обмінюватись даними, щоб створити навчальну систему, що використовує технологію доповненої реальності. Розглянемо основну складову потрібної нам системи - компоненти навчальної системи та взаємодію між ними. Ми використали платформу LMS як основу. Основними компонентами архітектури навчальної системи є:

– User's web-interface module.
– IAM (Identity and Access Management).
– Student Module, Tutor Module, Admin Module.
– API Connectors.
– LMS Knowledge Base.
– Third-party Service та Standards.

Ці компоненти разом створюють навчальну систему, яка забезпечує інтегровану і зручну платформу для навчання, викладання та управління навчальним процесом. Для ефективної взаємодії та обміну даними між компонентами необхідно описати й зв’язки між ними:

– User взаємодіє з User's web-interface module – це забезпечує інтерфейс взаємодії між користувачами і системою. Цей модуль дозволяє користувачам увійти до системи, переглядати та редагувати свої профілі, виконувати завдання, спілкуватися з викладачами та іншими студентами, а також отримувати доступ до різноманітного навчального контенту.

– User's web-interface module взаємодіє з IAM для управління ідентифікацією та доступом користувачів. Це означає, що модуль звертається до IAM для автентифікації та авторизації користувачів, забезпечуючи доступ до відповідних ресурсів та функціоналу в системі.

– User's web-interface module, Student Module, Tutor Module та Admin Module взаємодіють між собою за допомогою API Connectors. Це дозволяє різним користувачам (студентам, викладачам та адміністраторам) взаємодіяти з системою, використовуючи відповідні модулі та отримувати доступ до потрібного функціоналу.

– Student Module та Tutor Module взаємодіють з LMS Knowledge Base для доступу до навчальних матеріалів, курсів, завдань тощо. Студенти та викладачі

можуть отримувати доступ до відповідних навчальних ресурсів та матеріалів, використовуючи свої модулі та спілкуватися з LMS Knowledge Base для отримання актуальної інформації.

– API Connectors забезпечують зв'язок між системою та сторонніми сервісами Third-party Service. Це дозволяє обмінюватися даними з іншими системами або використовувати стандарти для взаємодії з зовнішніми сервісами, такими як платіжні системи або поштові сервіси.

Описані зв'язки між компонентами забезпечують якісну взаємодію і обмін даними в рамках навчальної системи. Вони допомагають забезпечити ефективну роботу користувачів, надаючи їм доступ до потрібного функціоналу та ресурсів для навчання, викладання та управління навчальним процесом. Схематичне зображення архітектури навчальної системи зображено на рисунку 2.1.

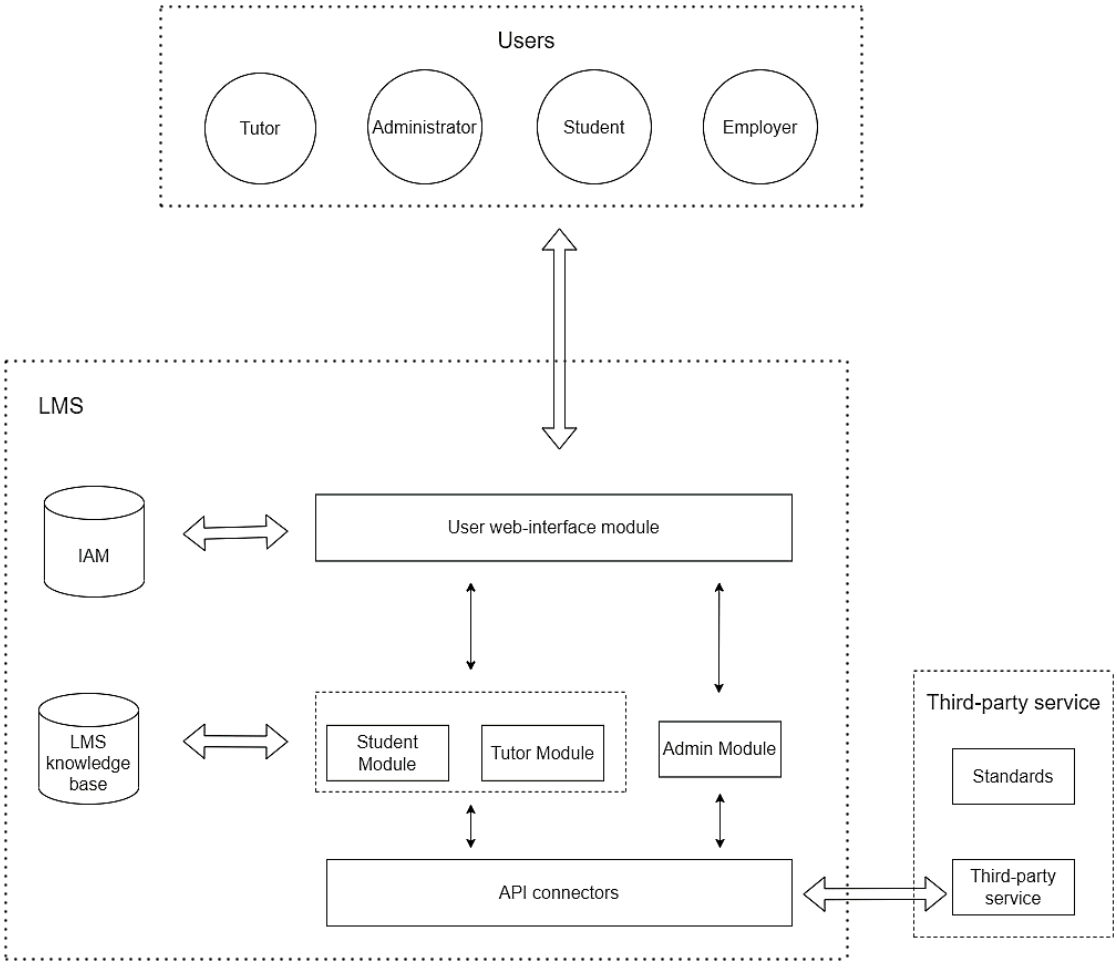

Рисунок 2.1 - Архітектура навчальної системи

Перейдемо до іншої важливої складової нашої системи, яка використовує технологію доповненої реальності - узагальненої архітектури AR. Основними компонентами AR є:

1) Sensors:
   - Cameras.
   - Gyroscopes and accelerometers.
   - Distance sensors.
   - GPS.
2) Tracking:
   - Marker tracking.
   - SLAM tracking.
3) Data processing:
   - Computer vision.
   - Motion tracking.
   - Depth processing.
4) AR engine:
   - Rendering.
   - Shaders.
   - Physical modeling.
5) User interface:
   - Control elements.
   - Information display.
6) Cloud services:
   - Server-side data processing.
   - Data storage.
   - Network interaction.
7) Network connection:
   - Data transfer.
   - Receiving data.

– Data storage.

8) AR content:

– Generation of virtual content.

– Content positioning.

– Content display.

9) Security:

– Data protection.

– Application security.

– User privacy.

На рисунку 2.2 представлено компоненти узагальненої архітектури доповненої реальності та зв’язки між ними, завдяки яким користувачі можуть отримати доступ до доповненої реальності, де віртуальний та реальний світи злиті в єдине ціле.

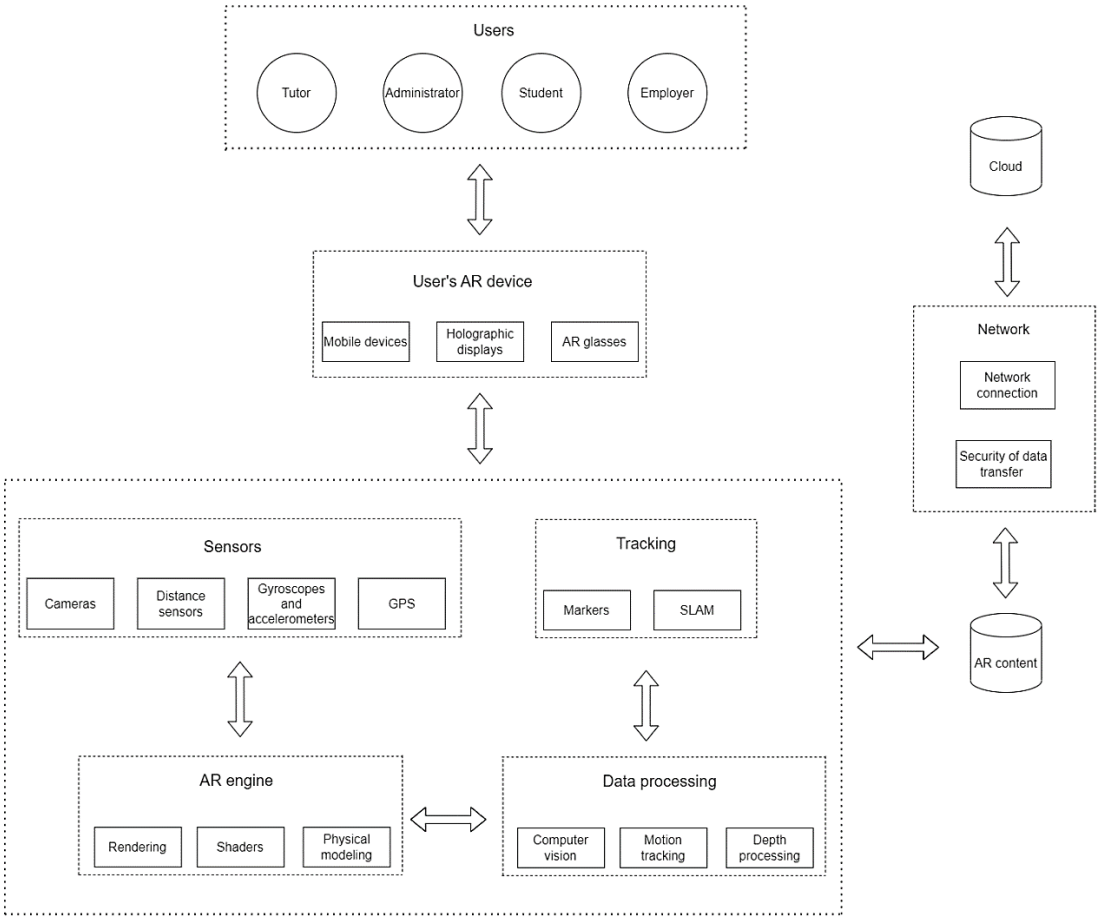

Рисунок 2.2 – Узагальнена архітектура доповненої реальності

Як бачимо схема архітектури AR системи включає різноманітні компоненти, такі як сенсори, відслідковування, обробку інформації, графічний рушій, інтерфейс користувача, хмарні сервіси, зв'язок з мережею, доповнений контент та безпеку, а зв'язки між компонентами системи були побудовані таким чином, щоб забезпечити ефективну взаємодію між різними компонентами AR системи та забезпечити реалістичний та інтерактивний AR контент для користувачів. Кожен зв'язок відображає важливу роль, яку відповідні компоненти виконують у створенні доповненого контенту та відображенні його в реальному часі. Розглянемо кожен із них:

– Зв'язок між такими компонентами як Users та User's AR device є ключовим елементом, який забезпечує користувачам доступ до доповненого віртуального контенту. Ці пристрої мають вбудовані сенсори, такі як камери, гіроскопи та акселерометри, які забезпечують збір інформації про реальне оточення. Крім того, вони мають доступ до AR додатків та платформ для взаємодії з AR контентом.

– Зв'язок між Sensors та Tracking ілюструє, як сенсори AR системи, такі як камери, гіроскопи та акселерометри, співпрацюють з компонентами відслідковування, такими як відслідковування маркерів або SLAM (одночасна локалізація та картографування). Сенсори збирають дані про реальне оточення, а відслідковування використовує ці дані для визначення положення та орієнтації AR пристрою у просторі.

– Зв'язок між Sensors та Data processing показує, як дані, зібрані сенсорами, передаються до компонентів обробки інформації, таких як комп'ютерний зір, відслідковування руху та обробка глибини. Ці компоненти аналізують отримані дані, виявляють ознаки та розпізнають об'єкти в реальному часі.

– Зв'язок між Sensors та AR engine показує, як дані з сенсорів, такі як відео та орієнтація, використовуються графічним рушієм для відображення віртуального контенту на дисплеї AR пристрою. Графічний рушій враховує освітлення та інші фактори для створення реалістичного зображення.

– Зв'язок між Tracking, Sensors, Data processing, AR engine та User interface показує, що відслідковування має прямий зв'язок з іншими компонентами системи. Відслідковування використовує дані з сенсорів та передає їх до обробки

інформації, графічного рушія та інтерфейсу користувача для точного позиціонування віртуального контенту та забезпечення взаємодії з ним.

– Зв'язок між Cloud services та Network connection показує, як хмарні сервіси використовують зв'язок з мережею для передачі даних між AR пристроєм та віддаленими серверами. Це може включати виконання складних обчислень, зберігання AR контенту та користувацьких даних, а також мережеву взаємодію з іншими джерелами даних.

– Зв'язок між Network connection та Cloud services показує, як зв'язок з мережею використовується для забезпечення зв'язку між AR пристроєм та хмарними сервісами. Це може включати передачу даних, отримання оновлень віртуального контенту, інструкцій, географічних даних та іншого.

– Зв'язок між AR content, Tracking, Data processing, AR engine показує, як доповнений контент співпрацює з іншими компонентами для створення реалістичного AR контенту. Він залежить від відслідковування для правильного позиціонування, обробки інформації для аналізу отриманих даних та графічного рушія для відображення віртуального контенту.

– Зв'язок між Security та Network connection, доповненим контентом показує, що безпека та приватність важливі для збереження конфіденційності користувачів та захисту їхніх даних. Він включає контроль зв'язку з мережею для забезпечення безпечної передачі даних та захисту від вразливостей. Також безпека та приватність враховуються при збереженні та обробці доповненого контенту, забезпечуючи захист особистої інформації користувачів.

Узагальнена архітектура навчальної системи з використанням технології доповненої реальності включає в себе взаємодію двох основних компонентів: компонента доповненої реальності і навчальної системи, представленої модулем LMS.

Доповнена реальність виконує ключову роль у створенні віртуального контенту, який є основою для навчального процесу. Він включає такі компоненти, як сенсори (камери, гіроскопи, акселерометри, датчики відстані, GPS), відслідковування (відслідковування маркерів, відслідковування SLAM), обробка інформації (комп'ютерний зір, відслідковування руху, обробка глибини), графічний

рушій (рендеринг, шейдери, фізичне моделювання), інтерфейс користувача (елементи керування, відображення інформації), хмарні сервіси (обробка даних на стороні сервера, зберігання даних, мережева взаємодія), зв'язок з мережею (передача даних, отримання даних, зберігання даних), доповнений контент (генерація віртуального контенту, позиціонування контенту) та безпека та приватність (захист даних, безпека додатків, приватність користувачів).

Модуль LMS навчальної системи виконує функції управління, організації та навчання. Він включає такі компоненти, як управління користувачами, управління курсами, організація навчального контенту, оцінювання та звітність. Цей модуль дозволяє студентам доступатися до навчального матеріалу, виконувати завдання, спілкуватися з викладачами та іншими студентами, а також отримувати оцінки та звіти про свою успішність.

В свою чергу, зв'язок між Users, User's AR device та LMS відбувається через User web-interface module. Користувачі використовують свої AR пристрої для доступу до системи, де вони можуть отримувати інформацію, виконувати завдання, спілкуватися з іншими користувачами та викладачами, а також здійснювати контроль над своїм навчальним процесом. User web-interface module забезпечує зручний та інтуїтивно зрозумілий інтерфейс для взаємодії з системою, що дозволяє користувачам ефективно використовувати можливості технології доповненої реальності у навчальних цілях. Таким чином, компонент Users, разом з User's AR device та User web-interface module, створює зв'язок між користувачами та навчальною системою, що дозволяє студентам, викладачам та адміністраторам використовувати потенціал доповненої реальності для збагачення навчального досвіду та підвищення ефективності навчального процесу.

З'єднання між компонентом доповненої реальності і модулем LMS здійснюється через компонент AR content (див. рисунок 2.3). Доповнена реальність створює AR content, який потім використовується в навчальній системі для проведення навчального процесу. AR content може включати в себе віртуальні об'єкти, симуляції, інтерактивні завдання, відео та інші компоненти, які допомагають студентам вивчати предмети більш ефективно та цікаво.

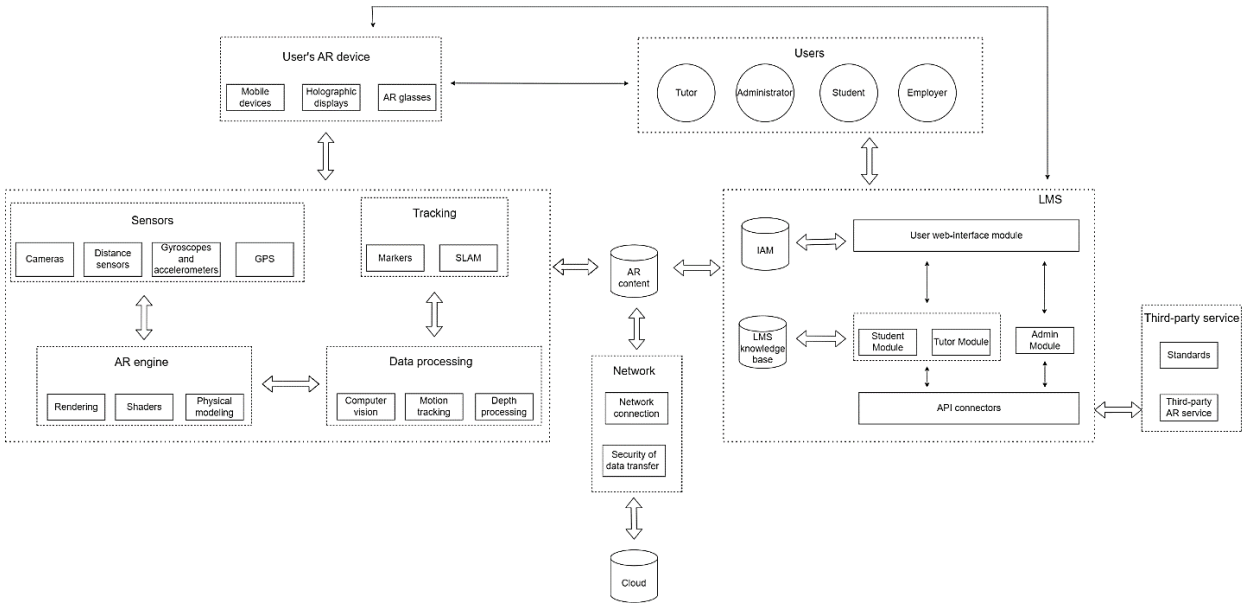

Рисунок 2.3 - Узагальнена архітектура навчальної системи з використанням технології доповненої реальності

В результаті об'єднання цих архітектур була створена навчальна система, яка поєднує в собі силу технології доповненої реальності з функціональністю інструментів платформи LMS, яка входить в основу нашої навчальної системи. Ця інтеграція дозволяє отримувати віртуальні інтерактивні навчальні матеріали, здійснювати практичні вправи та дослідження у віртуальному середовищі, а також взаємодіяти з викладачами та іншими студентами через платформу LMS. Така узагальнена архітектура навчальної системи з використанням технології доповненої реальності забезпечує зручну та ефективну організацію навчального процесу та створює умови для успішного навчання студентів.

2.3 Важливість забезпечення безпеки навчальних систем з використанням доповненої реальності

У сучасному цифровому світі зростає популярність та використання навчальних систем, які використовують технологію доповненої реальності (AR). Ці системи надають унікальний досвід навчання, де віртуальні об'єкти накладаються на реальний світ, стимулюючи активне та досвідчене навчання. Однак, разом зі зростанням використання AR в освітніх системах, постають питання про безпеку цих систем.

Актуальність обговорення безпеки навчальних систем з використанням технології доповненої реальності випливає з кількох ключових факторів. По-перше, зростання популярності та використання AR систем у сфері освіти та навчання створює потребу у забезпеченні безпеки цих систем. Використання AR може включати обмін конфіденційною інформацією, включаючи особисті дані користувачів, що потребує захисту. По-друге, AR системи залучають широкий спектр користувачів, включаючи дітей та молодь. Забезпечення безпеки цих систем стає особливо важливим, оскільки необхідно забезпечити безпечне та захищене навчання для учнів та студентів. Доступ до навчальної інформації та даних повинен бути контрольованим та обмеженим, щоб уникнути можливих загроз.

Забезпечення конфіденційності, цілісності та доступності даних також є важливими аспектами безпеки AR навчальних систем. Конфіденційні дані користувачів, такі як особиста інформація та навчальні досягнення, повинні бути захищені від несанкціонованого доступу та витоку інформації. Цілісність даних включає забезпечення недоступності для зловмисників та запобігання неправомірній зміні даних. Крім того, доступність системи для користувачів має бути забезпечена, щоб забезпечити неперервний та ефективний процес навчання.

Для підтвердження актуальності обговорення безпеки AR навчальних систем, проведемо аналіз досліджень та випадків, пов'язаних з безпекою таких систем. Дослідження та статті в цій області показують, що існують значні потенційні загрози та ризики, які потребують належної уваги.

В дослідженні [12] вказано, що в 2021 році освіта та начальні системи були сектором, який зазнав найбільшої кількості атак (див. рисунок 2.4), в середньому 1605 атак на організацію щотижня, що на 75% більше, ніж у 2020 році. Далі йдуть урядовий/військовий сектор, який мав 1136 атак на тиждень (зростання на 47%), і галузь зв’язку, яка мала 1079 атак на тиждень на організацію (збільшення на 51%).

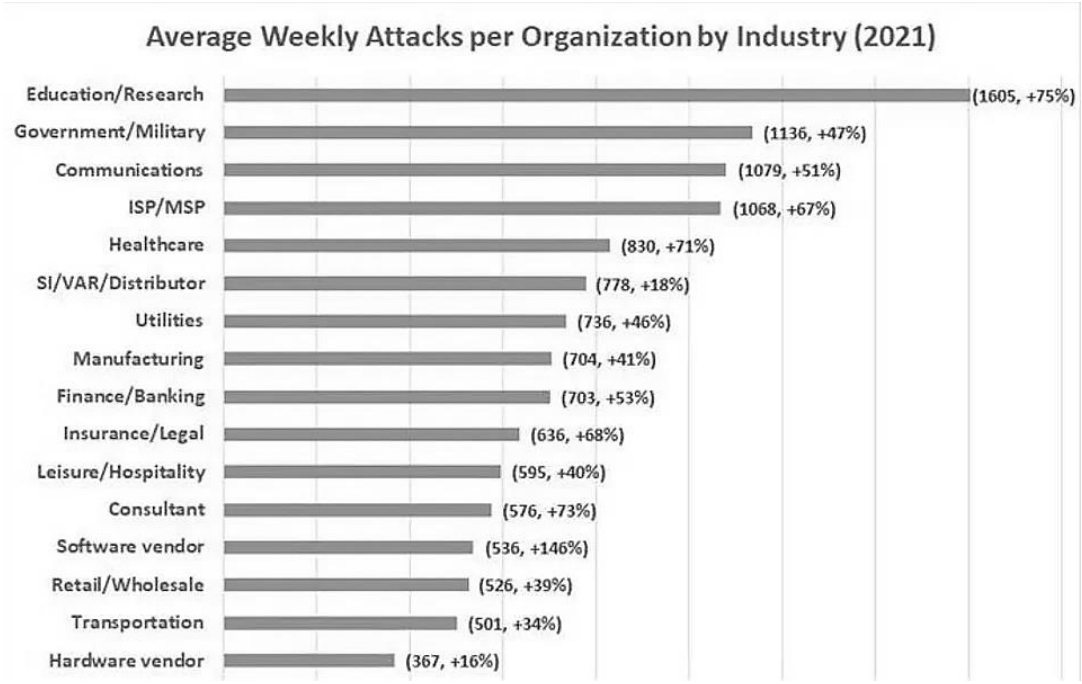

Рисунок 2.4 – Середня тижнева кількість атак на організації за галузями

Стаття [13] є значним дослідженням, що виявляє різноманітні загрози безпеці AR систем. Дослідження виявило такі потенційні загрози:

– Викрадення особистих даних: AR системи можуть збирати та обробляти особисту інформацію користувачів, що створює ризик її витоку або використання без дозволу.

– Атаки з використанням шкідливого контенту: Зловмисники можуть створювати шкідливий контент, який може бути відображений у AR системах, що може призвести до впливу на користувачів, порушення конфіденційності або викликати інші негативні наслідки.

– Викривання конфіденційної інформації: AR системи можуть бути вразливі до атак, які спрямовані на викриття конфіденційних даних, таких як паролі, ключі доступу або інші конфіденційні відомості.

Стаття [14] проводить аналіз безпеки AR додатків на платформі Android. Дослідження виявляє потенційні ризики, пов'язані з несанкціонованим доступом до даних та змінами в системі. Він наголошує на наступних аспектах:

– Несанкціонований доступ до даних: AR додатки на платформі Android можуть мати деякі слабкі місця, що дозволяють несанкціонованим користувачам отримувати доступ до приватної інформації, яка зберігається на пристрої.

– Зміни в системі: Деякі AR додатки можуть мати властивості, які дозволяють їм внесення змін до налаштувань або системних файлів, що може призвести до порушення безпеки пристрою або вплинути на його функціональність.

Ці статті є лише декількома прикладами досліджень, що демонструють потенційні загрози безпеці AR навчальних систем. Цей аналіз підкреслює необхідність ретельного дослідження та впровадження заходів захисту для забезпечення безпеки таких систем та захисту користувачів. Дослідження та розуміння потенційних загроз та ризиків є ключовим етапом у розробці ефективних стратегій та методів захисту AR навчальних систем.

Існує ряд публікацій, які проводять детальний аналіз ризиків та проблем безпеки AR навчальних систем. Наприклад, стаття [15] розглядає наступні ризики та загрози:

– Витоки даних: AR системи можуть збирати і зберігати значну кількість даних про користувачів, включаючи особисту і конфіденційну інформацію. Це створює потенційні загрози безпеці, особливо якщо дані не належним чином захищені. Витоки даних можуть відбуватися через недостатню захищеність системи, зловживання дозволами доступу або атаки на комунікаційний канал.

– Несанкціонований доступ: Зловмисники можуть намагатися отримати несанкціонований доступ до AR системи з метою отримання конфіденційної інформації або зміни її функціоналу. Це може стати наслідком вразливостей у програмному забезпеченні системи, слабкостей в автентифікації та авторизації, недостатньої захищеності мережевих протоколів або зловживання довіри користувачів.

– Порушення цілісності: AR системи піддаються ризику атак, спрямованих на зміну або спотворення віртуального контенту. Зміна цілісності може призвести до недостовірної інформації, неправильних вказівок або навіть небезпеки для користувачів. Це може відбутися через вразливості в AR движках, атаки на комунікаційні канали або недостатні контрольні механізми для перевірки цілісності контенту.

На додаток до статті [13] є й інші публікації, що досліджують ризики та проблеми безпеки AR навчальних систем. Одна з таких статей [15], яка зосереджується на безпеці додатків AR на мобільних пристроях. У цій статті зазначаються такі ризики та загрози:

– Вразливості додатків: Дослідження виявили, що деякі додатки AR на мобільних пристроях мають вразливості, які можуть бути використані для несанкціонованого доступу до пристрою або отримання неправомірного контролю над ним.

– Зловживання дозволів доступу: Деякі додатки AR можуть вимагати доступу до різних функцій і даних на пристрої, включаючи камеру, мікрофон, контакти, місцезнаходження тощо. Зловмисники можуть зловживати цими дозволами, щоб отримати доступ до приватної інформації або здійснювати небезпечні дії.

– Вплив на фізичну безпеку: Використання AR може впливати на фізичну безпеку користувачів, особливо у випадках, коли вони втрачають свідомість про своє оточення або не розуміють потенційні небезпеки, такі як перешкоди на дорозі або небезпечні зони.

Ці статті демонструють, що безпека AR навчальних систем є важливою проблемою, яка потребує подальшого дослідження та заходів для забезпечення надійності та захищеності таких систем.

Окрім вище вказаного прикладу, в AR навчальних системах можуть відбуватись інші види атак, які потенційно загрожують безпеці та приватності користувачів. Один з таких видів атак - це атаки з використанням шкідливого контенту. Деякі дослідження вказують на можливість інтеграції шкідливих елементів у доповнений контент AR системи. Зловмисники можуть створювати та розповсюджувати шкідливі AR об'єкти або додавати шкідливий контент до існуючих об'єктів. Це може викликати різноманітні наслідки, включаючи шкоду для пристрою користувача, викрадення особистих даних або поширення зловмисного програмного забезпечення.

Поряд з атаками з використанням шкідливого контенту, існують й інші види атак, які можуть торкатись безпеки AR навчальних систем. Один з таких видів атак

- це атаки на розпізнавання маркерів. Деякі AR системи використовують маркери для визначення положення та орієнтації віртуальних об'єктів. Зловмисники можуть спробувати використати цей механізм для впливу на систему, накладаючи неправильні маркери або модифікуючи існуючі, що може призвести до некоректного розпізнавання та неправильного позиціонування об'єктів.

Інший вид атак - це атаки на перехоплення та модифікацію даних, що передаються між AR системою та серверами. Зловмисники можуть спробувати перехопити комунікацію та отримати доступ до передаваних даних. Це може стати загрозою для конфіденційності та цілісності даних, а також призвести до втручання у взаємодію користувача з AR системою.

Також варто враховувати можливість атак на пристрої користувача, які використовують AR. Зловмисники можуть використовувати вразливості пристрою, зокрема операційну систему або додатки, для отримання несанкціонованого доступу до даних користувача або здійснення шкідливих дій.

Крім кібернетичного впливу, ризики безпеки AR навчальних систем можуть мати серйозні наслідки для життя та здоров'я користувачів. Наприклад, атаки на датчики та системи відслідковування можуть призвести до некоректного функціонування AR системи та створення небезпечних ситуацій для користувачів. Однією з таких можливих атак є атака на датчик камери. Зловмисники можуть зламати або контролювати датчик камери AR пристрою, що може привести до неправильного відображення віртуального контенту на реальному світі. Це може викликати непередбачувану реакцію користувача та потенційно призвести до небезпечних ситуацій, таких як зіткнення з об'єктами або несанкціонований доступ до областей, які мають бути обмежені.

Також варто згадати про можливість атак на системи відслідковування. Деякі AR системи використовують датчики, такі як акселерометр, гіроскоп та GPS, для визначення положення та орієнтації пристрою в просторі. Атаки на ці системи можуть призвести до неправильного визначення положення та орієнтації, що може призвести до некоректного взаємодії з віртуальним контентом. Наприклад, неправильне визначення висоти під час використання AR навчальної системи на

висоті може призвести до потенційно небезпечних ситуацій, які можуть вплинути на безпеку користувача.

А ще атаки несуть значні репутаційні збитки для організацій, навчальні системи не виключення. У сучасному цифровому світі, де довіра є важливою складовою успіху, навіть один серйозний інцидент безпеки може спричинити втрату довіри користувачів і клієнтів до системи. Коли система стає жертвою атаки, це може призвести до розголосу, а публічність, яка оточує такі події, зазвичай супроводжується негативними коментарями і обговореннями щодо безпеки системи. Негативна репутація внаслідок інцидентів безпеки може призвести до різкого зниження довіри користувачів і клієнтів до системи. Користувачі можуть почувати себе незахищеними і з недовірою використовувати таку систему. Якщо розголос негативних подій затягнеться, це може призвести до втрати значної частини користувачів і навіть до зменшення попиту на такі навчальні системи або послуги чи навіть до втрати своєї конкурентоспроможності.

Описані загрози, атаки та їх наслідки підкреслюють важливість забезпечення безпеки AR навчальних систем. Розробка та впровадження ефективних механізмів захисту, таких як шифрування даних, аутентифікація користувачів, контроль доступу та моніторинг системи на предмет виявлення аномалій, є необхідними для запобігання таким атакам та забезпечення безпеки та захисту користувачів у середовищі AR навчання.

Аналіз статей та проведених досліджень робить очевидним, що безпека AR навчальних систем потребує серйозної уваги. Вивчення загроз та атак на такі системи є важливим етапом для розуміння потенційних ризиків та вибору ефективних методів захисту. Отже, на основі аналізу статей та досліджень можна зробити висновок, що безпека AR навчальних систем є актуальною та важливою темою, яка потребує додаткових досліджень та заходів захисту. Розуміння потенційних загроз та ризиків є ключовим для розробки ефективних стратегій безпеки та захисту користувачів в середовищі AR навчання.

РОЗДІЛ 3 ЗАСТОСУВАННЯ MITRE ATT&CK ДЛЯ МОДЕЛЮВАННЯ ЗАГРОЗ БЕЗПЕКИ НАВЧАЛЬНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

3.1 Аналіз підходів для моделювання загроз безпеки

Важливим етапом в забезпеченні безпеки навчальної системи є виявлення потенційних загроз та розуміння, яким чином вони можуть вплинути на систему. Для досягнення цієї мети існує ряд різних підходів, які дозволяють аналізувати можливі атаки та ідентифікувати слабкі місця в системі. Вибір належного підходу має вирішальне значення, оскільки це дозволить отримати максимально комплексне та об'єктивне уявлення про загрози, з якими можуть зіткнутися навчальні системи з використанням технології доповненої реальності.

Проаналізуємо деякі з найбільш поширених підходів, що використовуються для моделювання загроз безпеки:

– STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) – визначає шість основних категорій загроз безпеки (див. рисунок 3.1). STRIDE дозволяє виявляти потенційні слабкі місця в системі та розробляти заходи для їх захисту.

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Рисунок 3.1 – Категорії безпеки за STRIDE

– PASTA (The Process for Attack Simulation and Threat Analysis) – це структура моделювання загроз, орієнтована на ризик. Містить сім етапів, кожен з кількома видами діяльності, які проілюстровані на рисунку 3.2. PASTA використовує різноманітні інструменти виявлення на різних етапах. Цей метод

підіймає процес моделювання загроз на стратегічний рівень. Широко розглядається як структура, орієнтована на ризик, PASTA використовує перспективу, орієнтовану на нападника, для отримання результату, орієнтованого на активи, у формі перерахування загроз та оцінки.

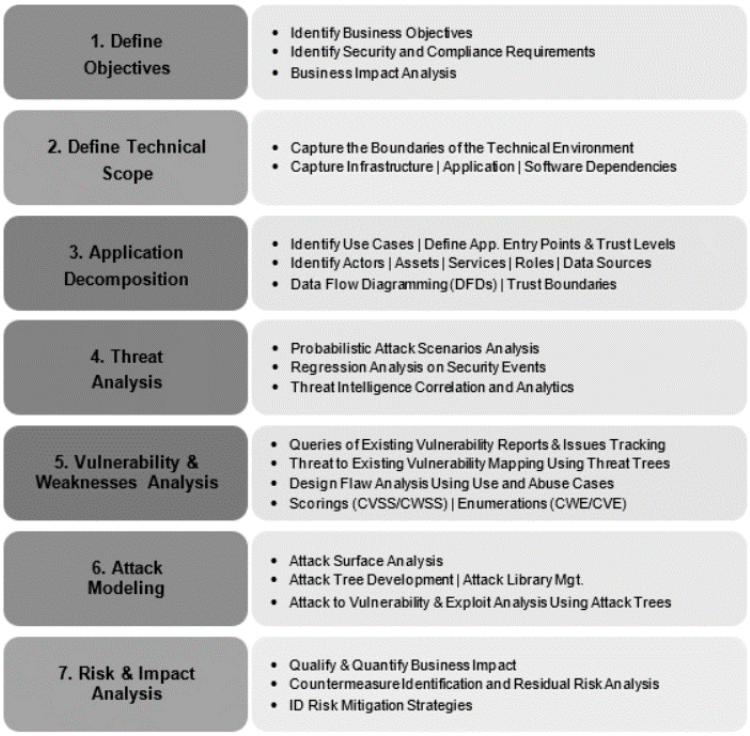

Рисунок 3.2 – Етапи симуляції та аналізу атак за PASTA

– DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) – оцінює загрози безпеки на основі п'яти факторів: збитки, повторюваність, кількість ушкоджених користувачів, вірогідність успішної експлуатації атаки та ймовірність виявлення, а також надає числову оцінку кожній з них (див. рисунок 3.3). Вона допомагає визначити, наскільки серйозними є загрози та як вони можуть вплинути на систему.

Рисунок 3.3 – Фактори DREAD

– Attack Trees (Дерева атак) – використовує деревоподібну структуру для моделювання можливих атак на систему (див. рисунок 3.4). Кожен вузол дерева представляє окрему атаку, а гілки показують шляхи, по яких атака може розгортатися. Це дозволяє виявити слабкі місця в системі та розробити стратегії захисту.

Рисунок 3.4 – Приклад дерева атак

– MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) – надає опис різних тактик, методів та технік, які зловмисники можуть використовувати для здійснення атак на систему (див. рисунок 3.5). MITRE ATT&CK відображає широкий спектр можливих атак та допомагає виявити слабкі місця в системі.

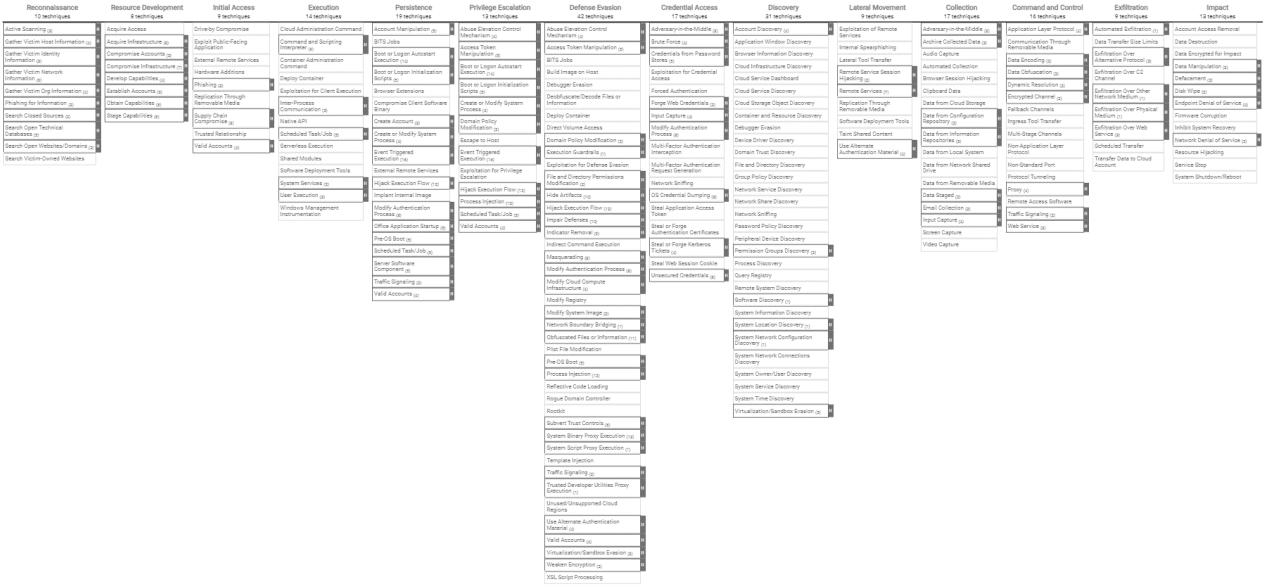

Рисунок 3.5 – Тактики та техніки MITRE ATT&CK

– LINDDUN (linkability, identifiability, nonrepudiation, detectability, disclosure of information, unawareness, noncompliance) – фреймворк для моделювання загроз конфіденційності (див. рисунок 3.6). Забезпечує підтримку систематичного виявлення та пом'якшення загроз конфіденційності в архітектурах програмного забезпечення.

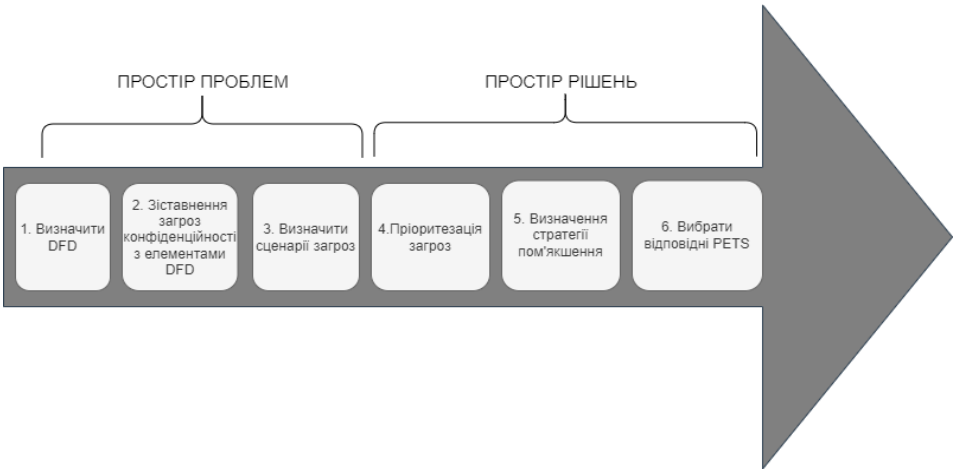

Рисунок 3.6 – Кроки LINDDUN

– OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - це метод стратегічної оцінки та планування кібербезпеки на основі ризиків (див. рисунок 3.7). OCTAVE фокусується на оцінці організаційних ризиків і не розглядає

технологічні ризики. Його основними аспектами є операційні ризики, практики безпеки та технології.

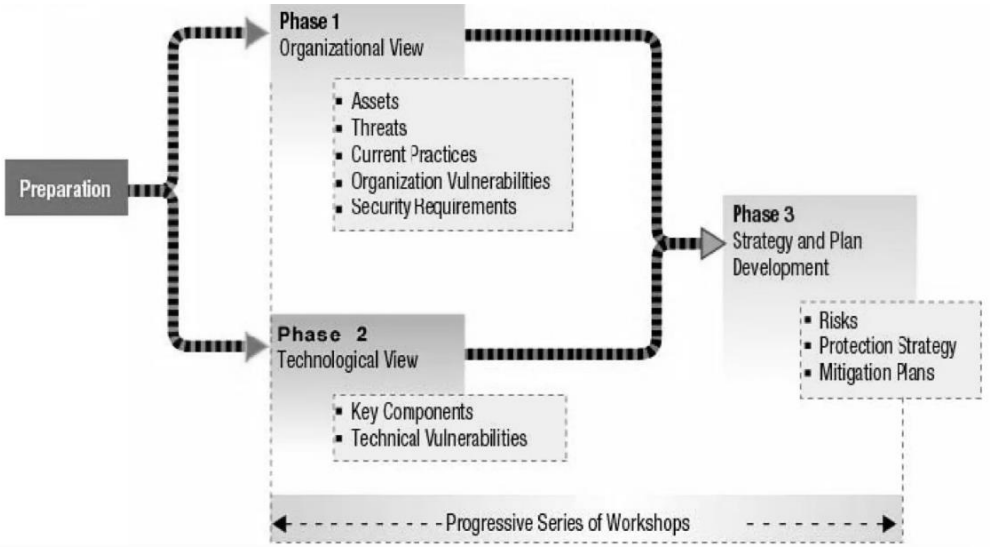

Рисунок 3.7 – Фази OCTAVE

З врахуванням важливості виявлення потенційних загроз та їх впливу на навчальну систему з використанням технології доповненої реальності, після ретельного аналізу різних підходів для моделювання загроз безпеки і ретельного розгляду кожної з них, було прийняте рішення обрати MITRE ATT&CK.

Вибір MITRE ATT&CK як фреймворку для моделювання загроз безпеки в нашій навчальній системі з технологією доповненої реальності зумовлений кількома перевагами, які він надає в порівнянні з іншими:

– По-перше, MITRE ATT&CK надає широкий огляд різних тактик, методів та технік, що використовуються зловмисниками для атак на системи. Це дозволяє нам охопити різноманітність можливих загроз і мати комплексне розуміння їх впливу на безпеку навчальної системи з використанням технології доповненої реальності.

– По-друге, MITRE ATT&CK надає систематичний підхід до моделювання атак. Розглядає атаки як послідовні процеси, що включають фази підготовки, виконання та наслідки. Це дозволяє нам виявити не лише окремі атаки, а й їх комплексне вплив на систему.

– По-третє, MITRE ATT&CK є широко відомою та використовуваною системою в галузі кібербезпеки. Має детально пророблені тактики, методи та

техніки, які забезпечують нам практичність та конкретність у вивченні загроз безпеки навчальної системи.

Таким чином, вибір MITRE ATT&CK в якості фреймворку для моделювання загроз безпеки в нашій навчальній системі з використанням технології доповненої реальності є обґрунтованим рішенням. Його широкий огляд атак, систематичний підхід до моделювання та практичність надають потрібний інструментарій для аналізу потенційних загроз та ідентифікації слабких місць в системі. Завдяки цим перевагам, зможемо отримати максимально комплексне та об'єктивне уявлення про загрози та розробити ефективні заходи для захисту нашої навчальної системи.

3.2 Аналіз фреймворку MITRE ATT&CK

MITRE ATT&CK - це глобально доступна база знань, що містить інформацію про тактики та техніки противника, яка ґрунтується на реальних спостереженнях. ATT&CK є основою для розробки моделей та методологій загроз у приватному секторі, урядових структурах та галузі кібербезпеки загалом. Існує три типи матриць ATT&CK: Enterprise ATT&CK, Mobile ATT&CK та ICS. Кожна матриця фокусується на різних техніках і тактиках.

Enterprise ATT&CK є однією з матриць фреймворку MITRE ATT&CK, яка спеціалізується на аналізі атак, спрямованих на операційні системи Linux, Windows та macOS. Ця матриця надає важливу інформацію для розробки стратегій захисту від цих атак, включаючи опис конкретних тактик та технік, що використовуються зловмисниками, а також вказівки щодо запобігання або виявлення таких атак. Enterprise ATT&CK охоплює широкий спектр атак, таких як використання вразливостей, перехоплення аутентифікаційних даних, впровадження шкідливого програмного забезпечення, розповсюдження через мережу та багато інших. Це дозволяє організаціям краще розуміти потенційні загрози для їхніх систем і розробляти ефективні заходи безпеки для захисту від них.

Mobile ATT&CK є ще однією з матриць у складі фреймворку MITRE ATT&CK і спрямована на аналіз атак, спрямованих на мобільні пристрої, такі як смартфони та планшети. Ця матриця ретельно досліджує різні тактики та техніки,

що використовуються зловмисниками для атак на мобільні платформи. Вона надає важливу інформацію про загрози, пов'язані з мобільними пристроями, включаючи експлойти, шкідливе програмне забезпечення, розвідку та методи поширення. Mobile ATT&CK охоплює широкий спектр атак, включаючи фішинг, використання підозрілих додатків, маніпуляцію з комунікаціями, експлуатацію вразливостей, отримання неправомірного доступу до приватних даних та багато іншого. Вона надає детальні описи цих тактик та технік, а також приклади реальних атак, спрямованих на мобільні платформи.

Матриця MITRE ATT&CK для ICS (Industrial Control Systems) є спеціалізованою матрицею, яка досліджує атаки на промислові системи керування. Вона зосереджується на тактиках та техніках, що використовуються зловмисниками для нападу на системи, що управляють критичними інфраструктурними об'єктами, такими як електростанції, системи водопостачання, транспортні мережі та інші. Ця матриця надає детальний опис різних тактик та технік, що використовуються зловмисниками, включаючи аутентифікацію, проникнення в мережу, контроль процесів, впровадження шкідливого програмного забезпечення та багато іншого. Вона допомагає організаціям, що використовують ICS, краще розуміти загрози та розробляти ефективні стратегії захисту для забезпечення безпеки своїх індустріальних систем.

MITRE ATT&CK є широко використовуваним фреймворком і отримав підтримку від різних організацій та установ:

- Національне управління з кібербезпеки США (CISA).
- Агентство національної безпеки США (NSA).
- Агентство національної безпеки та кібербезпеки Великої Британії (NCSC).
- Агентство кібербезпеки Європейського Союзу (ENISA).

Ці організації, разом з багатьма іншими урядовими та приватними суб'єктами, спонсорують та використовують фреймворк MITRE ATT&CK для підвищення своєї кібербезпеки та реагування на сучасні загрози.

На даний момент актуальною версією є ATT&CK v13, а основні матриці MITRE ATT&CK мають наступне наповнення:

1. Enterprise ATT&CK:

– кількість тактик: 14;

– кількість технік: 227.

2. Mobile ATT&CK:

– кількість тактик: 12;

– кількість технік: 78.

3. ICS ATT&CK:

– кількість тактик: 12;

– кількість технік: 92.

Щодо вигляду матриць, кожна матриця в рамках MITRE ATT&CK представлена у вигляді табличної структури. Кожний рядок у матриці відповідає окремій тактиці, а стовпці відображають різні техніки та їхні підтехніки.

– Тактики – це загальні цілі або стратегії, які зловмисники намагаються досягти під час атаки. Кожна тактика описує групу пов'язаних технік, які можуть бути використані зловмисниками для досягнення цілей.

– Техніки – це конкретні методи або прийоми, що використовуються зловмисниками для досягнення своїх цілей. Кожна техніка описує певну дію або процедуру, яку можуть використовувати зловмисники під час кібератаки та має унікальний ідентифікатор і детальний опис.

– Підтехніки - конкретні варіації або специфічні виконання технік з більш детальним описом. Вони використовуються для більш точного опису дій зловмисників.

– Процедури – специфічний приклад використання тактик/технік в реальних інцидентах. Тобто, це реальний приклад сценарій реалізації загроз.

MITRE регулярно оновлює фреймворк ATT&CK, вносячи нові техніки, тактики та інші зміни для відображення сучасних кіберзагроз. Зміни можуть включати додавання нових технік, виправлення помилок, уточнення описів або видалення застарілих або менш актуальних елементів.

У фреймворку MITRE ATT&CK існують деякі додаткові, допоміжні інструменти, які можуть бути використані для розширення функціональності та

покриття специфічних потреб аналізу та використання ATT&CK. Ось кілька з таких інструментів:

– MITRE ATT&CK Navigator - веб-платформа, яка надає інтерактивний інтерфейс для огляду та використання матриць ATT&CK. ATT&CK Navigator дозволяє користувачам візуалізувати, редагувати та аналізувати дані ATT&CK, створювати та зберігати власні варіації матриць, позначати прогрес аналізу та інше.

– Caldera - фреймворк для автоматизованої емуляції атак, який побудований на основі MITRE ATT&CK. Caldera надає можливість створювати та запускати сценарії атак, що дозволяє організаціям перевіряти ефективність своїх заходів безпеки та виявляти слабкі місця в системах.

– ATT&CK STIX/TAXII: STIX (Structured Threat Information Expression) та TAXII (Trusted Automated Exchange of Indicator Information) - стандарти обміну інформацією про загрози, які допомагають стандартизувати та автоматизувати обмін даними ATT&CK. Вони дозволяють організаціям обмінюватись та спільно використовувати інформацію про техніки, тактики та підтехніки ATT&CK для поліпшення загального рівня кібербезпеки.

Ці додаткові інструменти інтегруються з фреймворком MITRE ATT&CK і надають додаткові функціональні можливості, що полегшують роботу з ATT&CK та допомагають організаціям у покритті своїх специфічних потреб.

3.3 Застосування MITRE ATT&CK Navigator для моделювання загроз

У світі кібербезпеки, можливість передбачити, виявити і протидіяти потенційним загрозам є ключовим аспектом ефективного управління ризиками. Для цього ми повинні розуміти, як зловмисники можуть атакувати наші системи, і наскільки ці системи вразливі до різних видів атак.

Один з популярних методів для моделювання кіберзагроз та планування заходів з кіберзахисту - це використання MITRE ATT&CK Navigator. Цей інструмент дозволяє нам візуалізувати загрози і стратегії захисту в контексті конкретних технологій та компонентів системи.

У цьому розділі зосередимось на використанні MITRE ATT&CK Navigator для побудови матриць загроз для ключових компонентів нашої навчальної системи з використанням доповненої реальності: AR пристрою користувача, бази знань LMS, мережевого з'єднання та веб-інтерфейсу користувача. Ми будемо використовувати Mobile ATT&CK для моделювання загроз для AR пристрою користувача, та Enterprise ATT&CK для моделювання загроз для інших компонентів.

При побудові матриці загроз, особливо важливо враховувати всі компоненти системи. Однак, деякі компоненти можуть бути включені в інші як внутрішні елементи. Наприклад, сенсори, технології відстеження, обробка інформації, графічний рушій - всі вони є частиною AR пристрою, схожа ситуація і з іншими компонентами нашої системи. Здійснюючи аналіз кіберзагроз для кожного компонента системи окремо, можемо стикнутися зі значними витратами ресурсів, таких як час, кошти та потреба в більшій кількості кваліфікованих спеціалістів. Крім того, варто враховувати, що для доступу, наприклад, до внутрішніх елементів AR пристрою, зловмисник спершу мусить компрометувати сам пристрій. Таким чином, первинна атака на AR пристрій є ключовою загрозою, яку ми повинні враховувати.

З огляду узагальненої архітектури навчальної системи з доповненою реальністю (див. рисунок 2.3), бачимо, що кожен з компонентів містить у собі окремі елементи. Однак детальний аналіз кожного з цих елементів окремо не є оптимальним рішенням. В реальному світі така деталізація зазвичай використовується лише для систем, що мають особливу важливість, наприклад, урядових, військових, стратегічних або критично важливих об'єктів. Це пов'язано з тим, що компрометація їх даних може мати критичні наслідки на національному або навіть глобальному рівні. Саме тому, при моделюванні загроз безпеки, зосереджуємо свою увагу на ключових компонентах.

Розпочнемо моделювання загроз безпеки з векторів потенційних атак на AR пристрої нашої системи. На рисунку 3.8 продемонстровано вектори атак на AR пристрої.

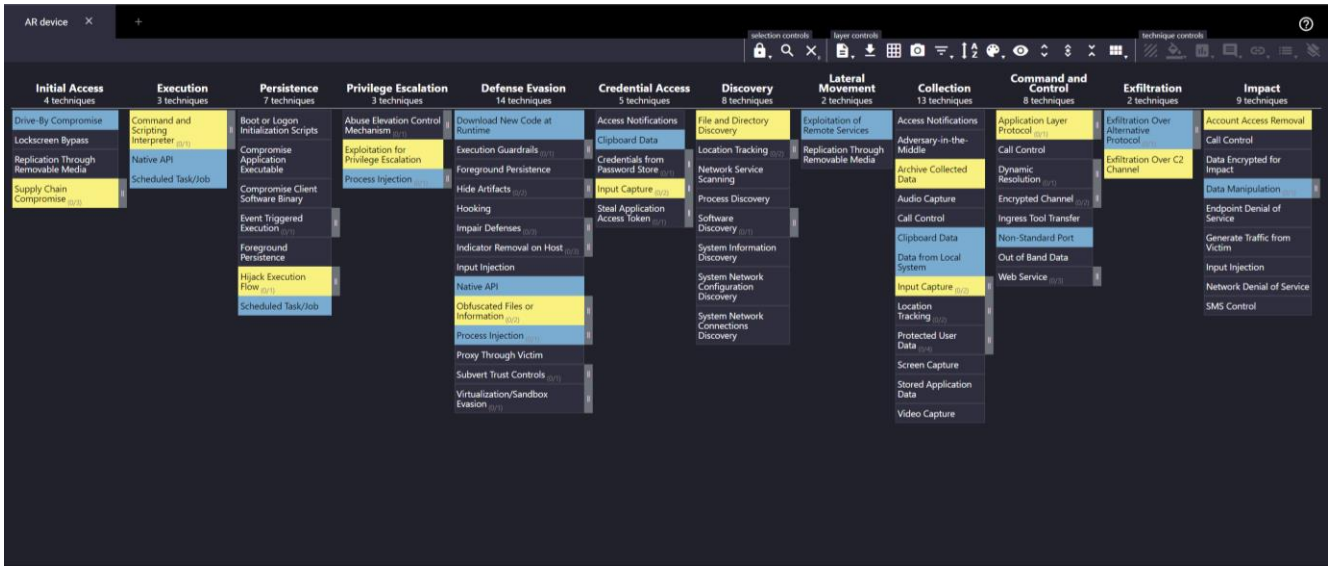

Рисунок 3.8 – Вектори атак на AR пристрої

Розглянемо кроки кожного з векторів. Перший вектор покроково складається з таких технік:

– Supply Chain Compromise - зловмисник використовує цю техніку для отримання доступу до системи, зазвичай шляхом компрометації компонентів програмного забезпечення або обладнання, яке використовується в окулярах AR.

– Command and Scripting Interpreter - зловмисник використовує цю техніку для запуску шкідливого коду на цільовому пристрої.

– Hijack Execution Flow - зловмисник використовує цю техніку для створення постійної присутності шкідливого коду, зазвичай шляхом зміни потоку виконання додатків або системних процесів.

– Exploitation for Privilege Escalation - техніка за якою зловмисник може підвищити свої привілеї на пристрої, набуваючи більшого контролю над системою.

– Obfuscated Files or Information - зловмисник використовує цю техніку для приховування присутності зловмисника та дій на пристрої.

– Input Capture – зловмисник використовує цю техніку для перехоплення користувацького вводу, наприклад, паролів або інших облікових даних.

– File and Directory Discovery - за допомогою цієї техніки зловмисник може дослідити систему, знаходячи важливі файли та директорії.

– Archive Collected Data - зловмисник використовує цю техніку для збору та архівації даних перед їхнім витоком.

– Application Layer Protocol - зловмисник використовує цю техніку для використання протоколів додатків для керування шкідливим кодом.

– Exfiltration Over C2 Channel - зловмисник використовує цю техніку для передачі зібраних даних через канал C2.

– Account Access Removal - останній етап, на якому зловмисник може видалити доступ до облікового запису, щоб завадити відновленню системи.

Другий вектор складається з таких кроків:

– Drive-By Compromise - зловмисник використовує цю техніку для отримання початкового доступу до пристрою, зазвичай шляхом компрометації веб-сайту, який користувач відвідує.

– Native API - зловмисник використовує цю техніку для виконання шкідливого коду на цільовому пристрої.

– Scheduled Task/Job - зловмисник використовує цю техніку для забезпечення постійної наявності шкідливого коду, зазвичай шляхом запуску завдань, які автоматично виконують шкідливий код.

– Process Injection - зловмисник використовує цю техніку для збільшення привілеїв на пристрої, внесенням коду зловмисника в довірчий процес.

– Download New Code at Runtime - зловмисник використовує цю техніку для завантаження нового шкідливого коду в процесі виконання.

– Clipboard Data - зловмисник використовує цю техніку для отримання доступу до даних, збережених у буфері обміну.

– Exploitation of Remote Services - зловмисник використовує цю техніку для переміщення по системі, експлуатуючи віддалені служби.

– Data from Local System – зловмисник використовує цю техніку для збору даних з локальної системи.

– Non-Standard Port - зловмисник використовує цю техніку нестандартного порту для управління шкідливим кодом та витоку даних.

– Exfiltration Over Alternative Protocol - зловмисник використовує цю техніку для передачі зібраних даних через альтернативний протокол.

– Data Manipulation - останній етап, на якому зловмисник виконує зміни в даних, може включати втрату, зміну або знищення даних.

Для моделювання загроз безпеки та векторів атаки для бази даних системи управління навчанням (Learning Management System, LMS), мережевого з'єднання та веб-інтерфейсу користувача, ви можна використовувати фреймворк MITRE ATT&CK для Enterprise.

Для моделювання вектора атаки на базу знань LMS (Learning Management System) через фреймворк MITRE Enterprise ATT&CK, ми можемо розглянути різні техніки, які можуть використовувати зловмисники. Бази даних, як правило, є основною метою, оскільки вони часто містять цінну інформацію. На рисунку 3.9 зображено вектори атак бази даних LMS.

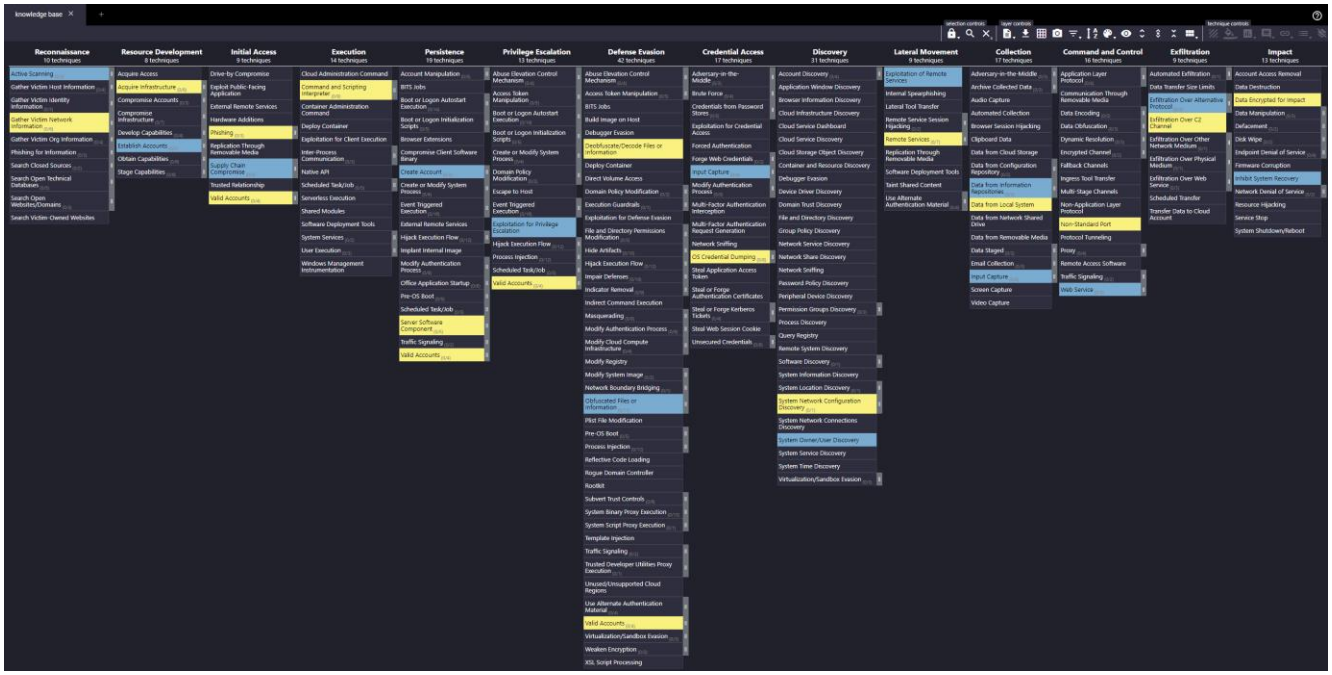

Рисунок 3.9 – Вектори атак на бази знань LMS

В першому векторі використовуються такі технології:

– Gather Victim Network Information – зловмисник проводить активні або пасивні дослідження для збору інформації про мережеву інфраструктуру системи LMS.

– Acquire Infrastructure - зловмисник створює інфраструктуру, необхідної для виконання атаки.

– Phishing – зловмисник надсилає шкідливе посилання користувачу LMS, наприклад, від імені служби підтримки LMS.

– Command and Scripting Interpreter – після отримання доступу зловмисник виконує команди для додаткового дослідження або для внесення шкідливих змін.

– Server Software Component – зловмисник додає шкідливий компонент до серверного програмного забезпечення LMS.

– Valid Accounts – зловмисник обходить контроль користувачів, щоб отримати більше прав в системі.

– Deobfuscate/Decode Files or Information – зловмисник приховує свої дії від систем безпеки.

– OS Credential Dumping – зловмисник витягує облікові дані користувачів із системи.

– System Network Configuration Discovery – зловмисник з'ясовує подробиці мережевої конфігурації LMS.

– Remote Services – зловмисник використовує w. техніку для руху по мережі та компрометації інших систем.

– Data from Local System – зловмисник збирає дані з локальної системи.

– Non-Standard Port – зловмисник використовує нестандартний порт для контролю шкідливого коду та витоку даних.

– Exfiltration Over C2 Channel – зловмисник передає зібрані дані через канал управління та контролю.

– Data Encrypted for Impact – зловмисник здійснює шифрування важливих даних на скомпрометованих системах з метою унеможливити доступ до них.

Другий вектор атак має таку послідовність використаних технік:

– Active Scanning - зловмисник проводить активне сканування для виявлення вразливостей у системі LMS.

– Establish Accounts - зловмисник створює фальшивий обліковий запис у системі LMS для подальшого використання.

– Supply Chain Compromise - зловмисник компрометує програмне забезпечення чи послуги, які використовує система LMS.

– Create Account - зловмисник створює додатковий обліковий запис для забезпечення постійного доступу до системи.

– Exploitation for Privilege Escalation - зловмисник використовує виявлені вразливості для підвищення своїх привілеїв у системі.

– Obfuscated Files or Information – зловмисник використовує обфускацію для приховування шкідливої активності.

– Input Capture - зловмисник встановлює keylogger для викрадення облікових даних користувачів.

– System Owner/User Discovery - зловмисник визначає власників або користувачів системи для подальшого цілеспрямованого атакування.

– Exploitation of Remote Services - зловмисник використовує вразливості віддалених сервісів для розповсюдження по мережі.

– Data from Information Repositories - зловмисник збирає дані з бази знань LMS.

– Command and Control - Web Service - зловмисник використовує веб-службу для управління шкідливим кодом.

– Exfiltration Over Alternative Protocol - зловмисник витягує дані через альтернативний протокол.

– Inhibit System Recovery - зловмисник знищує або модифікує дані для ускладнення відновлення системи.

Для мережевого з'єднання, атаки зазвичай зосереджуються на перехопленні трафіку, злому захисту мережі, або на спробах знищити стабільність мережі. Наступні вектори атаки засновані на моделі MITRE ATT&CK для мереж (див. рисунок 3.10).

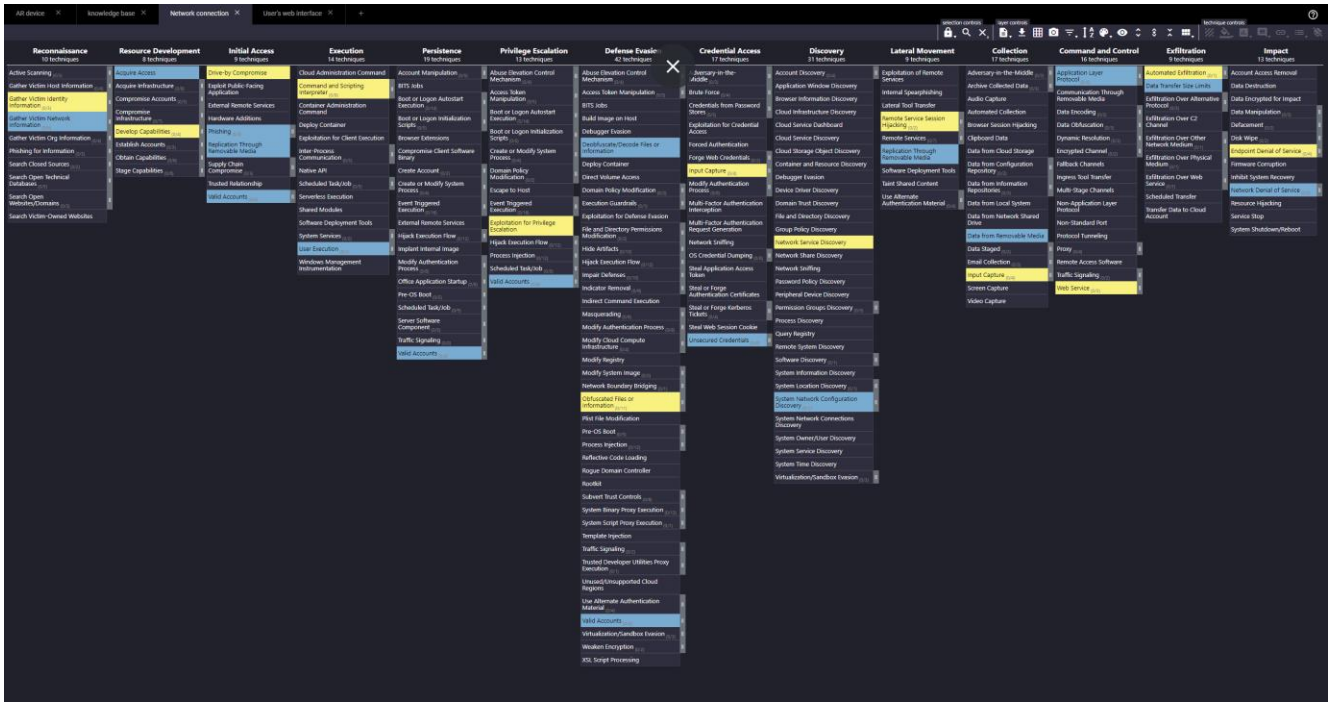

Рисунок 3.10 – Вектори атак на мережеві з’єднання

Перший вектор використовує такі технології:

– Gather Victim Identity Information - зловмисник може збирати інформацію про потенційні цілі в мережі, наприклад, імена облікових записів, групи, ролі та іншу інформацію про користувачів.

– Develop Capabilities - зловмисник може розробити спеціалізовані засоби або методики для подальших кроків атаки.

– Drive-by Compromise - зловмисник може використовувати вразливості в веб-браузерах для компрометації системи.

– Exploitation for Privilege Escalation – зловмисник використовує вразливості в системі для підвищення своїх привілеїв.

– Obfuscated Files or Information - зловмисник використовує обфускацію для приховування своєї активності.

– Input Capture - зловмисник встановлює keylogger для викрадення облікових даних користувачів.

– Network Service Scanning - зловмисник сканує мережеві сервіси для виявлення вразливостей.

– Lateral Movement - SSH Hijacking - зловмисник захоплює сеанси SSH для переміщення по мережі.

– Data from Network Shared Drive - зловмисник збирає дані з мережевих спільних дисків.

– Web Service - зловмисник використовує веб-службу для керування шкідливим кодом.

– Automated Exfiltration - зловмисник автоматично витягує дані з компрометованої системи.

– Endpoint Denial of Service - зловмисник запускає атаку типу "відмова в обслуговуванні", щоб виключити компрометовану систему з мережі.

Другий вектор атак має таку послідовність використаних технік:

– Gather Victim Network Information - зловмисник збирає інформацію про мережеву структуру, маршрутизацію та мережеве обладнання.

– Acquire Infrastructure - зловмисник придбає інфраструктуру, яку він використовує в атакі, наприклад, сервери для контролю та керування (C2).

– Phishing - зловмисник використовує спеціально підготовлені електронні листи для компрометації цілі.

– User Execution - зловмисник переконує користувача запустити шкідливе програмне забезпечення, яке він відправив.

– Valid Accounts - зловмисник використовує легітимні облікові записи для забезпечення свого присутності в мережі та для підвищення своїх привілеїв в системі.

– Deobfuscate/Decode Files or Information - зловмисник розшифровує або деобфускує файли та інформацію, щоб уникнути виявлення.

– Unsecured Credentials - зловмисник шукає та використовує незахищені облікові дані.

– System Network Configuration Discovery - зловмисник виявляє конфігурацію мережі системи для подальшого планування атаки.

– Replication Through Removable Media - зловмисник копіює файли через знімні носії для переміщення по мережі.

– Data from Removable Media - зловмисник збирає дані з знімних носіїв, які використовуються в мережі.

– Application Layer Protocol - зловмисник використовує протоколи верхнього рівня для управління.

– Data Transfer Size Limits - зловмисник обмежує розмір передачі даних, щоб уникнути виявлення.

– Network Denial of Service - зловмисник проводить атаку типу "відмова в обслуговуванні", щоб перешкодити доступу до мережі.

Веб-інтерфейси користувачів часто є основними мішенями для атак, оскільки вони слугують точками входу до системи. Використовуючи Enterprise ATT&CK фреймворк, ми можемо розробити наступні вектори атаки (див. рисунок 3.11):

– Active Scanning - зловмисник активно сканує веб-інтерфейс на наявність потенційних вразливостей або налаштувань за замовчуванням.

– Compromise Infrastructure - зловмисник може компрометувати сервер, на якому розміщений веб-інтерфейс, наприклад, через фішинг або експлойти.

– Drive-by Compromise - зловмисник може спробувати скомпрометувати веб-браузер користувача через веб-сторінку, що містить шкідливий код.

– System Services - шкідливий код виконується на сервері веб-інтерфейсу, маніпулюючи його сервісами.

– Server Software Component - використання служб системи зловмисниками як механізму виконання

– Exploitation for Privilege Escalation - зловмисник використовує вразливості в веб-інтерфейсі або серверному програмному забезпеченні для здобуття більших привілеїв.

– Obfuscated Files or Information - зловмисник використовує обфускацію для приховування шкідливих файлів або інформації від оборонних механізмів.

– Input Capture - зловмисник може використовувати keyloggers або подібні засоби для перехоплення введення користувача, такого як імена користувачів та паролі.

– File and Directory Discovery - зловмисник шукає файли та директорії, які можуть містити цінну інформацію.

– Exploitation of Remote Services - зловмисник може використовувати шкідливий код або вразливості для переходу до інших систем в мережі.

– Data from Information Repositories - зловмисник збирає дані з репозиторіїв інформації, таких як бази даних, які доступні через веб-інтерфейс.

– Web Service - зловмисник використовує веб-сервіси для контролю за компрометованою системою.

– Defacement - зловмисник може змінити веб-інтерфейс, щоб вплинути на репутацію або відволікти увагу від його дій.

Наступний вектор атак складається з таких технік:

– Search Victim-Owned Websites - зловмисник проводить пошук веб-сайтів, що належать потенційній жертві, для збору інформації.

– Establish Accounts - зловмисник створює облікові записи, які можуть бути використані пізніше в атаках.

– Drive-by Compromise - зловмисник використовує уразливості на веб-сайті для впровадження шкідливого коду, який буде виконуватися на системах користувачів при перегляді сайту.

– User Execution - зловмисник може спонукати користувача виконати шкідливий код, можливо, за допомогою соціальної інженерії або шкідливого файлу, прикріпленого до електронного листа.

– Valid Accounts - зловмисник використовує легітимні облікові записи, отримані в результаті фішингу або викрадення облікових даних, для постійного доступу до системи.

– Obfuscated Files or Information - зловмисник маскує шкідливі файли або інформацію для уникнення виявлення антивірусними програмами або механізмами оборони.

– Input Capture - зловмисник може захоплювати введення, такі як натискання клавіш, для отримання облікових даних користувача.

– System Information Discovery - зловмисник може зібрати важливу інформацію про систему, включаючи версії ОС, встановлене ПЗ тощо.

– Remote Services - зловмисник може використовувати віддалені служби для переміщення по мережі.

– Data from Information Repositories - зловмисник збирає дані з різних репозиторіїв інформації в системі, як-от бази даних.

– Exfiltration Over C2 Channel - зловмисник може вивантажувати зібрані дані через канал C2.

– Service Stop - на завершальному етапі зловмисник може зупинити важливі служби, щоб завдати шкоди системі або викликати перебої в роботі.

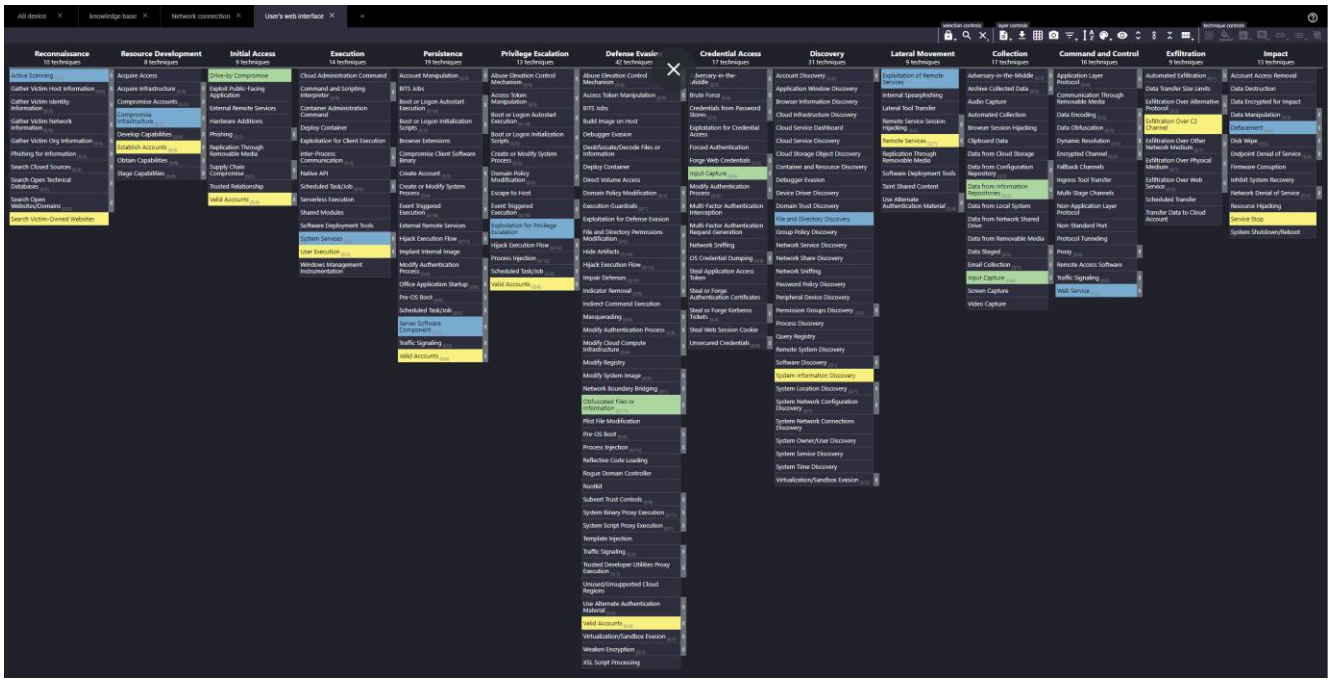

Рисунок 3.11 – Вектори атак на веб інтерфейс користувача

Описані етапи включають різні тактики, які зловмисники можуть використовувати для атаки на систему через веб-інтерфейс.

Кожен компонент системи (база даних LMS, мережеве з'єднання, веб-інтерфейс користувача, пристрої доповненої реальності) має свої слабкі місця, і різні вектори атак можуть бути застосовані до кожного з них. Проте, оскільки ці компоненти також взаємодіють одна з одною, атака на один компонент може вплинути на інші.

Щоб отримати загальну картину загроз системи, необхідно накласти вектори атак кожного компонента системи один на одного, тим самим змоделювати загрози безпеки для цілої навчальної системи з доповненою реальністю (див. рисунок 3.12). Це допоможе ідентифікувати нові потенційні вектори атак, які виникають в результаті взаємодії між компонентами системи. Така інтеграція векторів атак також допоможе виявити можливі стратегії оборони, щоб зміцнити систему і зменшити її вразливість перед різними видами загроз.

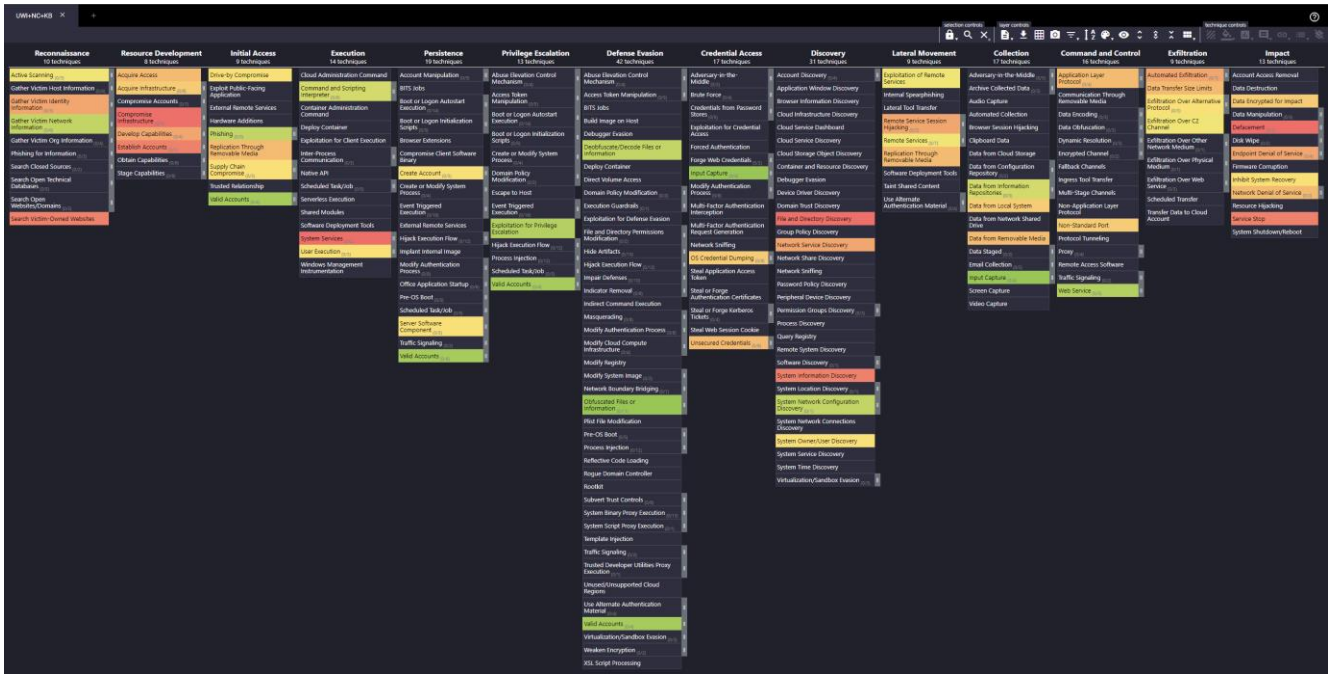

Рисунок 3.12 – Модель загроз безпеки навчальної системи з доповненою реальністю

MITRE ATT&CK Navigator надає можливість об'єднувати матриці лише одного типу. Наприклад, матриці, що входять до Enterprise ATT&CK, не можна поєднувати з матрицями Mobile ATT&CK. Отже, для створення моделі загроз безпеки навчальної системи з доповненою реальністю, ми використовували накладання шарів, що відповідають компонентам: User's AR device, LMS knowledge base, Network connection, User web-interface. На рисунку 3.12 можемо бачити цю модель, де кожен шар відображається окремо і містить відповідні матриці загроз. Злиття цих шарів дозволяє нам отримати узагальнений огляд загроз безпеки для системи, що використовує доповнену реальність. Використовуючи MITRE ATT&CK Navigator, ми отримуємо цінний інструмент для аналізу загроз та розробки ефективних стратегій кіберзахисту.

3.4 Розробка заходів та засобів забезпечення безпеки

Працюючи над моделюванням векторів атак, було створено карту потенційних слабких місць в нашій навчальній системі з доповненою реальністю. Кожен компонент системи - база даних LMS, мережеве з'єднання, веб-інтерфейс

користувача і пристрої доповненої реальності - виявився вразливим для конкретного набору технік атаки, що відображено в створених векторах атак.

Враховуючи цю інформацію, можемо перейти до розробки ефективних заходів та засобів забезпечення безпеки. Цей процес вимагає системного підходу: не тільки аналізу потенційних слабких місць та розробки стратегій їх усунення, але і розуміння того, як різні компоненти взаємодіють між собою і як атака на один компонент може вплинути на інші.

На основі аналізів та розуміння архітектури системи, пропонуються наступні загальні рекомендації щодо заходів та засобів забезпечення безпеки для кожного компонента:

1) База знань Learning Management System (LMS):
– Регулярне створення резервних копій і відновлення бази даних.
– Використання захищених протоколів для передачі даних.
– Шифрування даних.
– Автентифікація на основі ролей.
– Регулярне оновлення бази даних.
– Використання систем захисту від вторгнень (IDS/IPS).
2) Мережеві з'єднання:
– Використання захищених протоколів.
– Обмеження віддаленого доступу.
– Використання фаєрволів та IDS/IPS.
3) Веб-інтерфейс користувача:
– Регулярне оновлення веб-серверів та програмного забезпечення.
– Використання веб-застосувань файрволів (WAF).
– Застосування HTTPS та інших захищених протоколів.
– Використання багатофакторної автентифікації.
– Активне моніторинг та аудит веб-логів.
4) Пристрої доповненої реальності:
– Оновлення пристроїв та їх програмного забезпечення.
– Використання шифрування для захисту даних.
– Обмеження віддаленого доступу до пристроїв.

– Проведення регулярного аудиту та перегляду логів пристроїв.

Безпека має важливе значення для забезпечення приватності та захисту цих даних. Крім того, забезпечення безпеки є ключовим для впевненості користувачів у тому, що їхні дані захищені. Це, в свою чергу, сприяє довірі до системи та її широкому використанню.

Більше того, наслідки атаки на навчальну систему можуть включати втрату або пошкодження важливих даних, порушення нормального функціонування системи та навіть її повну відмову. Це може призвести до перебоїв у навчальному процесі, а також до фінансових збитків.

З урахуванням всього вищевказаного, можна зрозуміти, наскільки важливим є забезпечення безпеки навчальної системи з доповненою реальністю. Це не лише запобігає потенційним загрозам, але й сприяє створенню надійного та ефективного навчального середовища.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Психофізіологічне розвантаження для працівників

Успішна профілактика виробничого травматизму можлива лише за умови ретельного вивчення причин їх виникнення, в тому числі психофізіологічних.

Психофізіологічні причини – помилкові дії внаслідок втоми працівника через надмірну важкість і напруженість роботи, монотонність праці, хворобливий стан працівника, необережність, невідповідність психофізіологічних чи антропометричних даних працівника використовуваній техніці чи виконуваній роботі.

До небезпечних та шкідливих психофізіологічних виробничих чинників належать фізичні (статичні, динамічні) і нервово-психічні перевантаження (розумова перенапруга, монотонність праці, перенапруження зорового, слухового, тактильного аналізаторів, емоційні перевантаження).

Робота працівників у сфері інформаційних технологій характеризується:

– тривалою багатогодинною (8 годин і більше) працею в одноманітному напруженому положенні;

– малою руховою активністю при значних локальних динамічних навантаженнях кістково-м’язового апарату кистей рук.

Трудова діяльність комп’ютерних і програмних інженерів належить до категорії робіт, які пов’язані з використанням великих обсягів інформації, із застосуванням комп’ютеризованих робочих місць, із частим прийняттям відповідальних рішень в умовах дефіциту часу та безпосереднім контактом із людьми різних типів темпераменту.

Тривала робота на комп’ютеризованому робочому місці призводить до значного навантаження на всі елементи зорової системи. Напружена зорова робота викликає біль, печію та різь в очах, почервоніння повік та очей. Все це зумовлює високий рівень нервово-психічного перевантаження, знижує функціональну активність центральної нервової системи, призводить до розвитку втоми, стресу.

Праця таких професій як будівельники, сільськогосподарські працівники і механізатори, працівники деревообробної, нафтової, газової промисловостей, металурги, ливарники та вантажники є обумовлена надмірним фізичним перевантаженням, що призводить до втоми м'язів через їх напруження. Чим більше навантаження та тривалість напруження м'яза, то швидше він втомлюється.

Надмірні фізичні та нервово-психічні перевантаження зумовлюють зміни у фізіологічному та психічному станах працівника, призводять до розвитку втоми та перевтоми.

Як відомо, розвиток втоми та перевтоми веде до порушення координації рухів, зорових розладів, неуважності, втрати пильності та контролю реальної ситуації. При цьому працівник порушує вимоги технологічних інструкцій, припускається помилок та неузгодженості в роботі; у нього знижується відчуття безпеки. Спостерігається погіршення сприйняття подразників, внаслідок чого працівник окремі подразники зовсім не сприймає, а інші сприймає із запізненням; зменшення здатності концентрувати увагу, свідомо її регулювати; посилення мимовільної уваги до побічних подразників, які відволікають працівника від трудового процесу; погіршення запам'ятовування та труднощі пригадування інформації, що знижує ефективність професійних знань; сповільнення процесів мислення; підвищення дратівливості, поява депресивних станів, зміни частоти слуху, зору.

Це призводить до того, що ближче до кінця робочої зміни збільшується кількість випадків виробничого травматизму. Згідно статистичних даних, кожному четвертому випадку передувала явно виражена втома.

Основні заходами у запобіганні втомлюваності, а отже і у попередженні виникнення виробничого травматизму є:

– механізація і автоматизація виробничих процесів – вони усувають фізичне напруження і велику кількість рухів руками;

– покращення санітарно-гігієнічних умов виробничого середовища (площа приміщень, мікрокліматичні умови, освітлення, вентиляція, опалення);

– професійний відбір;

– раціональна організація робочого місця, яка має бути спрямована на те, щоб конструкція виробничого устаткування відповідала антропометричним даним і психофізіологічним можливостям людини;

– правильне робоче положення; ритм роботи;

– раціоналізація трудового процесу;

– використання емоційних стимулів, впровадження раціональних режимів праці та відпочинку;

– виконання комплексу вправ для очей, рук та хребта для поліпшення мозкового кровообігу, а також комплексу прийомів психофізіологічного розвантаження.

Безпека праці є основною гарантією стабільності та якості будь якого виробництва. Відсутність випадків виробничого травматизму позначається на професійній активності працюючих, на моральному кліматі в колективі, а отже і на ефективності та продуктивності праці.

4.2 Долікарська допомога при вивихах

Вивихи - це поширена травма, яку можна отримати не тільки під час спортивних заходів, але й в повсякденному житті. В той же час, вони виступають потенційною загрозою для кожного, хто відкриває для себе світ доповненої реальності - новий вимір, що дарує необмежені можливості, але й несе у собі потенційні ризики. Сенсори або програмне забезпечення доповненої реальності можуть дещо спотворювати реальність, що призводить до некоректного сприйняття простору, несподіваних падінь та, як наслідок, до вивихів. Нагадаємо, що вивихи часто відбуваються через несподівані події, такі як випадкове падіння, зіткнення з предметами або некоректні рухи. Вони можуть спричиняти значний дискомфорт, біль та обмеження функцій суглобу, що в свою чергу значно впливає на якість життя постраждалих. Сучасні технології можуть дозволити нам відійти від реальності, але вони не в змозі відмінити фізичність наших тіл, відчуття болю та емоцій, які вони спричиняють. Тому навички надання ефективної долікарської

допомоги при вивихах мають велике значення для швидкого полегшення страждань постраждалого та запобігання подальшим ускладненням.

Вивих - це травма, яка виникає, коли кінці кісток, що утворюють суглоб, зсуваються зі свого звичного положення, при цьому одна з кісток може вийти за межі своєї звичайної позиції. Цей зсув стає можливим через розрив капсули суглоба або інших структур, що утримують кістки у суглобовій порожнині, що призводить до виходу однієї кістки з суглобової порожнини і її неправильного розташування.

Вивих може бути двох типів:

– повний вивих: в цьому випадку суглобові поверхні кісток повністю перестають стикатися одна з одною. Це означає, що кістка повністю вийшла зі свого звичайного положення в суглобовій порожнині. Повний вивих може бути видимим зовні, де можна спостерігати деформацію та видиме відхилення в структурі суглобу;

– неповний вивих: у цьому випадку між суглобовими поверхнями є часткове зіткнення, але їх положення все ж не відповідає нормальному анатомічному стану. Це може відбуватися через незначний зсув кісток або неправильну орієнтацію суглобових поверхонь.

Симптомами вивиху включають:

– біль: постраждала кінцівка дуже болюча. Біль може бути гострим, інтенсивним і збільшується при спробі руху або при натисканні на пошкоджений суглоб;

– деформація ділянки: вивих може викликати замітну деформацію в місці пошкодження. Це може виявлятися у вигляді неправильної анатомічної форми суглобу, видимого зсуву кісток або незвичайного розташування суглобних поверхонь;

– відсутність активних і пасивних рухів в суглобі: постраждалий може не здатний здійснювати нормальні рухи в суглобі, навіть при активній спробі. Зсув кісток у суглобі може призводити до блокування руху або значного обмеження діапазону руху.

Ці симптоми є ключовими показниками вивиху і їх наявність вказує на потребу в негайній долікарській допомозі та медичному втручанні для відновлення правильного положення кісток у суглобі.

Домедична допомога при вивихах включає такі заходи:

– застосування знеболюючих речовин: у постраждалого може бути надана анальгетика, наприклад, 0,25-0,5 г анальгіну, для полегшення болю. Проте, слід пам'ятати, що самолікування не рекомендується, і перед вживанням будь-яких лікарських препаратів слід звернутися до кваліфікованого медичного працівника;

– іммобілізація кінцівки: для запобігання подальшому пошкодженню та забезпечення стабільності постраждалого суглобу, кінцівку слід іммобілізувати в тому положенні, яке вона прийняла після вивиху. Це може бути здійснено за допомогою шин або підручних засобів, що дозволяють утримувати суглоб у правильному положенні;

– фіксація верхньої кінцівки: якщо вивих стосується верхньої кінцівки, наприклад, плечового суглобу, може бути застосована косинка або інша спеціальна фіксаційна конструкція для стабілізації та утримання кінцівки у відповідному положенні;

– транспортування до лікувальної установи: в разі вивиху потерпілий повинен бути якомога швидше транспортований до лікувальної установи, де медичний персонал зможе провести вправлення вивиху та надати подальше лікування;

– уникання самовправлення: не рекомендується намагатися самостійно вправити вивих, оскільки це може бути небезпечним та призвести до подальшого ушкодження. Крім того, вивихи часто супроводжуються тріщинами або переломами кісток, тому важливо звернутися до медичного фахівця для правильної діагностики та встановлення оптимального плану лікування.

Важливо пам'ятати, що домедична допомога при вивихах має на меті лише тимчасове стабілізування постраждалого суглобу і негайне звернення до кваліфікованого медичного фахівця є обов'язковим для подальшого лікування та вправлення вивиху.

Коли стикаєтеся з вивихом, надання домедичної допомоги є важливим етапом у процесі лікування та зменшення незручностей для постраждалої особи. Особливості цієї допомоги включають:

– спокій та забезпечення комфорту: важливо уникати будь-яких рухів, які можуть спричиняти біль. Допоможіть постраждалому зайняти найзручніше для нього положення;

– забезпечення нерухомості пошкодженої частини тіла: для запобігання подальшим ушкодженням та забезпечення стабільності постраждалого суглобу, використовуйте засоби для іммобілізації, такі як шина або підручні матеріали, щоб утримувати суглоб у правильному положенні;

– застосування холоду: при будь-якій травмі, за винятком відкритого перелому, можна прикласти холод. Холод допомагає зменшити біль і припухлість шляхом звуження кровоносних судин;

– режим застосування холоду: холодний компрес слід прикладати на пошкоджену область протягом 15 хвилин через кожну годину [ ]. Захистіть шкіру, розмістивши між компресом і шкірою прокладку з марлі або тканини.

– використання компресу: можна зробити компрес, поклавши лід у поліетиленовий пакет і обмотавши його рушником;

– обережність при відкритих переломах: не застосовуйте холодний компрес при відкритому переломі, оскільки тиск на місце перелому може викликати болісні відчуття;

– підведення пошкодженої частини тіла: підведення ушкодженої ділянки допомагає зменшити кровотік та припухлість. Постраждалу кінцівку можна підтримати піднятою за допомогою подушки або іншого підкладеного предмета.

ВИСНОВКИ

В межах даної кваліфікаційної роботи було проведено згруповане дослідження, що охоплює різні аспекти використання технології доповненої реальності в освітніх системах. Основний акцент дослідження було зроблено на аналізі та моделюванні потенційних загроз безпеки, з урахуванням специфіки навчальних систем, що використовують доповнену реальність.

Результатом аналізу технологій доповненої реальності стало глибоке розуміння потенціалу цих технологій та можливих ризиків, пов'язаних із їх використанням у навчальному процесі. Аналіз узагальненої архітектури навчальних систем, що використовують доповнену реальність, дозволив виявити найбільш вразливі складові та способи їх захисту.

Основна мета даного дослідження полягала в моделюванні потенційних загроз безпеки з використанням фреймворку MITRE ATT&CK. Адаптація цього інструментарію для потреб навчальних систем доповненої реальності дозволила побудувати повноцінну модель загроз та виробити стратегії протидії.

Результати дослідження є значними з погляду практичної реалізації. Вони забезпечують перспективу для підвищення надійності та безпеки систем доповненої реальності, що використовуються в освіті. Подальше застосування отриманих результатів може сприяти безпечному впровадженню та використанню систем доповненої реальності в освітніх установах.

Отже, проведена робота забезпечує значний внесок в галузь безпеки інформації, що є основою для подальшого розвитку технологій доповненої реальності в освіті. Дані, отримані в результаті аналізу, виявляють нові горизонти для досліджень в цій сфері, зокрема, стосовно впровадження розроблених механізмів захисту та стратегій протидії загрозам.

Окрім того, результати цього дослідження можуть бути використані як основа для розробки нових методів оцінки ризиків, визначення вразливостей і заходів їх запобігання у системах доповненої реальності, що використовуються в освіті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Virtual and Augmented Reality: Concepts, Methodologies, Tools, and Applications / Management Association, Information Resources. – IGI Global, 2023. – 1800 с.

2. Cybersecurity for the Digital Age: A Learning Guide for Executives to Understand the Risks and Challenges of Cybersecurity / Gartner Research. – Gartner, Inc., 2023. – 320 с.

3. Chuvakin A. Security Threat Modeling Using the ATT&CK Framework / Anton Chuvakin, Augusto Barros. – O'Reilly Media, Inc., 2023. – 420 с.

4. Azuma R. T. A Survey of Augmented Reality / Ronald T. Azuma. – Presence: Teleoperators & Virtual Environments, 1997. – 6 (4). – С. 355–385.

5. MITRE ATT&CK: A Comprehensive Guide [Електронний ресурс] / MITRE Corporation. – 2023. – Режим доступу: https://attack.mitre.org/ - Дата звернення: 10.06.2023.

6. 12 Available Methods [Електронний ресурс] / Software Engineering Institute, Carnegie Mellon University. – 2023. – Режим доступу: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/ - Дата звернення: 17.06.2023.

7. Top Threat Modeling Frameworks: STRIDE, OWASP Top 10, MITRE ATT&CK Framework [Електронний ресурс] / InfoSec Institute. – 2023. – Режим доступу: https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/ - Дата звернення: 17.06.2023.

8. MITRE ATT&CK Framework for Cyber Threats [Електронний ресурс] / Cybersecurity and Infrastructure Security Agency. – 2023. – Режим доступу: https://www.cisa.gov/mitre-attck-framework - Дата звернення: 17.06.2023.

9. Hermann E. Practical Augmented Reality: A Guide to the Technologies, Applications, and Human Factors for AR and VR / Steve Aukstakalnis. – Addison-Wesley Professional, 2016. – 448 с.

10. Oliva J. G. Cybersecurity: A Review and Taxonomy of Cyber Threat Information Sharing / José Guerra Oliva, David Cano Basave. – ACM Computing Surveys, 2023. – 56 (1). – С. 1-33.

11. Mapping Security Controls to ATT&CK Behaviors [Електронний ресурс] / MITRE Corporation. – 2023. – Режим доступу: https://www.mitre.org/publications/technical-papers/mapping-security-controls-to-attck-behaviors - Дата звернення: 17.06.2023.

12. Check Point Research: Cyber Attacks Increased 50% Year over Year [Електронний ресурс] / Check Point Software Technologies Ltd. – 2023. – Режим доступу: https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/ - Дата звернення: 17.06.2023.

13. Baiardi G., Chiti F. Security and Privacy Threats in Augmented Reality Systems: A Survey / G. Baiardi, F. Chiti et al. // ACM Computing Surveys. – 2019. – Vol. 52, No. 5, Article 104.

14. Saleh M., Moustafa N. Security Analysis of Augmented Reality Applications on Android / M. Saleh, N. Moustafa et al. // IEEE Transactions on Dependable and Secure Computing. – 2020. – Vol. 18, No. 1. – С. 144-157.

15. Rahman A. Security and Privacy Challenges in Augmented Reality: Current Status and Future Directions / A. Rahman et al. // IEEE Access. – 2021. – Vol. 9. – С. 54731-54752.

16. Tomlinson R. Using the MITRE ATT&CK Framework to Improve Cybersecurity Policies / Rob Tomlinson. – InfoSec Magazine, 2023. – 22 (5). – С. 14-18.

17. ATT&CK: Design and Philosophy [Електронний ресурс] / MITRE Corporation. – 2020. – 17 с. – Режим доступу: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf - Дата звернення: 17.06.2023.

18. Carmigniani J., Furht B., Anisetti M., Ceravolo P., Damiani E., Ivkovic M. Augmented Reality Technologies, Systems and Applications / J. Carmigniani, B. Furht, M. Anisetti, P. Ceravolo, E. Damiani, M. Ivkovic // Multimedia Tools and Applications. – 2011. – Vol. 51, No. 1. – С. 341–377.

19. LMS Guide: Learning Management System Architecture [Електронний ресурс] / Raccoon Gang. – 2022. – Режим доступу: https://raccoongang.com/blog/lms-guide-learning-management-system-architecture/ - Дата звернення: 17.06.2023.

20. Watson W.R., Watson S.L. Learning Management Systems: An Overview / W.R. Watson, S.L. Watson // In: Technology, Pedagogy and Education. – 2007. – Vol. 16, No. 3. – C. 317–332.

21. Graphanathan Y., Dutta K. A Study of the Learning Management System Using Component Based Software Engineering / Y. Graphanathan, K. Dutta // In: Procedia Engineering. – 2012. – Vol. 38. – C. 3454-3461.

22. MITRE ATT&CK Navigator [Електронний ресурс] / MITRE Corporation. – 2023. – Режим доступу: https://mitre-attack.github.io/attack-navigator/ - Дата звернення: 17.06.2023.

23. The Use of the ATT&CK Navigator in Threat Analysis and Assessment [Електронний ресурс] / Cybersecurity and Infrastructure Security Agency. – 2023. – Режим доступу: https://www.cisa.gov/publication/use-attck-navigator-threat-analysis-and-assessment - Дата звернення: 17.06.2023.

24. Fowler, S. Cyber Threat Analysis with MITRE ATT&CK Navigator / Scott Fowler. – ITProPortal, 2023. – (1). – C. 10–13.

25. MITRE ATT&CK Navigator: A Comprehensive Guide / IT Security Centre UK. – 2023. – Режим доступу: https://www.itsecuritycentre.co.uk/mitre-attck-navigator - Дата звернення: 17.06.2023.