Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Автоматики і комп'ютеризованих технологій
(повна назва)

Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розроблення програмного модуля для кібербезпеки виробничого обладнання
(тема)

Виконав:
Здобувач 4 року навчання,
групи АКТАКІТ-21-2
Антон ФОМЕНКО
(власне ім'я прізвище)
Спеціальності 151 Автоматизація та комп`ютерно-інтегровані технології
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Автоматизація та комп`ютерно-інтегровані технології
(повна назва освітньої програми)
Керівник доцент Світлана МАКСИМОВА
(посада, власне ім'я прізвище)

Допускається до захисту

Завідувач кафедри КІТАР _____ Ігор НЕВЛЮДОВ
(підпис) (власне ім'я прізвище)

2025 р.

Я, Фоменко Антон Денисович, як здобувач вищої освіти ХНУРЕ, розумію та підтримую політику закладу з академічної доброчесності. Я не надавав і неодержував недозволену допомогу під час підготовки кваліфікаційної роботи. Я не використовував штучний інтелект для підготовки кваліфікаційної роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

«15» червня 2025 р. _____ Антон ФОМЕНКО

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Факультет Автоматики і комп'ютеризованих технологій
Кафедра Комп'ютерно-інтегрованих технологій, автоматизації та робототехніки
Рівень вищої освіти перший (бакалаврський)
Спеціальність 151 Автоматизація та комп`ютерно-інтегровані технології
Тип програми освітньо-професійна
Освітня програма Автоматизація та комп`ютерно-інтегровані технології
(шифр і назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри КІТАР _____
(підпис)
« 28 » квітня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Фоменку Антону Денисовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення програмного модуля для кібербезпеки виробничого обладнання
затверджена наказом по університету від " 19 " травня 2025р. № 390 Ст.
2. Термін подання здобувачем роботи " 25 " червня 2025р.
3. Вихідні дані до роботи 3.1 Локальна обчислювальна мережа;
3.2 Програмне забезпечення для створення бази даних – CosmosDB;
3.3 Програмне забезпечення для створення серверної частини – Azure Cloud Services;
3.4 Мова програмування – C#;
3.5 Операційна система – Microsoft Windows 10.

4. Перелік питань, що потрібно опрацювати в роботі 4.1 Вступ;
4.2 Аналіз технічного завдання та предметної області;
4.3 Розроблення компонентів програмного модуля кібербезпеки локальної обчислювальної мережі виробничого підприємства;
4.4 Розроблення програмного модуля кібербезпеки локальної обчислювальної мережі виробничого підприємства;
4.5 Охорона праці;
4.6 Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) Демонстраційний матеріал представлений у форматі презентації PowerPoint (*.ppt) – 18 с. формату А4

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз технічного завдання та предметної області	28.04 – 04.05.25	виконано
2	Розроблення компонентів програмного модуля кібербезпеки локальної обчислювальної мережі виробничого підприємства	05.05 – 14.05.25	виконано
3	Розроблення програмного модуля кібербезпеки локальної обчислювальної мережі виробничого підприємства	15.05 – 28.05.25	виконано
4	Охорона праці	29.05 – 11.06.25	виконано
5	Оформлення пояснювальної записки	12.06 – 15.06.25	виконано
6	Подання роботи на перевірку Інтернет-системою StrikePlagiarism	16.06 – 18.06.25	виконано
7	Подання роботи на рецензію	19.06 – 21.06.25	виконано
8	Подання роботи на підпис зав. кафедри	22.06 – 24.06.25	виконано
9	Подання кваліфікаційної роботи в ЕК	25.06.25	виконано

Дата видачі завдання 28.04.2025р.

Здобувач _____ Антон ФОМЕНКО
(підпис)

Керівник роботи _____ доцент Світлана МАКСИМОВА
(підпис) (посада, власне ім'я прізвище)

РЕФЕРАТ

Пояснювальна записка: 70 с., 7 табл., 23 рис., 2 дод., 15 джерел.

ПРОГРАМНИЙ МОДУЛЬ, КІБЕРБЕЗПЕКА, ЛОКАЛЬНА ОБЧИСЛЮВАЛЬНА МЕРЕЖА, ВИРОБНИЧЕ ПІЛПРИЄМСТВО, ФУНКЦІОНАЛЬНА МОДЕЛЬ, ІНТЕРФЕЙС КОРИСТУВАЧА.

Мета роботи – розроблення програмного модуля для кібербезпеки локальної обчислювальної мережі виробничого підприємства.

Об’єкт розробки – кібербезпека локальної обчислювальної мережі виробничого пілприємства.

Предмет розробки – програмний модуль для кібербезпеки локальної обчислювальної мережі виробничого пілприємства.

Результати та їх новизна – реалізовано програмний модуль кібербезпеки локальної обчислювальної мережі, що забезпечить якісне та ефективне управління мережею, та дозволить отримувати високі показники надійності у функціонуванні та передачі інформації.

У кваліфікаційній роботі проведено аналіз особливостей захисту інформації локальної обчислювальної мережі. Розроблено принцип функціонування програмного модуля та його функціональну модель. Обрано метод кібербезпеки локальної обчислювальної мережі. Проведено розробку компонентів програмного модуля, інтерфейсу користувача та випробування програмного модуля. Опрацьовано питання, пов'язані з охороною праці.

Отримані результати роботи можна віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», зокрема до пункту 9.4 «Розвиток високотехнологічного машинобудування».

ABSTRACT

Explanatory note: 70 pp., 7 tab., 23 figs., 2 appendices, 15 sources.

PROGRAM MODULE, CYBERSECURITY, LOCAL AREA NETWORK, MANUFACTURING ENTERPRISE, FUNCTIONAL MODEL, USER INTERFACE.

Purpose – to develop a software module for cybersecurity of a local area network of a manufacturing enterprise.

Object of development – cybersecurity of the local computer network of a manufacturing enterprise.

Subject of development – a software module for cybersecurity of a local area network of a manufacturing enterprise.

Results and novelty – a software module for cybersecurity of a local area network has been implemented, which will ensure high-quality and efficient network management and will allow obtaining high reliability indicators in the functioning and transmission of information.

The qualification work analyzes the peculiarities of protecting the information of a local area network. The principle of functioning of the program module and its functional model are developed. The method of cybersecurity of a local area network is chosen. The components of the program module, the user interface, and the testing of the program module were developed. Issues related to labor protection have been worked out.

The results of the work can be attributed to Sustainable Development Goal 9 “Industry, Innovation and Infrastructure”, in particular to paragraph 9.4 “Development of high-tech engineering”.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система;

БД – база даних;

ДНК – дезоксирибонуклеїнова кислота;

ЕОМ – протоколів обміну даними;

КПО – коефіцієнт природної освітленості;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

GPS (Global Positioning System) – супутникова система навігації;

LAN (Local Area Network) – локальна обчислювальна мережа;

NAT (Network Address Translation) – перетворювач мережевого адресу.

ВСТУП

Еволюція нових інформаційних технологій, а також удосконалення потужних комп'ютерних систем зберігання та оброблення інформації спричинили підвищення вимог щодо рівня захисту інформації, зокрема, обґрунтували необхідність розроблення ефективних механізмів кібербезпеки, що адаптовані відповідно до сучасних архітектур зберігання даних. Зважаючи на це, поступово захист економічної інформації набуває обов'язкового впровадження. Так, розробляється безліч документів щодо захисту інформації, до того жстворюються рекомендації щодо кібербезпеки.

Забезпечення захисту інформації на виробництві характеризується як безперервний процес, який полягає у послуговуванні сучасними методами, забезпеченні контролю щодо зовнішнього та внутрішнього середовища підприємства, організації та реалізації заходів щодо підтримки стабільного функціонування локальної мережі та обчислювальної техніки, а також мінімізації втрат у зв'язку з витоком інформації. З метою запровадження кібербезпеки, як у мережах, так і на виробництві, на підприємствах доцільно сформувати певний звід правил і нормативних документів, які регламентуватимуть дії співробітників щодо забезпечення безпекий окреслюватимуть технічні та програмні модулі для кібербезпеки.

Так, політика інформаційної безпеки спирається на мінімізацію ризиків витоку інформації на підприємстві, а також забезпечення сталого функціонування інформаційної структури підприємства. Це може призвести до фінансових втрат через виток інформації, тому доречно приділяти пильну увагу питанням інформаційної безпеки.

Отже, загроза захисту інформації посприяла тому, що засоби забезпечення інформаційної безпеки стали одними з обов'язкових елементів інформаційної політики будь-якої організації. Перефразуємо, питання кібербезпеки розв’язуються для того, щоб ізолювати інформаційну систему,

що нормально функціонує, від несанкціонованих впливів керування, а також запобігти доступу сторонніх осіб або програм до даних задля розкрадання.

Актуальність роботи визначається необхідністю задовольнити підвищений попит на програмні модулі кібербезпеки.

Мета роботи – розроблення програмного модуля для кібербезпеки локальної обчислювальної мережі виробничого підприємства.

Об’єкт розробки – кібербезпека локальної обчислювальної мережі виробничого пілприємства.

Предмет розробки – програмний модуль для кібербезпеки локальної обчислювальної мережі виробничого пілприємства.

Задля досягнення окресленої мети доцільно розв’язати такі завдання:

– вивчити особливості захисту інформації локальної обчислювальної мережі;

– проаналізувати роботу програмних модулів кібербезпеки;

– виконати опис принципу функціонування програмного модуля кібербезпеки;

– розробити функціональні моделі програмного модуля;

– обрати програмні модулі для програмування;

– дібрати метод кібербезпеки локальної обчислювальної мережі;

– розробити інтерфейс користувача програмного модуля;

– реалізувати випробування програмним модулем;

– розв’язати питання, що пов’язані з охороною праці.

Пояснювальну записку кваліфікаційної роботи оформлено згідно з ДСТУ 3008:2015 [1], а також з рекомендаціями з підготовки і оформлення кваліфікаційної роботи здобувачами першого (бакалаврського) рівня вищої освіти [2-3], отримані результати роботи можна віднести до Цілі сталого розвитку 9 «Промисловість, інновації та інфраструктура», зокрема до пункту 9.4 «Розвиток високотехнологічного машинобудування».

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ТА ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз особливостей кібербезпеки локальної обчислювальної мережі

Локальна мережа складається з групи комп’ютеріві периферійних пристроїв, які застосовують спільну лінію зв'язку або бездротове з’єднання з сервером у межах окремої географічної області. Локальною мережею можуть послуговуватися не менше двох або трьох користувачів у домашньому офісічи кілька сотень користувачів у центральному офісі корпорації. Так, власники будинків або адміністратори інформаційних технологій налаштовують локальні мережі, щоб мережеві вузли могли обмінюватися ресурсами, зокрема, принтери чи мережеві сховища [4].

У цілому є два типи локальних мереж: однорангові та клієнт-серверні.

Клієнт-серверна локальна мережа ґрунтується на клієнтах (хоча б одному), котрі підключені до центрального серверу. Зі свого боку, сервер містить такі зобов’язання, як-от: зберігання файлів, доступ до застосунків, а також до пристроїв, вихідний мережевий трафік. Клієнт може підключатися через будь-який пристрій, який запускає чи звертається до застосунків або Інтернету. Клієнти підключаються до сервера шляхом застосування кабелів або бездротового з’єднання.

Здебільшого набори застосунків можуть зберігатися на сервері локальної мережі. Так, користувачі можуть отримувати доступ до баз даних (БД), електронної пошти, друку, спільного використання документів,а також інших служб через застосунки, що функціонують на сервері локальної мережі, з доступом для читання та запису, котрі підтримуються мережевим або ІТ-адміністратором. Більшість мереж середнього бізнесу, урядових, дослідницьких, також освітніх мереж утворені як локальні мережі на базі клієнт-серверної моделі [4].

Однорангова локальна мережа не містить центрального сервера, отже, не може справлятися з великими робочими навантаженнями, на противагу клієнт-серверній локальній мережі, тому вона переважно менша. До того ж, в одноранговій мережі LAN кожен пристрій бере участьу функціонуванні мережі в рівній мірі. Пристрої спільно використовують ресурси та дані за допомогою дротових або бездротових з'єднань із комутатором або маршрутизатором. Більшість домашніх мереж переважно однорангові.

Переваги локальної мережі тотожні, як і для будь-якої групи пристроїв, які об'єднані разом. Пристрої можуть послуговуватись єдиним підключенням до Інтернету, обмінюватися файлами один із одним, друкувати на спільних принтерах і, водночас, отримувати доступ чи навіть контролювати один одного.

Локальні мережі були розроблені в 1960-х роках для функціонування у коледжах, університетах і науково-дослідних установах, насамперед для підключення комп'ютерів до інших ЕОМ [5].

З огляду на те, що переваги пристроїв, які власне підключені до мережі, завжди були добре зрозумілі,втім лише після активного розвитку технології Wi-Fi локальні мережі стали буденним явищем майже для кожного типу середовища. У сьогоденні не лише підприємства та школи послуговуються локальними мережами, але й будинки, ресторани, кав'ярні та магазини.

Утім бездротове підключення теж значно розширило типи пристроїв, які можна під'єднати до локальної мережі. Наразі майже все різноманіття пристроїв можна «підключити», як-от від персонального комп'ютера (ПК), принтерів і телефонів до смарт-телевізорів, стереосистеми, динаміків, освітлення, термостатів, віконних відтінків, замкових дверей, камер безпеки.

У будь-якій компанії у разі роботи з великим обсягом конфіденційних даних постає першочергове завдання організації кібербезпеки, тобто формування заходів, які спрямовані на створення, забезпечення та підтримку інформаційної безпеки. Об'єкт захисту інформації є інформацією чи

інформаційним процесом, які потребують забезпечення захисту від несанкціонованого доступу, порушення цілісності та структурованості даних.

Зважаючи на інтенсивність та активний розвиток комп'ютерних технологій і систем трансляції інформації, все більш нагальною стає проблема забезпечення безпеки інформації. Власне під загрозою безпеки інформації розуміють діючи подію, котра може призвести до руйнування, спотворення чи несанкціонованого (недозволеного) використання інформаційних ресурсів.

Утім безпекою інформації називають стан, під час якого інформаційним ресурсам небезпека не загрожує.

Актуальність проблематики щодо забезпечення безпеки локальних мереж обґрунтована тим, що зміни в економічному житті нашої країни, зокрема, запровадження фінансово-кредитної системи, створення підприємств із різними формами власності, спричиняють помітний вплив у напрямку кібербезпеки. Тривалий час в Україні діяла лише державна форма власності, отже, інформація та секретні дані були також виключно державними. Втім проблеми інформаційної безпеки посилюються через проникнення до всіх напрямків діяльності технологій оброблення та трансферу даних, і передусім обчислювальних систем. До об'єктів, які потенційно можуть бути атаковані, належать різні технічні засоби, ПЗ або БД.

Зауважимо, що кожний збій мережі та комп'ютерних систем призводить до фінансових збитків. Так, значимість збоїв різної масштабності змінюється з огляду на те, яка власне мережа була атакована. В сучасному світі комп'ютерні технології інтегруються до кожної галузі, з якими взаємодіє людина. Ба більше, мережеві збої в медичних, військових або фінансових установах можуть призводити до невідновлених наслідків. Таким чином, важливість інформаційної безпеки миттєво набула статусу найважливішого питання як серед держав, так і комерційних установ.

Головні критерії інформаційної безпеки повинні забезпечувати:

– цілісність;

– конфіденційність;

– доступність інформації.

Мета захисту інформації окреслюється через отримання результатів від запобігання збитків, обумовлених витоком або несанкціонованим впливом на інформацію. Таким чином, ефективність кібербезпеки дозволяє визначити рівень відповідності результатів системи захисту даних, якою послуговувались, поставленим цілям.

Загрози щодо безпеки інформації можуть бути випадковими (ненавмисними), на кшталт загроз, джерелом яких стають помилки в ПЗ або вихід з ладу на рівні апаратного забезпечення, а також некоректні дії користувачів тощо. Водночас мета навмисних загроз полягає в нанесенні шкоди.

Отже, запровадження безпекиє доцільним для будь-яких організацій, незважаючи на їхні масштаби та форми діяльності, проте вразливими переважностають малі підприємства, що пов’язані локальними інформаційними мережами. З огляду на це, захист і контроль необхідно втілювати на всіх рівнях, зокрема, фізичному, програмному, призначеному для користувача і зовнішньому.

Ключові технічні загрози безпеки локальної мережі на малому підприємстві виникають через:

– помилки в ПЗ. Джерелами помилок у ПЗ стає робота конкретних людей з їхніми індивідуальними особливостями, кваліфікацією. Хоча більшість помилок не несе за собою небезпечні ситуації, втім деякі з них можуть призвести до серйозних наслідків, як-от отримання зловмисником прав доступу задля контролю над сервером або несанкціоноване використання ресурсів. Ці загрози можна усунути шляхом оновлення систем безпеки, котрі регулярно випускають виробники ПЗ. Отже, для коректної

роботи систем безпеки доречно застосовувати найновіші версії ПЗ від виробника (стабільні) [5];

– DoS (denial-of-service attack) та DDoS-атаки (distributed denial-ofservice attack). Атаки відмови в обслуговуванні DoS направляються, як правило, на інформаційні сервери підприємства, адже їхнє функціонування є критично важливою умовою для працездатності всього підприємства. Для реалізації таких атак зловмисники координують роботу кількох робочих станцій, зокрема, можлива і DDoS атака – розподілена атака до відмови обслуговування. Так, зловмисник перехоплює керування над групою віддалених комп'ютерів, надсилає потужний сумарний потік пакетів до комп'ютера, який було обраний для проведення атаки, спричинивши його перевантаження. Таким чином, реалізується вичерпування ресурсів операційної системи або процесора комп'ютера;

– шкідливі програми («троянський кінь», комп'ютерні віруси). Збитки, що виникають через функціонування шкідливих програм, можуть виявлятися у розкраданні, спотворенні,а також знищенні інформаціїчи приведення ПЗ у неробочий стан. Так, троянські програми видають себе за корисні застосунки, проте під час інсталяції або відкриттяфайлу заповнюють робочу станцію. Мережеві «хробаки» спроможні самостійно розповсюджуватися локальними та глобальниими мережами шляхом поширення своїх копій. Віруси проникають у різні типи файлів, однак не змінюють їхні розміри [5].

Загальні принципи забезпечення безпеки:

– мережеве обладнання, що виконує маршрутизацію трафіку до мережі Інтернет, повинно бути устатковане системою фільтрації трафіку з правилами за замовчуванням;

– локальна мережа повинна містити мінімальну кількість глобальних адрес;

– увесь трафік має бути отриманий із використанням кешування інформації за допомогою проксі-серверів;

– проксі-сервер повинен містити налаштовані Access Control List;

– на проксі-сервері повинно бути встановлено антивірусне ПЗ, яке заборонятиме доступ до потенційно небезпечних джерел;

– прямий доступ до мережі Інтернет із залученням механізму трансляції мережевих адрес (NAT) може бути активований лише для обмеженої кількості користувачів, щоб запобігти зверненню ззовні до внутрішніх хостів (користувачів мережі). ПЗ для перегляду інформації за http-протоколом повинен застосовувати максимальний рівень безпеки, а також попереджати користувача щодо всіх потенційно небезпечних дій [5];

– у мережі, що містить вихід до Інтернет, повинна бути розроблена політика автоматичного встановлення всіх доповнень і виправлень, які випускаються постачальником операційної системи. Встановлення оновлень і доповнень повинно проводитись для всіх комп'ютерів мережі, незалежно від прав користувача комп'ютера на отримання доступу до мережі Інтернет;

– усі мережеві комп'ютери повинні бути устатковані антивірусним ПЗ. Окрім того, оновлення антивірусного ПЗ повинно виконуватися щодня в певний час;

– для комп'ютерів, які використовують прямий вихід до Інтернет,доцільно зменшити до мінімуму кількість одночасних підключень;

– для всіх, без винятку, користувачів повинно бути заборонено встановлювати сторонні ПЗ.

Забезпечення безпеки інформації локальних мереж на малому підприємстві реалізується шляхом комплексу заходів, які спрямовані на запобігання несанкціонованого отримання інформаціїчи її фізичного знищення, а також модифікації. Запровадження таких заходів допоможе невеличким підприємствам успішно розвиватися, залишатися конкурентоспроможними та фінансово стабільними.

Насамперед виокремлюютьтакі види захисту інформації:

– захист інформації від витоків, тобто заходи, що спрямовані на збереження та цілісність конфіденційних даних, якими послуговуютьсяу разі внутрішнього і зовнішнього документообігу підприємства;

– захист даних від розголошень, тобто заходи, що спрямовані на запобігання необережних чи умисних дій як співробітників, так й інших осіб, які оприлюднили конфіденційну інформацію, що може призвести до подальшого передавання даних;

– захист даних від несанкціонованого доступу, тобто заходи, що спрямовані на заборону доступу до комп'ютерної мережі шляхом застосування комплексу інженерно-технічних, програмних та організаційних засобів. До того ж, необхідно розробити систему захисту даних,яка міститиме сукупність технічних, програмних, криптографічних і організаційних засобів. Вони дозволяють підтримувати безпеку мережі в будь-який момент часу від випадкового чи навмисного впливу, а також несанкціонованого використання.

Безпека даних позначає стан захищеності даних, у разі якого забезпечені цілісність, конфіденційність і доступність. Інформаційна безпека наразі є однією з головних проблем сучасного суспільства, котра обумовлена збільшенням значущості інформації в основних процесах на підприємстві.

У сьогоденні проблеми захисту інформації пов'язані з дестабілізуючим впливом зовнішніх і внутрішніх загроз,які виникають в компанії, а, отже, впливають і на її функціонування. Зі свого боку, поняття "проблема безпеки даних" взаємопов'язано з поняттям "загроза безпеці". Це призвело до того, що в діяльності підприємств усе більше виникає проблем, які чинять негативний вплив на систему керуванняі водночасна технологічну підтримку в питаннях зберігання та оброблення даних. У зв'язку з цим методи та інструменти з метою забезпечення комплексної системи захисту на підприємстві повинні здійснювати моніторинг загроз на рівні інформаційного, апаратного та програмного забезпечення. Так,розвиток комп'ютерних технологій, апаратного та програмного забезпечення значно розширило коло проблем захисту інформаційних потоків, які циркулюють у комп'ютерних мережах від несанкціонованого доступу [6].

Основна проблема полягає в необхідності забезпечення належного рівня захисту, у разі якого доцільно враховувати, що інформація, котра передана комп'ютерною мережею, може бути отримана зловмисником і передана каналами зв'язку.

У цілому проблеми інформаційної безпеки розподіляють на три головні види:

– перехоплення даних, яке виражається через порушення конфіденційності інформації;

– модифікація або зміна даних, які пов'язані зі зміною вихідного повідомлення або повної його підміни з подальшим пересиланням адресату;

– порушення авторства інформації, як-от передавання інформації не від імені автора, а від імені зловмисника.

Для того, щоб реалізувати перехоплення конфіденційної інформації, зловмисник задіює віруси, кейлогери, троянські програми, шкідливе та шпигунське ПЗ. Адже проблеми захисту мережі пов'язані з тим, що не кожна антивірусна програма спроможна своєчасно виявити чинні загрози в мережі. Таким чином, створюється сприятлива можливість для зловмисника послуговуватися мережею для досягнення поставлених цілей.

Утім можливість перехоплення інформації не завжди породжує можливість отримання доступу до захищених даних, із подальшою модифікацією. За приклад перехоплення інформації наведемо аналіз мережевого трафіку в мережі. У даному випадку зловмисник отримує інформацію про мережу підприємства, проте не може спотворювати дану інформацію.

Окрім того, проблеми безпеки даних пов'язані ще і з розвитком глобальної мережі Інтернет, яка набула популярності серед різних категорій користувачів. Так, посилення глобалізації, а разом із неюй інформатизації породжують можливості для зловмисника створювати загрози безпеці для комп'ютерної мережі з будь-якої точки світу.

До головних завдань інформаційної безпеки даних належать:

– забезпечення конфіденційності, цілісності, а також структурованості інформації;

– організація своєчасного виявлення та запобігання зовнішніх і внутрішніх загроз;

– упровадження організаційних, інженерно-технічних, апаратно-програмних методів,які дозволяють посилити захист даних;

– розроблення й удосконалення політики безпеки з урахуванням сучасних тенденцій розвитку апаратного та ПЗ.

Власне для підприємств завдання щодо забезпечення захисту даних стає одним із першочергових, оскільки виступаєяк об’єкт постійної уваги зловмисників. Насамперед інформаційна безпека спрямована на забезпечення достатнього та належного рівня кібербезпеки, адже багато в чому визначається платіжними, інформаційними й іншими процесами. Збої, що виникають у роботі інформаційної структури підприємства, можуть завдати значної шкоди в царині отримання інформації для забезпечення стабільності ключових бізнес-процесів.

Таким чином, інформаційна безпека постійно контролюється, вживаються заходи для керування ризиками, розробляються документи, котрі стають базою стандартизації керування захистом інформації. Втім, важливе значення під час забезпечення інформаційної безпеки надається формальним методам кібербезпеки, в основі яких є стандартизація.

Головна мета стандартизації – цепідвищення довіри, реалізація необхідних заходів щодо захисту інформації від загроз, які виникають, а також упровадження методів для зниження ризиків.

Задля забезпечення захисту даних перед підприємствами постають такі завдання:

– забезпечення високого рівня організації й функціонування підрозділів у галузі інформаційної безпеки підприємства;

– залучення корегування в напрямку функціонування системи захисту даних;

– розроблення планів щодо керування ризиками порушення інформаційної безпеки і забезпеченні високого рівня організації впровадження даних планів в основні бізнес-процесів підприємства;

– проведення корегування внутрішнього документообігу в напрямку захисту даних;

– ухвалення управлінських рішень щодо вдосконалення системи захисту даних, а також розроблення й організація програми навчання співробітників, заходи щодо підвищення обізнаності співробітників підприємства в питаннях захисту даних;

– постійний моніторинг із виявлення загроз та вдосконалення заходів щодо їхньої ліквідації;

– упровадження сучасних методів захисту даних, проведення внутрішнього та зовнішнього аудиту інформаційної безпеки;

– ухвалення рішень щодо вдосконалення політики безпеки підприємства, а також нагальне корегування концепції та стратегіїв питаннях інформаційної безпеки.

Політика інформаційної безпеки підприємства реалізована комплексом документів, за допомогою яких можнавідобразити вимоги щодо забезпечення захисту даних та основні напрямки підприємства щодо втілення кібербезпеки.

Під час формування політики безпеки доцільно виокремити три головних рівня: верхній, середній та нижній.

Верхній рівень політики безпеки даних організації дозволяє:

– сформулювати та продемонструвати позицію адміністрації підприємства до системи захисту інформації та відобразити ключові цілі і завдання в цьому напрямку;

– розробити індивідуальні політики безпеки, інструкції та правила, за допомогою яких регулюються окремі питання;

– інформувати співробітників організації про основні завдання і пріоритети в галузі кібербезпеки.

Політика інформаційної безпеки середнього рівня актуальна для відображення відносин і вимог підприємства до:

– використання інформаційних систем;

– телекомунікаційних та інформаційних технологій, методів і підходів до оброблення інформації;

– учасників процесів оброблення інформації, від яких залежить забезпечення захисту інформації на підприємстві.

Нижній рівень політики безпеки функціонує для опису певних процедур та документів з метою забезпечення інформаційної безпеки на виробничому підприємстві.

Етапи розроблення політики безпеки в організації складаються з:

– оцінювання особистого ставлення до загроз безпеці зі сторони власників і співробітників підприємства;

– проведення аналізу потенційно важливих інформаційних активів підприємства;

– виявлення чинних загроз безпеці підприємства з подальшою оцінкою ризиків.

Під час формування політики безпеки всіх рівнів потрібно звертати увагу на те, що політика безпеки, котра розроблена на нижньому рівні, повинна відповідати політиці безпеки, котра зазначена на верхньому рівні. Крім того, в тексті політики безпеки повинні бути наведені правила, які не містять подвійного трактування, і водночас він повинен бути достатньо зрозумілим для співробітників виробничого підприємства. Важливого значення для захисту інформації в компанії набуває політика безпеки, котра відображає логічно і семантично пов’язані, сформовані й аналізовані структури даних, якими послуговуються для захисту інформації на всіх рівнях функціонування виробничого підприємства [6].

1.2 Аналіз основних складових інформаційної безпеки мережі

Опрацюємо головні елементи політики інформаційної безпеки виробничого підприємства. В даному разі кібербезпека розглядається як застосування наведених у політиці безпеки підприємства організаційних заходів захисту інформації. За допомогою політики інформаційної безпеки на підприємствах виконують зовнішній і внутрішній аудит захисту даних, за результатами якого визначають рівень ефективності методів і засобів захисту, котрими послуговуються.

Зі свого боку, поліпшення відображається через підлаштовування заходів політики безпеки з використанням отриманих результатів проведення тестування та моніторингу. Ба більше, в процесі функціонування підприємства політика безпеки повинна повсякчас оновлюватися. Крім того, внесені зміни підлягають постійному порівнянню з тими методами та засобами, які вже застосовуються.

Так, у політиці інформаційної безпеки відображаються взаємопов’язані етапи організації інформаційної безпеки підприємства, що реалізуються через процедури, за допомогою яких можна систематизувати й ефективно розв’язувати поставлені завдання задля досягнення належного рівня захисту даних.

На першому етапі доцільно визначити межі, в яких функціонуватиме політика інформаційної безпеки підприємства, а також задати критерії для оцінки результатів.

На етапі аналізу ризиків інформаційної безпеки описуються складовій окреслюються пріоритети обраних засобів захисту з розподілом їх за ступенем важливості для підприємства. Крім того, ідентифікуються уразливості активів підприємства і визначаються збитки. Ґрунтуючись на результатах аналізу ризиків інформаційної безпеки підприємства,виконується планування роботи системи інформаційної безпеки, а також вибір найбільш ефективної стратегії і тактики. З метою підвищення ефективності політики

безпеки залучаються такі прийоми, як групове визначення об’єктів безпеки, непряме визначення з використанням правильних атрибутів і мандатне керування доступом.

Багато підприємств дотримуються глобальної та локальної політики безпеки, що ґрунтуються на принципах керування безпекою інформації. Так, глобальна політика інформаційної безпеки орієнтується на забезпечення захисту інформації на рівні бізнес-процесів компанії, водночас локальна політика спрямована на рівні захисту даних підприємства. У глобальній політиці підприємства чинні правила безпеки описують імовірну взаємодію між об'єктами, котрі потребують забезпечення захисту інформації.

Шляхом застосування глобальної політики власне забезпечення захисту інформаціїреалізують правила автентифікації об’єктів, обмін ключами, проводиться запис результатів подій безпеки до спеціального журналу разом із обліком ризиків безпеки даних. Як об’єкти для глобальної політики безпеки функціонують окремі робочі станції і підмережі, до складу яких належатьі структурні підрозділи підприємства [7].

Зауважимо, що у глобальній політиці безпеки компанії правила функціонально розподіляються на такі групи:

– правила VPN, які діють шляхом застосування протоколів IPSec. Як агент виконання даних правил є драйвер VPN, який встановлено в стеках клієнтських пристроїв або шлюзах безпеки;

– правила пакетної фільтрації дозволяють реалізовувати фільтрацію пакетів типів stateless і stateful;

– проксі-правила з активацією антивірусного захисту, що відповідають за фільтрацію трафіку, що передається через прикладні протоколи. У даному разіяк виконавчий агент буде проксі-агент;

– правила авторизованого доступу, із застосуванням правил одноразового входу, що дозволяють забезпечити роботу користувачів за паролями. Дані правила реалізуються агентами різних рівнів від

VPN-драйвера до проксі-агентів. Як агенти виконання таких правил захисту інформації будуть системи авторизації;

– правила, що відповідають за протоколювання подій, вразливостей у системі захисту інформації. У компанії політика ведення журналів подій реалізується через агента протоколювання, а власне виконавцями буде повністю вся інформаційна система.

За допомогою локальної політики безпеки підприємства проводиться налаштування засобів захисту інформації та реплікуються налаштування для вузлів із виконанням їхнього подальшого коригування. Загалом у локальній політиці безпеки підприємства зібрані правила, за допомогою яких регламентуються з'єднання, змінюються налаштування мережевих пристроїв, якими послуговуються.

Наразі на об'єктах підприємства й досі триває процес цілеспрямованого розроблення та впровадження політики інформаційної безпеки.

Застосування методів захисту інформації набувало епізодичного характеру і зводилося до інсталяції безкоштовних антивірусних програми та фізичного захисту. Така недбалість з боку інформаційно-технічного персоналу призводила не до інцидентів, а становила загрозу для діяльності організації. У зв’язку з цим було ухвалено рішення щодо необхідності розроблення комплексної політики з кібербезпеки.

Розглянемо наявний захист інформаційної безпеки з точки зору:

– програмного забезпечення;

– технічного забезпечення.

Аналіз виконання ключових завдань щодо забезпечення інформаційної безпеки містить такі задачі:

– забезпечення безпеки діяльності, захист інформації та відомостей, які вважаються комерційною таємницею;

– координування роботи щодо правового, організаційного та інженерно-технічного (фізичного, апаратного, програмного та математичного) захисту комерційної таємниці;

– запобігання необґрунтованому допуску та відкритому доступу до даних і робіт, які становлять комерційну таємницю;

– виявлення та локалізацію можливих каналів витоку конфіденційної інформації в процесі повсякденної виробничої діяльності, а також в екстремальних (аварія, пожежа тощо) дотримання режиму безпеки під час виконання таких видів діяльності, як різні зустрічі, переговори, наради, засідання та інші заходи, що пов'язані з діловою співпрацею на національному та міжнародному рівні;

– забезпечення охорони території, будівель приміщень, де зберігається захищена інформація [8].

Політика інформаційної безпеки окреслює систему поглядів на проблему забезпечення безпеки інформації і є систематизованим формуванням цілей і завдань захисту, правил, процедур, практичних прийомів, а також керівних принципів в галузі кібербезпеки, принципів побудови, організаційних, технологічних і процедурних аспектів забезпечення безпеки інформації в компанії.

Головними об’єктами системи інформаційної безпеки в компанії визначено: інформаційні ресурси, котрі необхідні для роботи. Так, інформація підприємства як ресурс набуває вагомого значення для стабільного розвитку компанії. Водночас стабільний розвиток компанії – це добробут її співробітників, тому інформацію необхідно піддавати ретельному захисту. Власне захист можливо втілювати згідно з політикою інформаційної безпеки.

Інформаційні технології, регламенти та процедури збирання, оброблення, зберігання та передавання інформації, персонал розробників і користувачів системи та її обслуговуючий персонал; інформаційна інфраструктура, що містить системи обробленнч та аналізу інформації, технічні та програмні модулі її оброблення, передавання та відображення, зокрема, канали інформаційного обміну і телекомунікації, системи та засоби захисту інформації, об’єкти та приміщення.

Основна мета політики кібербезпеки полягає у захисті суб’єктів інформаційних відносин від можливого нанесення їм матеріального, фізичного, морального чи іншого збитку шляхом випадкового або навмисного впливу на інформацію, її носії, процеси оброблення та передаванння, а також мінімізація рівня операційного і інших ризиків.

До того ж, мета інформаційної безпеки компанії окреслюється:

– захистом економічних даних компанії;

– захистом даних про розробки проєктів;

– захистом конфіденційності інформації клієнтів і співробітників;

– відповідністю вебсервісів, автоматизованих систем і внутрішніх мереж стандартам захисту інформації;

– захистом майна підприємства [8].

Для досягнення ключової мети забезпечення інформаційної безпеки доцільно розв’язати такі завдання:

– своєчасно виявляти, оцінювати та прогнозувати джерела загроз інформаційній безпеці, причини та умови, що сприяють завданню шкоди зацікавленим суб’єктам інформаційних відносин;

– створювати механізми оперативного реагування на загрози безпеки інформації та негативні тенденції;

– створювати умови для мінімізації та локалізації нанесеним неправомірним діям фізичних та юридичних осіб, послаблювати негативний вплив і ліквідовувати наслідки порушення безпеки інформації;

– захищати від втручання в процес функціонування інформаційної системи сторонніх осіб;

– розмежовувати доступкористувачів до інформаційних, апаратних, програмних та інших ресурсів, тобто захищати від несанкціонованого доступу;

– забезпечувати автентифікацію користувачів, які беруть участь у інформаційному обміні;

– захищати від несанкціонованої модифікації використовуваних програмних засобів, а також захищатм системи від запровадження несанкціонованих програм, зокрема, комп'ютерних вірусів;

– захищати інформацію обмеженого користування від витоку ПЗ технічним каналам під час її оброблення, зберігання та передавання каналамами зв'язку;

– забезпечувати криптографічним засобами захисту інформації.

Рішення наведених вище завдань можуть бути досягнуті шляхом:

– сувороговрахуванням всіх ресурсів, які підлягають захисту;

– обліку всіх дій співробітників,які виконують обслуговування та модифікацію програмних і технічних засобів корпоративної інформаційної системи;

– розмежування прав доступу до ресурсів у залежності від завдань, які постають перед співробітниками;

– чіткого знання і суворого дотриманнявсіма співробітниками вимог організаційно-розпорядчих документів з питань забезпечення безпеки інформації;

– персональної відповідальності за свої дії кожного співробітника, в межах своїх функціональних обов'язків;

– послуговування фізичними та технічними засобами захисту ресурсів системи та безперервної адміністративної підтримки їхнього використання.

Дана політика розповсюджується на всіх співробітників підприємства і вимагає повного виконання. Крім того, вона зміцнює загальну політику безпеки компанії. Весь персонал повинен бути ознайомлений і підзвітний за інформаційну безпеку щодо повноважень своїх посадових осіб [9].

Кожен начальник відділу несе відповідальність за те, щоб співробітники, котрі працюють під його керівництвом, дотримувались правил захисту інформації відповідно до стандартів організації.

Начальник підрозділу безпеки інформує низку керівників вищої ланки, надає консультативну допомогу співробітникам організації, а також забезпечує доступність звітів про стан інформаційної безпеки.

Кожен співробітник організації відповідає за інформаційну безпеку як частину виконання своїх посадових обов'язків.

Отже, визначено основні завдання щодо організації політики інформаційної безпеки в будівельній компанії та шляхи їхнього розв’язання.

1.3 Аналіз рішень кібербезпеки локальних обчислювальних мереж

Основою будь-яких систем захисту інформаційних систем визначено ідентифікацію та автентифікацію, адже всі механізми кібербезпеки спрямовані на роботу з поіменованими суб’єктами та об’єктами автоматизованих систем (АС).

Нагадаємо, що переважно суб’єктами АС можуть бути як користувачі, так і процеси, а об'єктами АС –інформація та інші інформаційні ресурси системи. Отже, присвоєння суб’єктам та об’єктам доступу особистого ідентифікатора та порівняння його з заданим переліком називають ідентифікацією.

Ідентифікація забезпечує реалізацію таких функцій:

– встановлення справжності та визначення повноважень суб’єкта під час його допуску до системи,

– контролювання встановлених повноважень у процесі сеансу роботи;

– реєстрація дій.

Автентифікацією називають перевірку належності суб’єкту доступу пред’явленого ним ідентифікатора та підтвердження його автентичності. Таким чином, автентифікація полягає в перевірці: чи насправді суб’єкт, який підключається, є тим, за кого він себе видає.

Якщо в процесі автентифікації справжність суб’єкта доведена, то система захисту інформації повинна визначити його повноваження

(сукупність прав). Це необхідно для подальшого контролю та розмежування доступу до ресурсів.

За контрольованими компонентами системи способи автентифікації можна розподілити на автентифікацію партнерів за спілкуванням і автентифікацію джерела даних. Автентифікація партнерів за спілкуванням є доречною у разі встановлення з'єднання під час сеансу. Вона служить для запобігання таких загроз, як маскарад і повтор попереднього сеансу зв'язку. Зі свого боку, автентифікація джерела даних є підтвердженням автентичності джерела окремої порції даних.

За спрямованістю автентифікація може бути як односторонньою (користувач доводить свою справжність системі, як-от при вході до системи), так і двосторонньою [9].

Найбільш актуальними простими і звичними стали методи автентифікації, що ґрунтуються на паролях – секретних ідентифікаторах суб'єктів. Так, у разі введення суб'єктом свого пароля підсистема автентифікації порівнює його з паролем, який зберігається в базі еталонних даних у зашифрованому вигляді. Якщо ж паролі співпадають, то підсистема автентифікації дозволяє доступ до ресурсів АС.

Переважній більшості АС характерні багаторазові паролі. Мова йде про те, що пароль користувача не змінюється від сеансу до сеансу протягом встановленого адміністратором системи терміну його дії. Це спрощує процедури адміністрування, проте підвищує загрозу розсекречення пароля.

Відомо безліч способів заволодіння паролем: від перегляду через плече до перехоплення сеансу зв'язку. Зауважимо, що ймовірність розкриття зловмисником пароля підвищується, якщо у паролі міститься смислове навантаження (рік народження, ім'я), невелика довжина, вводиться на одному регістрі, не має обмежень на період існування. Крім того, важливо, чи дозволено вводити пароль тільки в діалоговому режимі або є можливість звертатися з програми.

Більш надійний спосіб полягає у використанні одноразових або динамічно мінливих паролів.

Розглянемо методи парольного захисту, що засновані на одноразових паролях:

– методи модифікації схеми простих паролів;

– методи «запит-відповідь»;

– функціональні методи.

У першому випадку користувачеві видається список паролів. Під час автентифікації система запитує у користувача пароль, номер у списку якого визначено за випадковим законом. До того ж, довжина і порядковий номер початкового символу пароля можуть теж задаватися випадковим чином.

Під час використання методу «запит-відповідь» система ставить користувачеві деякі запитання загального характеру, правильні відповіді на які відомі лише конкретному користувачеві.

Утім методи автентифікації, що засновані на одноразових паролях, також не можуть гарантувати абсолютного захисту. Наприклад, якщо зловмисник має можливість підключатися до мережі і перехоплювати передані пакети, то він може надсилати останні як власні.

Наразі користуються попитом комбіновані методи ідентифікації, що вимагають, окрім знання пароля, наявність картки (token) – спеціального пристрою, котрий підтверджує справжність суб’єкта.

Картки поділяють на два типи:

– пасивні (картки з пам’яттю);

– активні (інтелектуальні картки).

Найбільш поширеними є пасивні картки з магнітною смугою, що зчитуються спеціальним пристроєм, який устаткований клавіатурою та процесором. Під час застосування цієї картки користувач вводить свій ідентифікаційний номер. У разі його збігу з електронним варіантом, який закодований у картці, користувач отримує доступ до системи. Це дозволяє достовірно встановити особу, котра отримала доступ до системи, і

виключити несанкціоноване використання картки зловмисником. Такий спосіб здебільшого йменують як двокомпонентна автентифікація.

До переваг застосування карток належить те, що оброблення автентифікаційної інформації реалізується пристроєм зчитування, без передавання до пам’яті ПК. Це виключає можливість електронного перехоплення через канали зв’язку.

Утім є і недоліки пасивних карток, зокрема, вони істотно дорожче паролів, потребують спеціальних пристроїв зчитування, а їхнє застосування обумовлено спеціальними процедурами безпечного обліку і розподілу.

Інтелектуальні картки крім пам’яті обладнані й власним мікропроцесором. Це дозволяє втілювати різні варіанти парольних методів захисту: багаторазові чи динамічно мінливі паролі, звичайні запити – відповідні методи. Всі картки реалізують двокомпонентну автентифікацію.

До наведених переваг інтелектуальних карток доречно додати їхню багатофункціональність. Так, ними можна послуговуватися не тільки з метою безпеки, але йяк-от для фінансових операцій. Однак значний недолік карток визначається їхньою високою вартістю[9].

Утім перспективним напрямком розвитку карток стає наділення їх стандартом розширення портативних систем PCMCIA (PC Card). Такі картки є портативними пристроями типу PC Card, які вставляються в роз’єм PC Card, а, отже, не потребують спеціальних пристроїв зчитування. Проте наразі вони надто дорогі.

Методи автентифікації, що ґрунтуються на вимірюванні біометричних параметрів людини, забезпечують майже повну ідентифікацію, розв’язуючи проблеми втрати паролів і особистих ідентифікаторів.

Утім цими методами не можна послуговуватися під часідентифікації процесів або даних, адже вони тільки починають розвиватися (наявні проблеми зі стандартизацією і поширенням), тому потребують поки складного і дорогого обладнання.

Як приклади впровадження зазначених методів наведемо системи ідентифікації користувача за малюнком райдужної оболонки ока, відбитками долоні, формами вух, інфрачервоним відображенням капілярних судин, за почерком, запахом, тембром голосу і навіть за ДНК.

Новим напрямком стає застосування біометричних характеристик в інтелектуальних розрахункових картках, жетонах-перепустках і елементах мобільного зв'язку. Так, під час розрахунку в магазині пред'явник картки кладе палець на сканер задля підтвердження того, що картка дійсно належить йому.

Розглянемо біометричні атрибути і відповідні системи, що набули найбільшого застосування.

Відбитки пальців. Такі сканери мають невеликий розмір, є універсальними та відносно недорогими. Біологічна повторюваність відбитка пальця становить 5 %. На сьогодні активно застосовуються правоохоронними органами через великі асигнування в електронні архіви відбитків пальців.

Геометрія руки. Відповідними пристроями послуговуються, коли через бруд або травми важко виконати сканування пальців. Біологічна повторюваність геометрії руки близько 2 %.

Райдужна оболонка ока. Такі пристрої характеризуються найвищою точністю. Теоретична ймовірність збігу двох райдужних оболонок становить 1 з 1078 [9].

Термічний образ обличчя. Дані системи дозволяють ідентифікувати людину на відстані до десятків метрів. Так, у комбінації з пошуком даних через БД такі системи застосовуються для розпізнавання авторизованих співробітників і відсіювання сторонніх. Утім у разі зміни освітленості сканерам обличчя властивий відносно високий відсоток помилок.

Голос. Перевірка голосу є зручною для використання в телекомунікаційних застосунках. Необхідні для цього 16-розрядна звукова плата і конденсаторний мікрофон коштують менше 1000 грн. Імовірність помилки становить 2–5 %. Зазначена технологія підходить для верифікації

ПЗ голосу через телефонні канали зв’язку. До того ж, вона більш надійна в порівнянні з частотним набором особистого номера. Наразі розвиваються напрямки ідентифікації особи таїї стану за голосом.

Введення з клавіатури. Так, під час введення пароля відстежуються швидкість і інтервали між натисканнями.

Підпис. Для контролю рукописного підпису застосовують дигітайзери.

Ще одним новітнім напрямком автентифікації стає доказ автентичності віддаленого користувача за його місцезнаходженням. Даний захисний механізм базується на використанні системи космічної навігації, на кшталт GPS (Global Positioning System). Користувач, який має апаратуру GPS, багаторазово посилає координати заданих супутників, що перебувають у зоні прямої видимості. Підсистема автентифікації, знаючи орбіти супутників, спроможна визначити місце розташування користувача з точністю до метра. Високий рівень надійності автентифікації визначається тим, що орбіти супутників схильні до коливань, які передбачити досить важко. До того ж, координати постійно змінюються, що зводить нанівець можливість їхнього перехоплення [9].

Апаратура GPS проста і надійна у використанні, а також порівняно недорога. Це дозволяє використовувати її у випадках, коли авторизований віддалений користувач повинен перебувати в потрібному місці [9].

Опрацювання сучасних модулів кібербезпеки локальної мережі результує про те, що пошук шляхів забезпечення захисту умов функціонування мережі наявні в достатній кількості. Проте для розроблення більш якісних, ефективних та надійних умов функціонування локальних обчислювальних мереж доцільно створити програмний модуль захисту шляхом опису принципу дії програмного модуля, підбору його програмних компонентів, складових частин та аналізу функціональних можливостей.

2 РОЗРОБЛЕННЯ КОМПОНЕНТІВ ПРОГРАМНОГО МОДУЛЯ КІБЕРБЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ВИРОБНИЧОГО ПІДПРИЄМСТВА

2.1 Принцип функціонування програмного модуля

Дослідивши сучасні технічні рішення кібербезпеки локальних обчислювальних мереж, опрацюємо принцип дії програмного модуля кібербезпеки локальних мереж, який розробляється.

З огляду на те, що різним організаціям доводиться враховувати різке збільшення кількості пристроїв, які отримують доступ до їхніх мереж, та ризики для безпеки, котрі вони несуть, важливо володіти інструментами, що забезпечують видимість мережі, контролем доступу та дотриманням пристроями політик безпеки, що є критично необхідним для безпеки їхніх мереж. Для розв’язання цієї задачі організації звертаються до таких нагальних засобів як модулі кібербезпеки та керування доступом до мережі.

З метою розв’язання задачі безпеки мережі доцільно реалізувати у модулі підтримку стандарту 802.1X, який є доречним для безпечної автентифікації користувачів, а також підтримку таких протоколів шифрування, як EAP-TLS, EAP-PEAP, PEAP-MSCHAPv2 [11].

Таким чином, ми отримаємо засіб, який надасть можливість користувачам отримувати доступ до мережі та послуговуватись її ресурсами, забезпечуючи максимальну безпеку. Водночас адміністратори матимуть можливість здійснювати контроль та керування таким доступом через зручний веб-інтерфейс.

Проведемо розроблення алгоритму процесу діяльності. На рисунку 2.1 відображено процес отримування користувачем доступу до мережі.

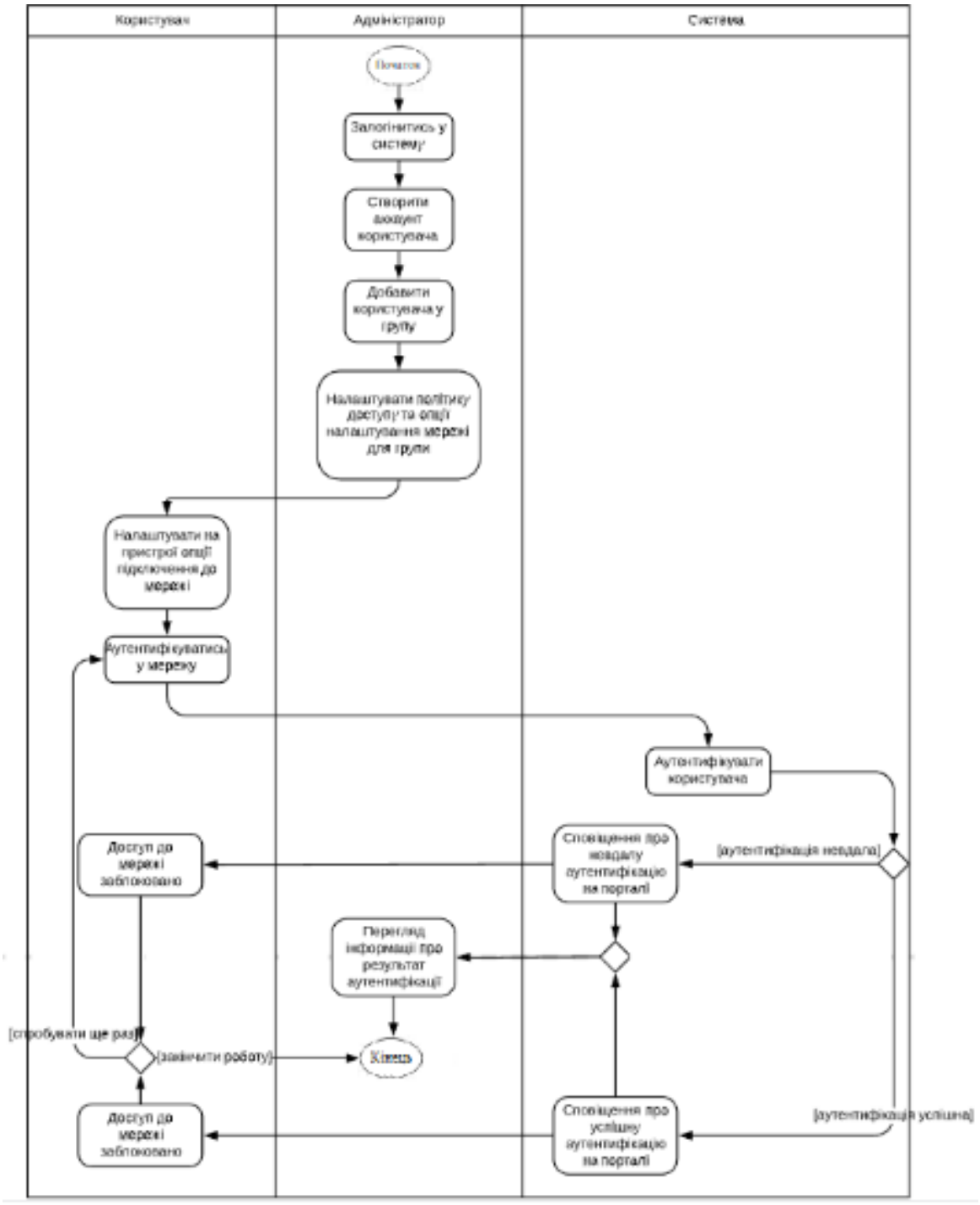

Рисунок 2.1 – Алгоритм схеми структурного процесу діяльності

Для того, щоб користувач зміг отримати доступ до мережі, адміністратору попередньо необхідно зробити певні налаштування. Спершу він повинен залогінитисьдо програмного модуля, а потім створити обліковий запис для користувача, де логін та пароль буде використовувати користувач під час автентифікації. Крім того, адміністратор повинен додати обліковий запис користувача до групи, адже доступ та мережа налаштовуються лише на

цьому рівні, зокрема, тип безпеки та тип шифрування, якими послуговуватиметься користувач під час підключення.

Далі користувач повинен налаштувати опції підключення до мережі на своєму пристрої таким чином, щоб вони співпадали з налаштуваннями, котрі зробив адміністратор. Після цього користувач може автентифіковуватись до мережі, застосувавши логін і пароль отримані адміністратором.

Якщо автентифікація пройшла успішно, користувач отримає доступ до мережі та зможе користуватись її ресурсами. Якщо ж ні, то користувачу буде відображене повідомлення, де зазначатиметься помилка.

Незважаючи на результат автентифікації користувача, на порталі для адміністратора відображатиметься відповідне сповіщення про автентифікацію та її результат. Ба більше, якщо автентифікація пройшла успішно, адміністратор зможе побачити користувача у відповідній таблиці, а також його пристрій та інформацію про нього.

На цьому робота системи для конкретного користувача добігає завершення, поки у нього не з’явиться необхідність перепідключитись до мережі. Втім для адміністратора система залишається активною і він продовжує спостереження за мережею.

2.2 Розроблення функціональної моделі програмного модуля

Мета користувача полягає в отриманні доступу до мережі, тому його дії окреслюються правильним налаштуванням опцій підключення на своєму пристрої та спробі автентифікацвї до мережі. До того ж, для автентифікації до мережі йому може знадобитись попереднє встановлення агента.

Відобразимо функціональну модель системи за допомогою структурної схеми варіантів застосування, що наведено на рисунку 2.2.

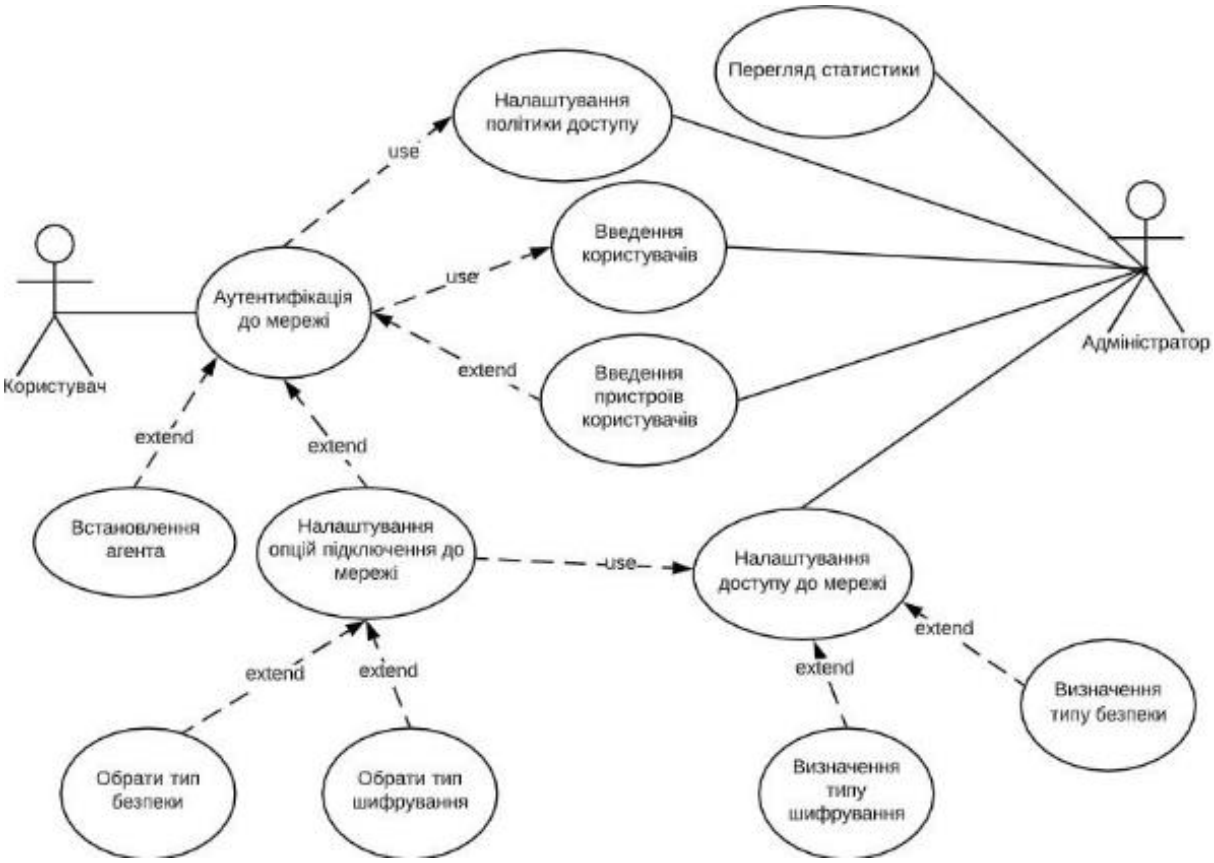

Рисунок 2.2 – Структурна схема варіантів застосування

Розглянемо, які функції може виконувати адміністратор у системі контролю та керування доступу до мережі:

– визначати налаштування мережі для групи користувачів;

– визначати політику доступу для груп користувачів;

– вводити користувачів;

– вводити пристрої користувачів;

– переглядати статистику та моніторити мережу.

Для того, аби забезпечити користувача та адміністратора вище наведеними властивостями, система повинна виконувати такі функції:

– здійснювати підтримку стандарту 802.1X;

– здійснювати підтримку протоколів шифрування на кшталт EAP-TLS, EAP-PEAP, PEAP-MSCHAPv2.

Коли користувач підключатиметься до мережі, то повинен буде ввести логін і пароль. Ці дані можна розглядати як вхідні дані для системи. Крім

того, разом із цими даними на бекенд системи, поза поля зору для користувача, надходитиме різна додаткова інформація, зокрема:

– MAC-адреса пристрою;

– публічна IP-адреса, від якої надходить запит;

– метод автентифікації (PAP/ MSCHAPV2/ TLS/ CHAP);

– тип тунелю (PEAP/TTLS);

– NtChallenge (RADIUSchallenge, що надсилається клієнту задля аутентифікації запиту);

– NtClientResponse (відповідь пристрою на RADIUS challenge).

Вихідні дані системи це те, що отримуємо після спроби користувача отримати доступ до мережі. До того ж, автентифікація користувача може бути як успішною, так і невдалою.

Після успішної автентифікації користувач отримає доступ до мережі, а також можливість послуговуватись її ресурсами, а адміністратор, зі свого боку, – сповіщення про успішну авторизацію користувача та можливість спостерігати за його пристроєм у таблиці облікових записів та пристроїв (рис. 2.3 – 2.4).

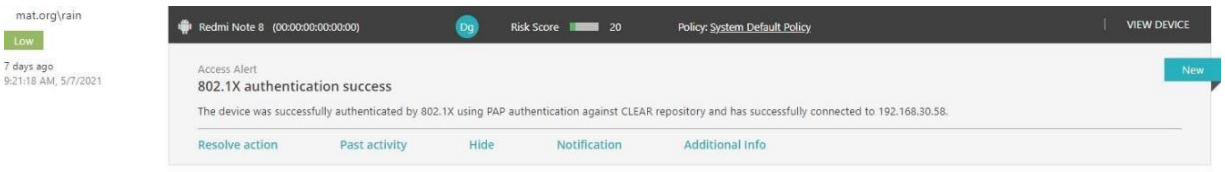

Рисунок 2.3 – Приклад сповіщення для адміністратора про успішну автентифікацію

Рисунок 2.4 – Таблиця облікових записів та пристроїв

У разі невдалої автентифікації користувачу надійде сповіщення із відповідною помилкою, а адміністратору – сповіщення про невдалу спробу доступу (рис. 2.5 – 2.6).

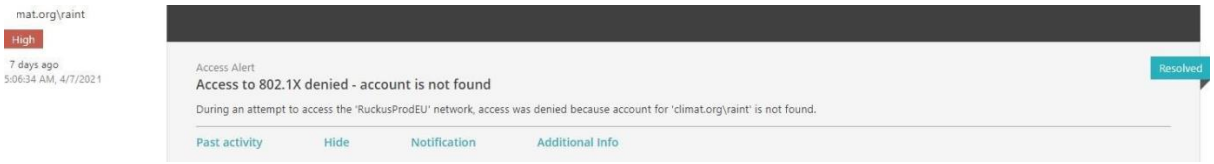

Рисунок 2.5 – Приклад сповіщення для адміністратора
про невдалу автентифікацію

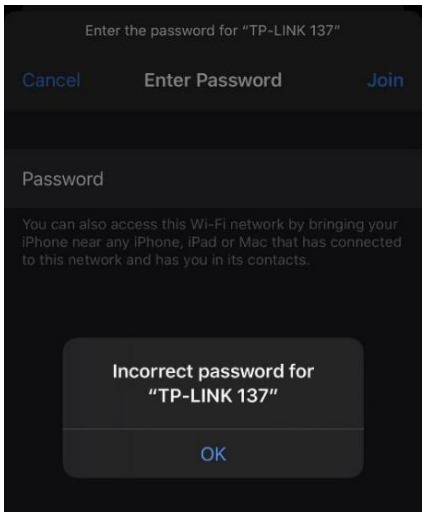

Рисунок 2.6 – Приклад помилки отримання доступу для користувача

2.3 Вибір програмних модулів для програмування

Для створення програмного модуля застосовуємо БД CosmosDB, яка надежить до БД хмарного сервісу Azure. Це є базою даних NoSQL, отже, дані у ній зберігаються так: один запис подається як документ JSON, а документи, зі свого боку,розташовані в колекціях [12].

У програмному модулі розміщено 3 основні колекції – це accounts, devices та orgs. Ці колекції призначені для зберігання різних документів, які стосуються облікових записів користувачів, їхніх пристроїв, а також організацій.

Наочний приклад області роботи з БД продемонстровано на рисунку 2.7.

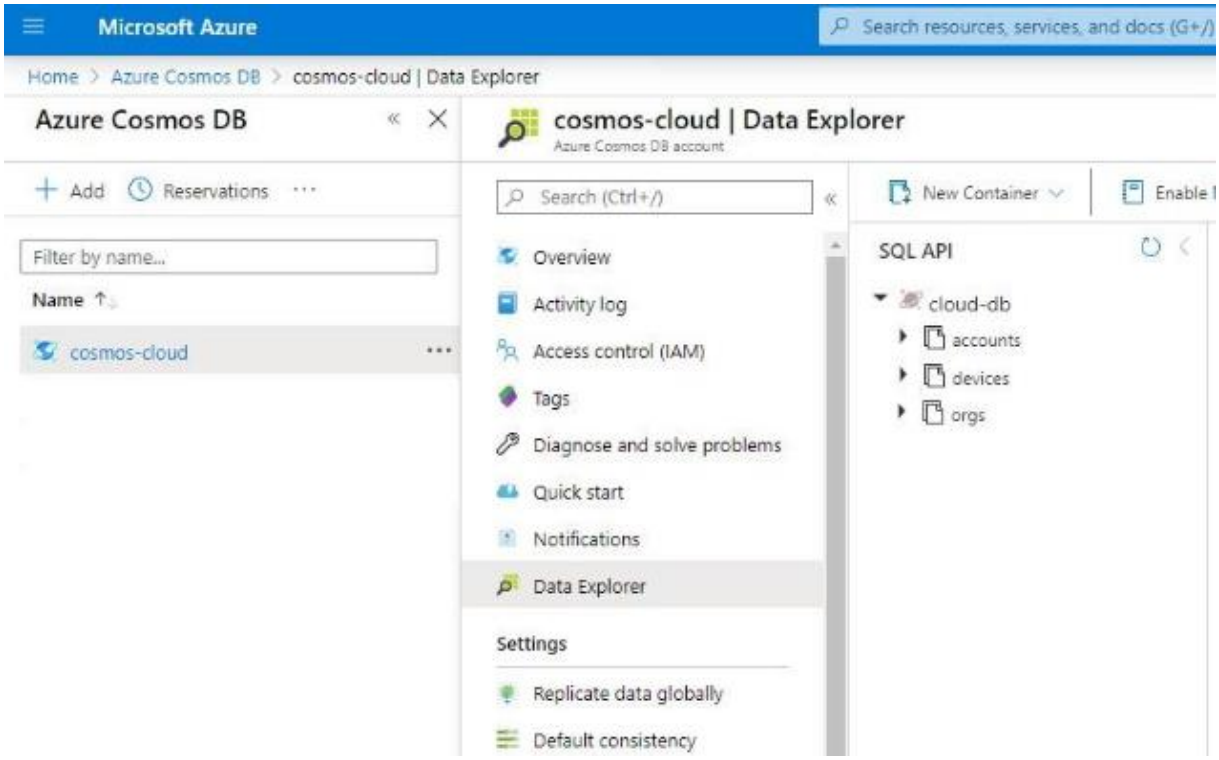

Рисунок 2.7 – Компоненти бази даних

Визначаємо, що головною сутністю, що зв’язує всі інші, буде організація.

Вона може налічувати багато груп користувачів, кожна з яких містить облікові записи користувачів та ідентифікатор політики, що буде до неї застосовуватись.

Для того, щоб показати сутності, котрі будуть зберігатись у документах БД, та зв’язки між ними, створено ER-діаграму, приклад якої продемонстровано на рисунку 2.8.

Зауважимо, що до облікового запису користувача може бути прив’язано багато пристроїв, а до пристроїв, зі свого боку, – багато даних, які надходитимуть від пристрою з деякою періодичністю.

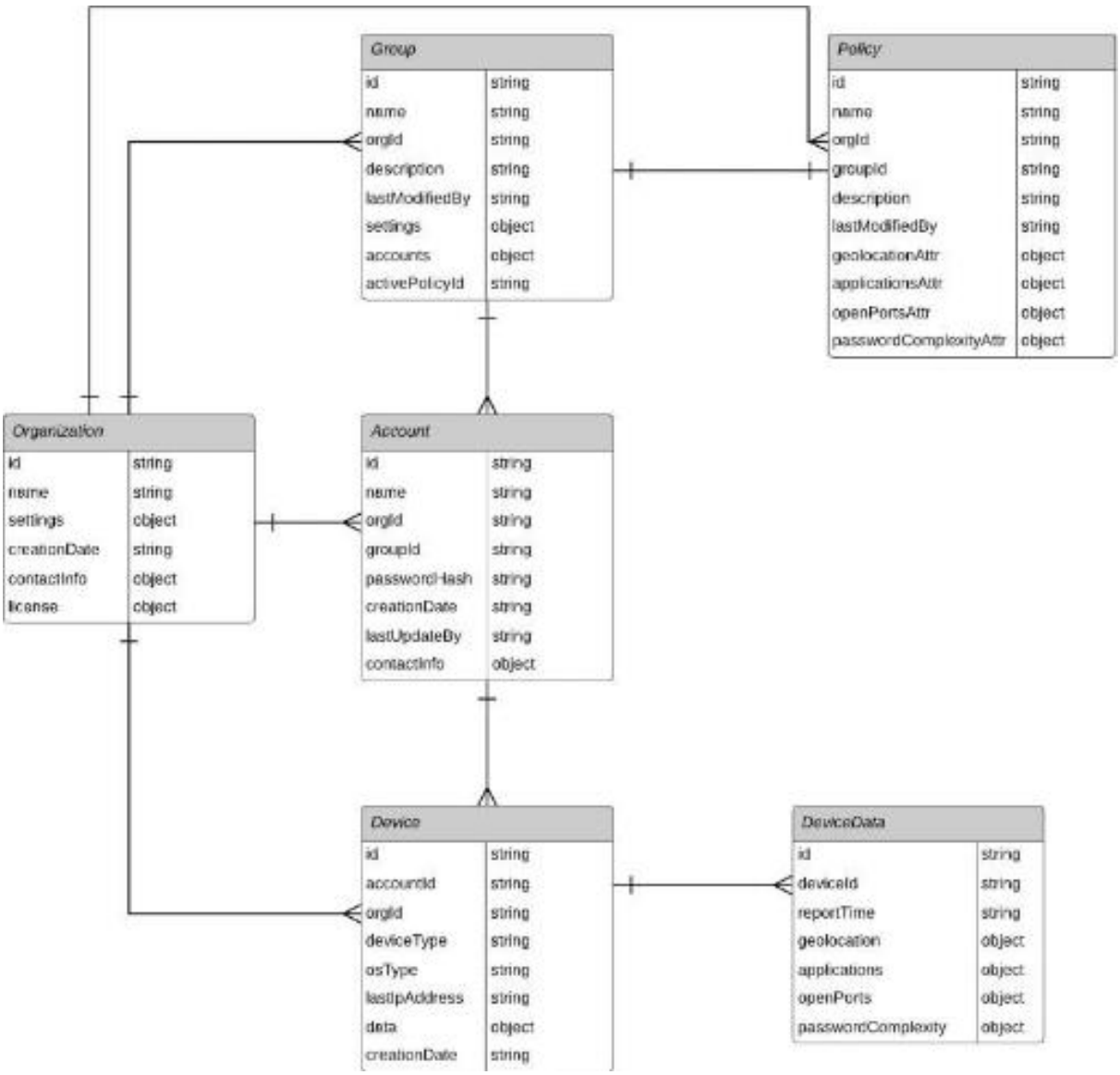

Рисунок 2.8 – ER-діаграма бази даних

Для розміщення програмного модуля обрано хмарну платформу Microsoft Azure [13]. Власне рішення застосовувати хостинг у хмарі було зумовлене тим, що це сприяє низці вагомих переваг: система стає повністю масштабованою, не прив’язаною до конкретного регіону і не вимагає жодного обладнання. Крім того, це свідчить про те, що поточна версія завжди буде найновішою, з останніми особливостями та можливостями. Одна з головних причин застосування саме хмарної платформи Microsoft Azure полягає в її сумісності з .net фремфорком, тобто однією з найвагоміших переваг Azure, і яка надає Microsoft значну перевагу над AWS (Amazon Web Services) та рештою конкурентів.

З метою створення серверної частини основних компонентів програмного модуля було обрано мову програмування C#. Вона набула визнання однієї з найкращих мов для створення великих застосунків. Це чітко типізована, об’єктно-орієнтована мова програмування, що надає можливість створювати застосунки, котрі будуть запущені на .Net фреймворку, тобто невід’ємному компоненті Windows, який складається з віртуальної системи виконання Common Language Runtime (CLR) й уніфікованого набору бібліотек класів.

Для створення клієнтської частини було обрано JavaScript бібліотеку React.

React – це JavaScript бібліотека з відкритим кодом, яка є актуальною для створення інтерфейсів користувача спеціально для односторінкових програм (SPA). React надає можливість розробникам створювати масштабні веб-застосунки, котрі можуть змінювати дані без перезавантаження сторінок [14]. Такі SPA характеризуються високою продуктивністю, оскільки застосовують віртуальний dom (Document Object Model) та механізми оновлення подано на базі різниць.

Для створення сервера автентифікації було використано продукт FreeRADIUS. FreeRADIUS є найпопулярнішим RADIUS-сервероміз відкритим кодом та найпоширенішим RADIUS-сервером у світі. Він підтримує всі поширені протоколи автентифікації. Так, FreeRADIUS-сервер – це високопродуктивний пакет для unix і unix-подібних операційних систем, який дозволяє налаштувати сервер radius протоколу, котрим можна послуговуватися для автентифікації та обліку різних типів доступу до мережі.

Для створення агента було застосовано технологію WPF, яка є частиною екосистеми .net і водночас підсистемою для створення графічних інтерфейсів.

2.4 Вибір методу кібербезпеки локальної обчислювальної мережі

З метою розв’язання задачі безпечної автентифікації у системі доцільно застосувати стандарт 802.1X. Мережа, котра базується на 802.1X стандарті, відрізняється від пересічних домашніх мереж одним важливим аспектом: у ній присутній сервер автентифікації, тобто RADIUS-сервер. Він перевіряє облікові дані користувачів,аби визначити, чи є вони членами організації, і, відповідно до політики доступу, надає користувачам різний рівень доступу до мережі. Це сприяє можливості користувачам послуговуватись унікальними обліковими даними (ім’ям і паролем) або сертифікатами для доступу до мережі, не покладаючись до того ж на єдиний мережевий пароль, який може бути легко викрадений.

Для реалізації автентифікації 802.1X застосовує інкапсуляцію Extensible Authentication Protocol (EAP) над IEEE 802, який відомий як «EAP over LAN» або EAPOL. EAP. Мова йде про фреймворк для автентифікації або, як його ще йменують, фреймворк для інкапсулювання даних автентифікації. Він визначений у RFC 3748 та задіюється під час підключень до локальних мереж або до Інтернету. Підкреслимо, що власне EAP не є протоколом, а це фреймворк, який визначає формат повідомлень, що надсилаються, і підтримує різні методи автентифікації.

Так, у 802.1X автентифікації беруть участь 3 сторони:

– заявник (supplicant);

– автентифікатор (authenticator);

– сервер автентифікації (authentication server) (рис. 2.9).

Заявником іменують пристрій користувача, що під’єднується до LAN або WLAN. Автентифікатором визначено мережевий пристрій, який реалізує з’єднання між користувачем і мережею, а також може дозволяти чи блокувати трафік між ними, на кшталт Ethernet-комутатора чи бездротової точки доступу. Сервером автентифікації, здебільшого, є довірений сервер,

який підтримує протоколи RADIUS і EAP. Зрідка ПЗ сервера автентифікації може функціонувати на апаратному модулі автентифікатора.

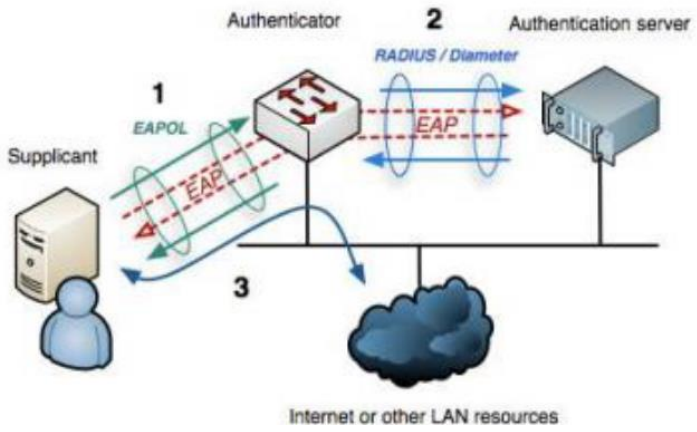

Рисунок 2.9 – Компоненти 802.1X [11]

Типовий процес 802.1X автентифікації складається з:

– ініціалізації (Initialization) – у разі виявлення нового заявника порт на маршрутизаторі (автентифікаторі) є включеним і набуває статусу «unauthorized». У цьому стані дозволений лише 802.1X трафік. Увесь інший трафік, зокрема, Internet Protocol (разом із цим TCP і UDP) нівелюється;

– ініціації (Initiation) – щоб ініціювати автентифікацію, автентифікатор періодично надсилає «EAP-Request / Identity»-пакети на спеціальну адресу (01:80:C2:00:00:03 (Ethernet multicast address)) у локальному мережевому сегменті Layer 2. Заявник слухає цю адресу і під час отримання «EAP-Request / Identity»-пакета надсилає автентифікатору пакет «EAP-Response / Identity», в якому міститься ідентифікатор заявника, на кшталт User ID. Після чого автентифіктор інкапсулює цю відповідь до «RADIUS AccessRequest» пакета інадсилає його на сервер автентифікації. До того ж, заявник може ініціювати або перезапустити автентифікацію, надіславши «EAPOL-Start»-пакет автентифікатору, котрий тоді відповість «EAP-Request / Identity»-пакетом;

– перемовин (Negotiation) – сервер автентифікації надсилає відповідь (інкапсульовану до RADIUS Access-Challenge пакета) автентифікатору, що містить «EAP Request», в якому зазначається конкретний «EAP Method» (Тип

EAP-based автентифікації, котру він бажає, щоб заявник виконав). Автентифікатор інкапсулює «EAP Request» до EAPOL-пакета і надсилає його заявнику. В цій точці заявник може почати застосовувати EAP-метод, згаданий вище, або зробити NAK («Negative Acknowledgement») і відповісти з EAP-методами, котрі він хоче виконати;

– автентифікації (Authentication) – якщо сервер автентифікації і заявник погоджуються з EAP-методом (EAP Method), тоді «EAP Requests» і «EAP Responses» надсилатимуться між заявником і сервером автентифікації доки сервер автентифікації не відповість «EAP-Success»-пакетом (інкапсульованим до «RADIUS AccessAccept»-пакета) чи «EAP-Failure»-пакетом (інкапсульованим до «RADIUS Access-Reject»-пакета). Якщо ж автентифікацію пройдено успішно, то автентифікатор встановить статус порту «authorized» і трафік буде дозволений. У протилежному разіл порт залишиться у стані «unauthorized». Коли заявник вилогіниться з мережі, він надішле «EAPOL-logoff»-пакет автентифікатору, а той, зі свого боку,переведе порт у статус «unauthorized», блокуючи знову весь неEAP traffic.

802.1X налічує безліч переваг серед яких пріоритетними є:

– 802.1X дозволяє застосовувати сертифікати й облікові дані користувачів для автентифікації в мережі. Це сприяє кращий безпеці, ніж використання спільного паролю для мережі (PSK), а також легшу підтримку великих мереж, адже PSK не масштабуються;

– видимість 802.1X забезпечуєякісну видимість у мережі, оскільки процес автентифікації задіює спосіб зв’язати ім'я користувача з IP-адресою, MAC-адресою, комутатором і портом. Ця видимість є доречною для аудиту безпеки, статистики використання мережі, а також усунення несправностей;

– безпека 802.1X – це найбезпечніший спосіб автентифікації. Він функціонує на рівні 2 (Data link layer) у мережі, що дозволяє контролювати мережевий доступ на межі доступу. Крім того, 802.1X інкапсулює EAP, що сприяє можливості залучати різні EAP-методи автентифікації, зокрема, EAP-

TLS, EAP-PEAP, PEAP-MSCHAPv2 тощо, які гарантують дуже високий рівень безпеки шляхом автентифікації як клієнта, так і сервера автентифікації, використання шифрованих тунелей для передавання даних автентифікації;

– підтримка – майже всі пристрої на ринку, що можуть під’єднуватись до бездротової мережі, підтримують 802.1X;

– послуги на базі ідентичності – 802.1X дозволяє послуговуватись автентифікованою ідентичністю для динамічного надання мережевих послуг.

3 РОЗРОБЛЕННЯ ПРОГРАМНОГО МОДУЛЯ КІБЕРБЕЗПЕКИ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ВИРОБНИЧОГО ПІДПРИЄМСТВА

3.1 Опис компонентів програмного модуля

Даний програмний модуль складається з чотирьох компонент: веб-застосунку, що містить інтерфейс для роботи з системою та складається із серверної та клієнтської частин, серверної частини модуля, сервера автентифікації і застосунку робочої області агента. Перші два компоненти розгортаються як Azure Cloud Services, де серверна частина веб-застосування розгортається як Web role, а бекенд системи – Worker role.

Архітектура програмного забезпечення є типовою для клієнт-серверних застосунків іналічує три рівні: рівень відображення, рівень бізнес-логіки і рівень доступу до даних. Утім для серверних частин нашої системи достатньо лише двох шарів: бізнес-логіки та доступу до даних. Дана архітектура продемонстрована на рисунку 3.1.

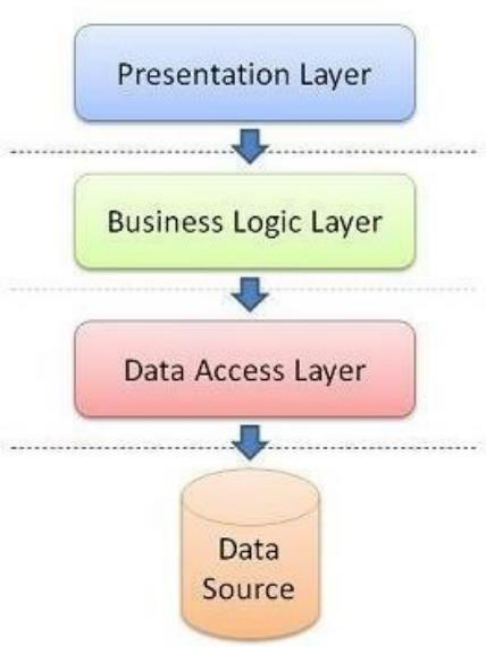

Рисунок 3.1 – Архітектура структури компонентів

На рівні відображення перебуває ASP.NET Web Application, який забезпечує інтерфейс для користувача [14].

Веб-застосунок створено за допомогою HTML (мова гіпертекстової розмітки документів), куди вбудовуються React компоненти, TypeScript (мова програмування, що транспілюється у JavaScript і реалізується у браузері клієнта) та CSS (каскадні таблиці стилів) для оформлення вебсторінок.

Рівень логіки складається із C# проєктів, у яких функціонує безліч C# класів та функцій, які забезпечують логіку системи [14].

Архітектура застосунку агента заснована на архітектурному патерні MVVM (Model-View-ViewModel). Цей патерн дозволяє розмежувати логіку застосунку із візуальною частиною (відображення) і нативно підтримується WPF.

Окрім того, підкреслимо, що у коді задіяно багато сторонніх бібліотек, які надходять у вигляді Nuget-пакетів (менеджер пакетів, який надходить як розширення Visual Studio). Серед них можна виокремити:

– Microsoft.ApplicationInsights (бібліотека для роботи з сервісом Azure ApplicationInsights, який придатний для зберігання логів системи);

– Microsoft.Azure.DocumentDB (бібліотека для роботи з сервером базою даних CosmosDB, яка розміщена Azure);

– Newtonsoft.Json (бібліотека для серіалізації та десеріалізації);

– Selenium.WebDriver (фреймворк для тестування вебзастосунків);

– Unity (IoC) контейнер – фреймворк для автоматичного впровадження залежностей.

Веб-застосунок утворено з 6 вебсторінок: Organizations (організації), Alerts (сповіщення), Devices and accounts (пристрої та аккаунти), Groups (групи), Policies (захист), Settings (налаштування).

На сторінці Organizations (Організації) адміністратор зможе бачити перелік існуючих організацій, отже,зможе переходитидо будь-якої з них.

Коли він відкриє якусь організацію, то опиниться на вкладці Alerts (сповіщення), де будуть розміщені всі сповіщення, що стосуються мережі.

На сторінці Devices and accounts (Пристрої та облікові записи) відображатиметься таблиця з наявними пристроями та обліковими записами. До того ж, у таблиці активовано кнопку, натиснувши на яку можна створити новий обліковий запис.

На сторінці Groups (групи) адміністратор може переглядати список чинних груп, моніторити користувачів у цих групах, а також змінювати налаштування цих груп: встановювати опції підключення до мережі та активний захист.

На сторінці Policies (захист) можна переглядати список чинних захисних елементів, редагувати їх та створювати нові.

На сторінці Settings (налаштування) можна переглядати налаштування як організації, так і її адміністраторів.

Розроблена система налічує безліч класів, однак головними визначено: Organization, Group, Policy, Device, DeviceData та Account. Їхній вміст зв’язку відтворено на структурній схемі класів, яку наведено на рисунку 3.2.

Розглянемо зв’язки між класами. Клас Organization уособлює організацію, тому вважається ключовим класом, оскільки зв’язує всі інші. Одна організація може налічувати багато груп, облікових записів користувачів, політик, а також безліч пристроїв. Одна група можемістити лише одну активну політику, проте багато користувачів. Один користувач може володіти багатьма пристроями, водночас кожен пристрій може містити багато даних.

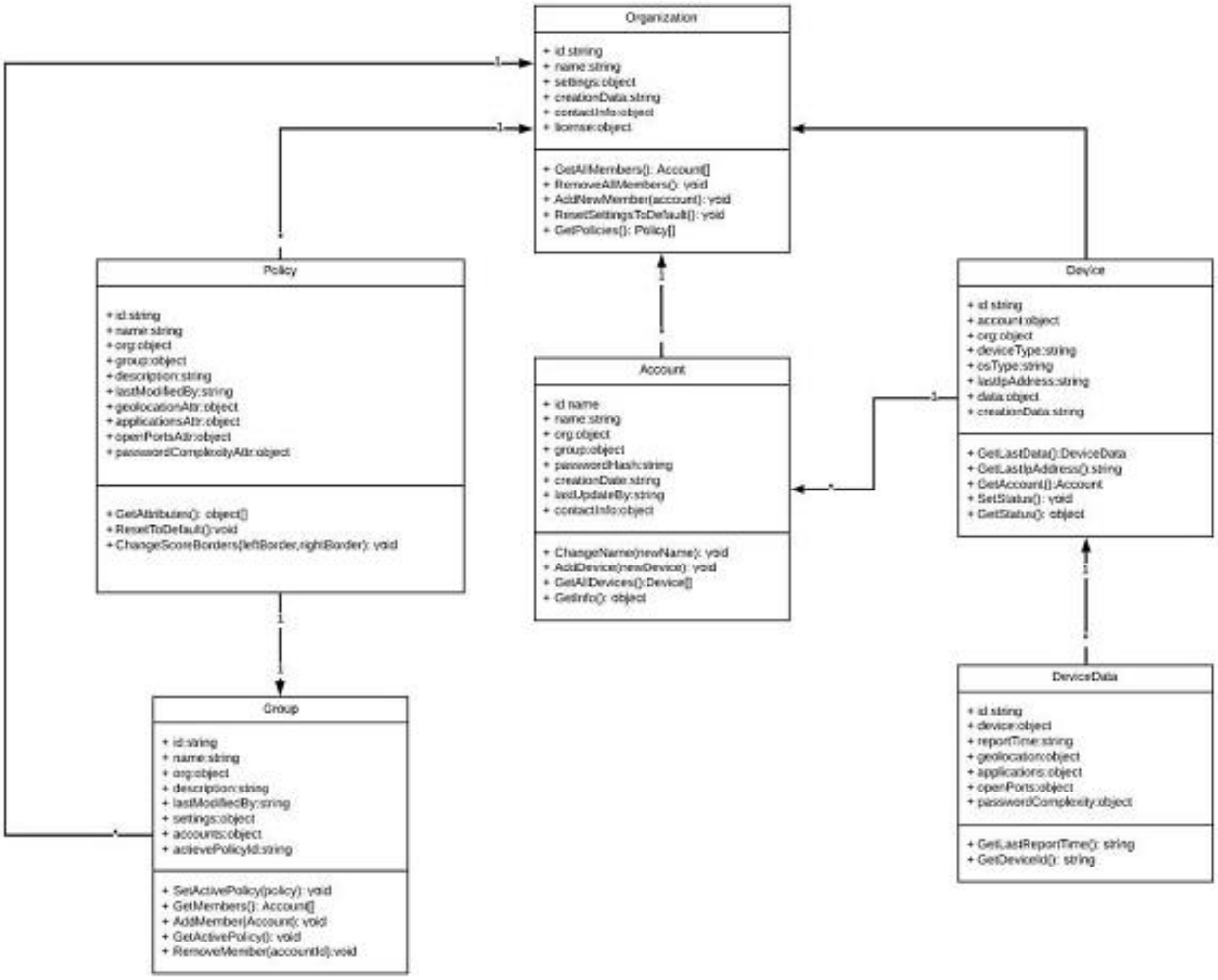

Рисунок 3.2 – Структурна схема класів програмного забезпечення

Вивчимо структурну схему послідовності, котру наведено на рисунку 3.3.

Для того, щоб користувач зміг отримати доступ до мережі, спершу адміністратор повинен виконати деякі попередні налаштування. Для цього йому необхідно створити обліковий запис для користувача, логіном та паролем якого користувач послуговуватиметься під час автентифікації. Ба більше, адміністратор повинен налаштувати політики доступу та мережі, зокрема, тип безпеки та тип шифрування, котрі будуть задіяні користувачем під час підключення. Потім користувач виконує автентифікацію, що проводиться через сервер автентифікації. Після цього користувач отримує результат автентифікації, відповідно до якого він отримає чи не отримає доступ до мережі.

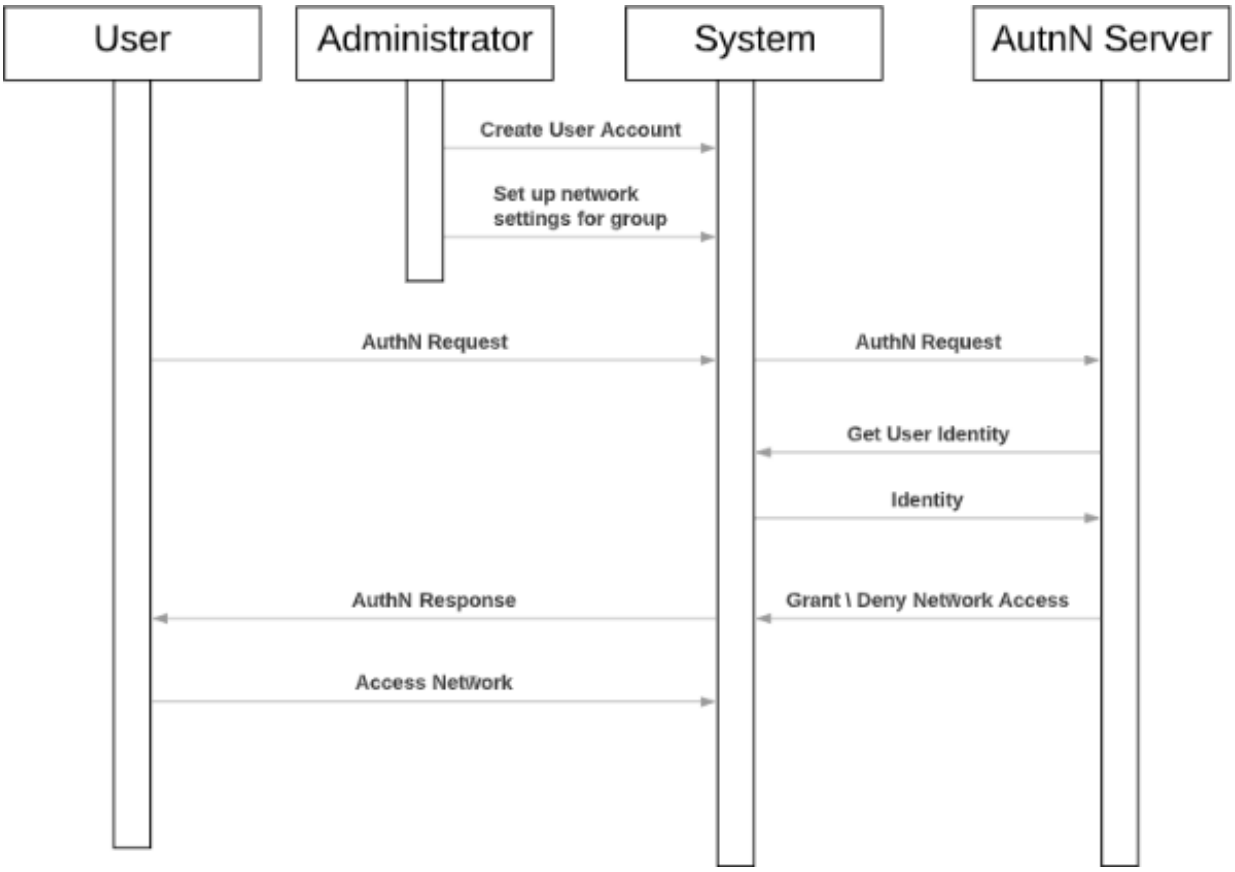

Рисунок 3.3 – Структурна схема послідовності

Розроблений програмний код програмного модуля продемонстровано у Додатку А.

3.2 Розроблення інтерфейсу користувача

Проведемо розроблення інтерфейсу користувач, у межах системи на користувача покладаються такі функції: встановлення агента, налаштування опцій підключення й автентифікація до мережі.

Для того, щоб користувач міг реалізувати автентифікацію, адміністратору необхідно створити для нього обліковий запис, як це продемонстровано на рисунках 3.4 – 3.5.

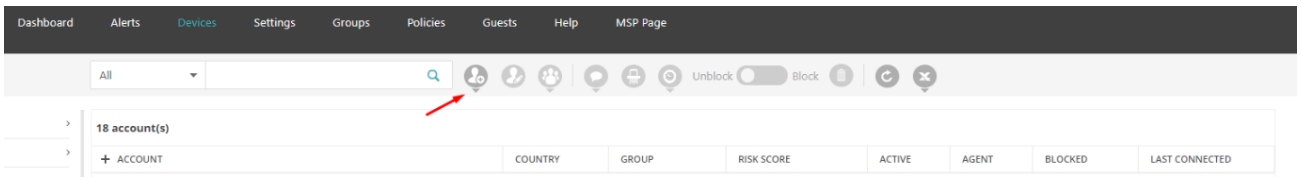

Рисунок 3.4 – Кнопка створення нового користувача

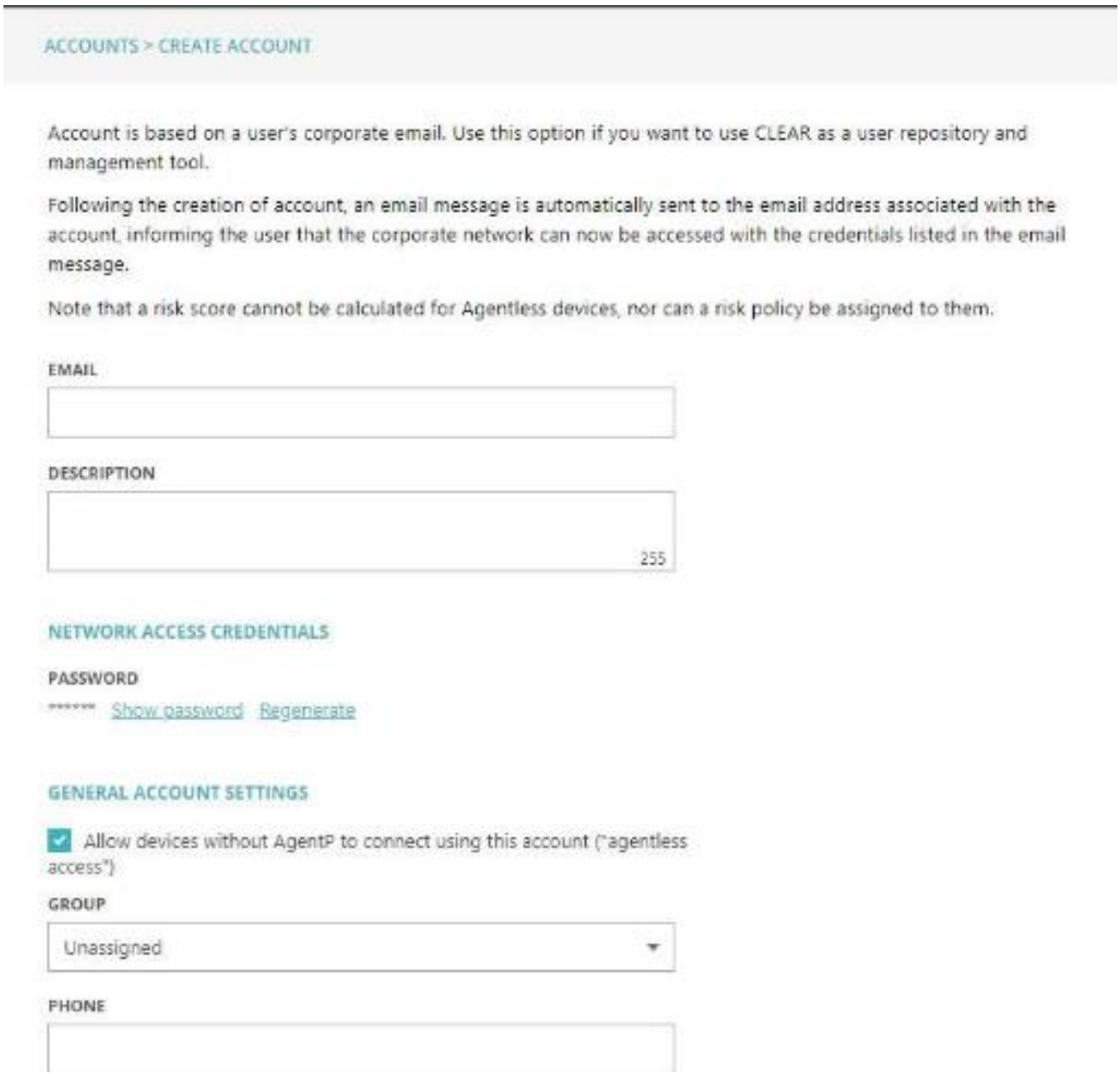

Рисунок 3.5 – Форма створення нового користувача

На наступному етапі адміністратору необхідно оприлюднити для групи відповідну політику, а також налаштувати мережу. Наочний приклад наведено на рисунку 3.6.

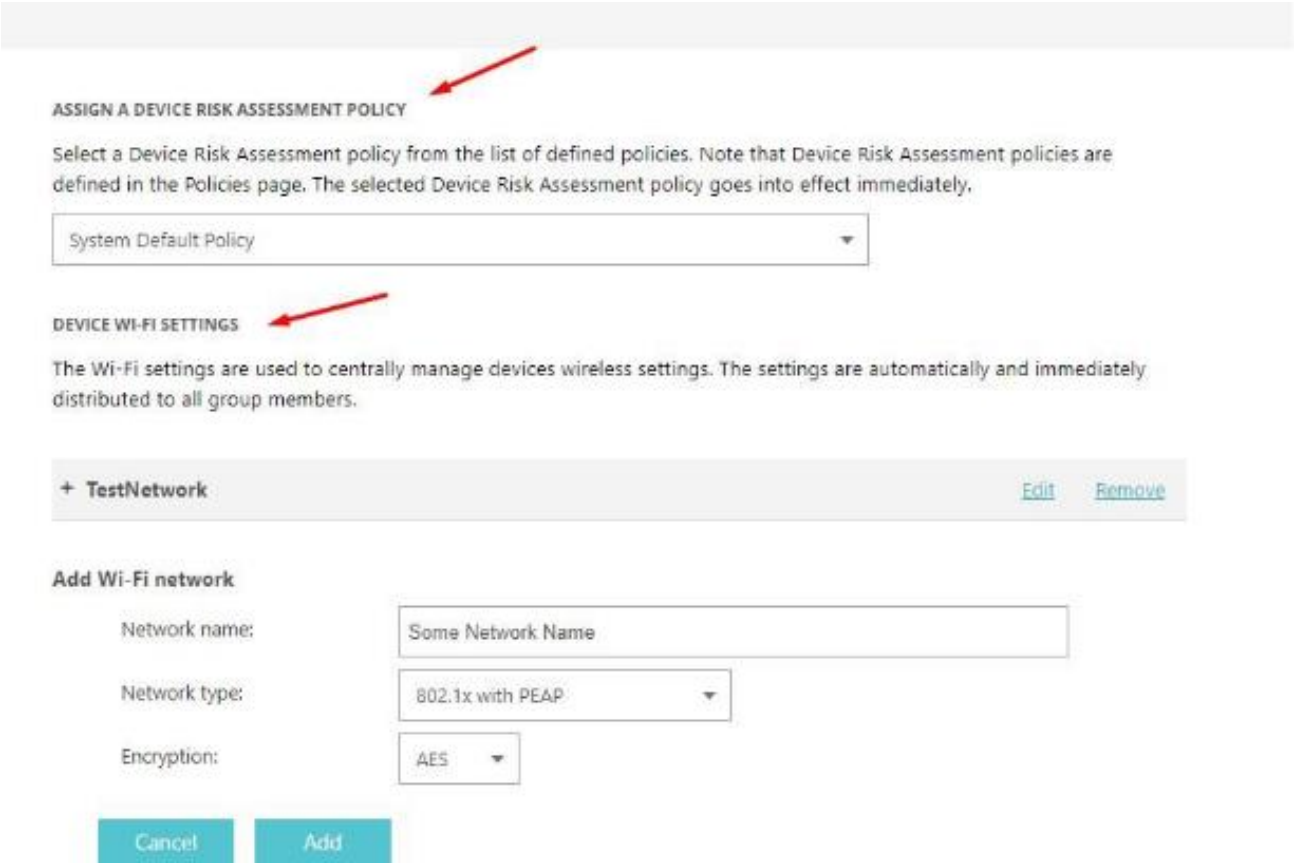

Рисунок 3.6 – Налаштування мережі та політики для групи

З урахуванням установленої політики адміністратором, користувачу може знадобитись агент з метою автентифікації до мережі. Для цього користувач повинен перейти за посиланням і завантажити відповідний .exe файл, щоб інсталювати агента (рисунок 3.7).

Рисунок 3.7 – Сторінка з інсталюванням агента

Потім необхідно проінсталювати агента за допомогою облікових даних, які були надані адміністратором. Приклад інсталяції агента продемонстровано на рисунку 3.8.

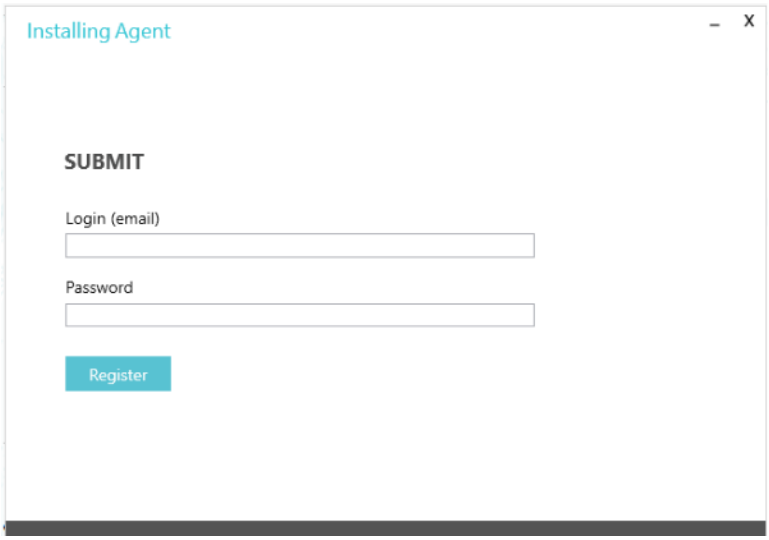

Рисунок 3.8 – Інсталяція агента

Тепер агент спроможний запускатися як бекграунд сервіс і може збирати дані про користувача. Зі свого боку, користувачу необхідно налаштувати опції підключення до мережі на своєму пристрої, як це продемонстровано на рисунках 3.9 – 3.10.

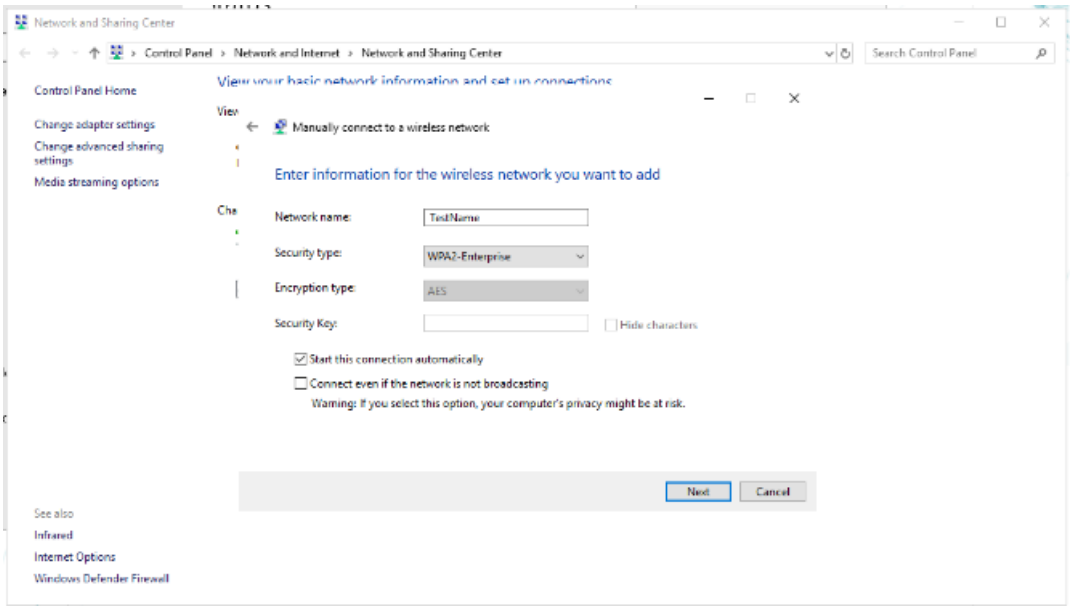

Рисунок 3.9 – Налаштування опцій підключення до мережі

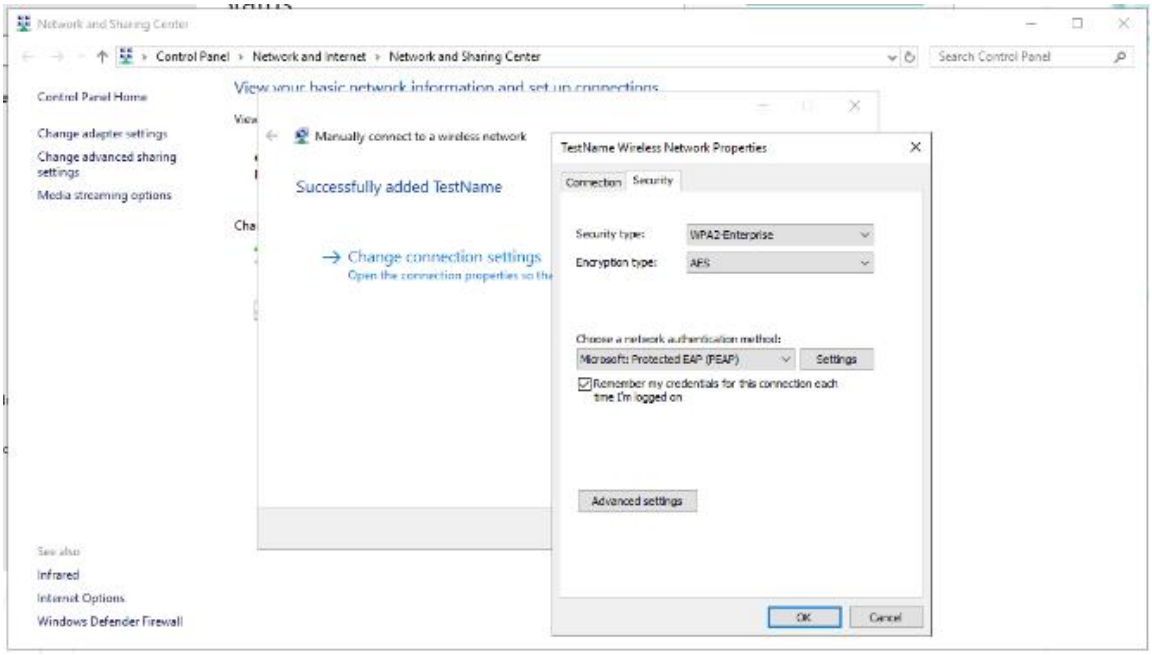

Рисунок 3.10 – Налаштування опцій підключення до мережі

Після того, як користувач це виконав, йому слід вибрати зі списку доступу мережу, яка йому необхідна, та зробити спробу автентифікації. Так, після успішної автентифікації користувач отримає доступ до мережі разом із можливістю послуговуватись її ресурсами. Водночас адміністратору надійде сповіщення про успішну авторизацію користувача, отже, він зможе спостерігати за пристроєм користувача у таблиці облікових записів та пристроїв. Приклади наведені на рисунках 3.11 – 3.12.

Рисунок 3.11 – Сповіщення для адміністратора
про успішну автентифікацію

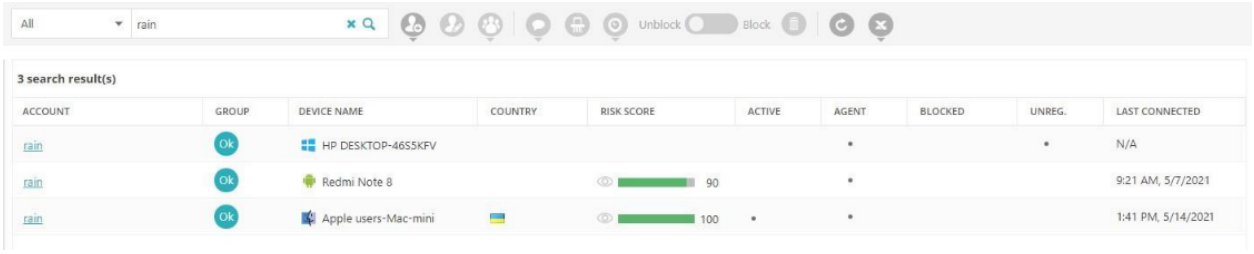

Рисунок 3.12 – Таблиця облікових записів та пристроїв

У разі невдалої автентифікації користувач отримає сповіщення із відповідною помилкою, а адміністратор – сповіщення про невдалу спробу доступу, як це продемонстровано на рисунках 3.13 – 3.14.

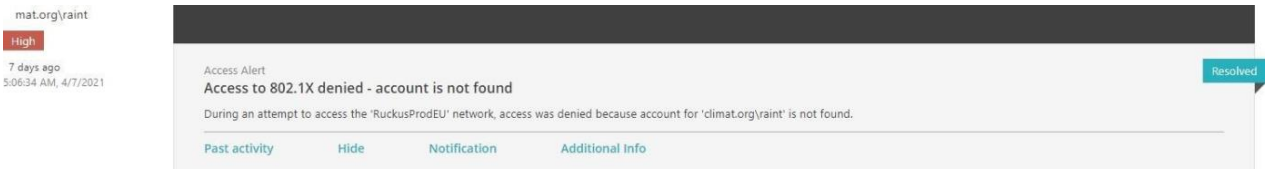

Рисунок 3.13 – Оповіщення для адміністратора
про невдалу автентифікацію

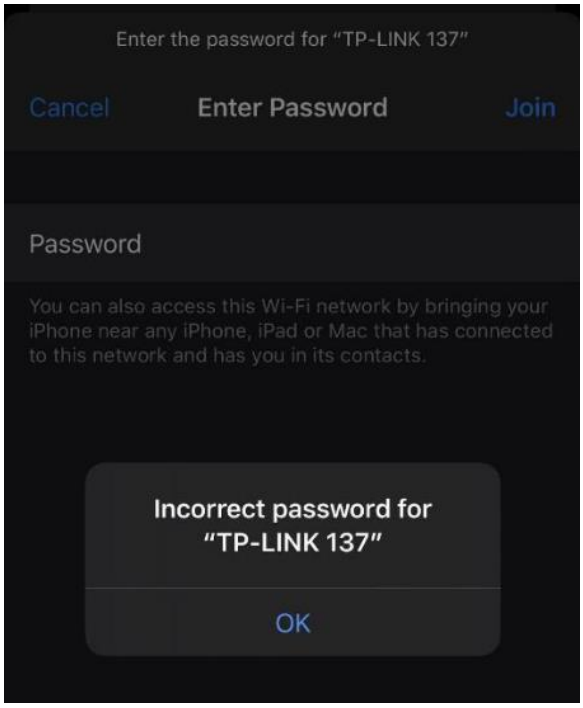

Рисунок 3.14 – Приклад помилки отримання доступу для користувача

3.3 Проведення випробовування програмного модуля

Мета випробувань програмного модуля полягає у виявленні слабких місць у системі та впровадженні рішень щодо їхнього усунення. Для цього ми скористаємось Unit-тестуванням та E2E-тестуванням.

Unit-тестування позначає процес у програмуванні, що дозволяє перевірятм на коректність окремі модулі вихідного коду програми.

E2E-тестування є інтеграційними тестами, що взаємодіють з інтерфейсом на кшталт дій користувача. Цих двох видів тестів буде цілком достатньо, щоб перевірити коректність роботи системи.

Для досягнення даної мети доречно розглянути функції, що реалізує програмний модуль, а також описати очікуваний результат роботи функцій.

Для кожного тесту необхідно задіяти функцію та оцінити достовірність отриманих результатів.

У процесі тестування було перевірено часткову роботу системи.

У таблиці 3.1 наведено тест створення нового облікового запису користувача в програмному модулі.

Таблиця 3.1 – Створення нового облікового запису користувача

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка функції «Створення нового облікового запису користувача»
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Вхідні дані	Створена організація
4.	Схема проведення	Натиснути кнопку «Sign in», перейти на сторінку з пристроями та користувачами, натистнути кнопку «Create new account», заповнити форму і натиснути кнопку «Create»
5.	Очікуваний результат	Створений обліковий запис відображається у таблиці з пристроями та користувачами. Користувач зафіксований у базі даних
6.	Стан модуля після випробувань	Створений обліковий запис відображається у таблиці з пристроями та користувачами. Користувач зафіксований у базі даних

У таблиці 3.2 наведено тест створення нового типу захисту в програмному модулі.

Таблиця 3.2 – Створення нової політики

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка функції «Створення нової політики»
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Схема проведення	Натиснути кнопку «Sign in», перейти на сторінку із захистом, натистнути кнопку «Create new policy», заповнити дані і натиснути кнопку «Create»
4.	Очікуваний результат	Створений вид захисту відображається у таблиці із захистом. Захист існує у базі даних
5.	Стан системи випробувань	Створений вид захисту відображається у таблиці із захистом. Захист існує у базі даних

У таблиці 3.3 наведено тест перевірки коректного відображення сповіщення в програмному модулі.

Таблиця 3.3 – Перевірка коректного відображення сповіщення

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка коректного відображення сповіщення
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Схема проведення	Натиснути кнопку «Sign in» і зайти до організації
4.	Очікуваний результат	На вкладці зі сповіщеннямичинне сповіщення про створення організації
5.	Стан системи після випробувань	На вкладці зі сповіщеннями чинне сповіщення про створення організації

У таблиці 3.4 наведено тест перевірки успішної автентифікації в програмному модулі.

Таблиця 3.4 – Перевірка успішної автентифікації

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка успішної автентифікації
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Вхідні дані	Створена організація, обліковий запис користувача та правильно налаштована група
4.	Схема проведення	Виклик функції автентифікації з обліковими даними користувача та параметрами
5.	Очікуваний результат	Пристрій користувача відображається у таблиці користувачів та пристроїв. Пристрій існує у БД
6.	Стан системи випробувань	На вкладці із сповіщенням присутнє сповіщення про успішну автентифікацію

У таблиці 3.5 наведено тест блокування автентифікації в ПЗ.

Таблиця 3.5 – Перевірка блокування автентифікації за допомогою кібербезпеки

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка блокування автентифікації за допомогою політики
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Вхідні дані	Створена організація, політика та обліковий запис користувача з параметрами, які порушують кібербезпеку
4.	Схема проведення	Виклик функції автентифікації з обліковими даними користувача
5.	Очікуваний результат	Пристрій користувача не відображається у таблиці користувачів та пристроїв. Пристрій не існує у БД
6.	Стан системи після випробувань	На вкладці із сповіщенням наявне сповіщення про невдалу автентифікацію через порушення політики

У таблиці 3.6 наведено тест перегляду інформації про пристрої та облікові дані користувачів.

Таблиця 3.6 – Перегляд інформації про пристрої та облікові дані користувачів

№	Назва параметра тестування	Виконана дія
1.	Мета тесту	Перевірка можливості перегляду інформації про пристрої та облікові дані користувачів
2.	Початковий стан	Відкрита сторінка входу до веб-застосунку
3.	Вхідні дані	Створена організація та велика кількість облікових записів користувачів та їхніх пристроїв
4.	Схема проведення	Натиснути кнопку «Sign in», перейти на сторінку з пристроями та користувачами
5.	Очікуваний результат	У таблиці повинні відображатись коректні дані про створені облікові записи та їхні пристрої
6.	Стан системи випробувань	У таблиці повинні відображатись коректні дані про створені облікові записи та їхні пристрої

Отже, сформовано керівництво користувача та наведено екранні форми розробленого вебзастосунку інтерфейсу модуля та агента. Було встановлено мету проведення випробувань і визначено тести, котрі необхідно провести над деякими із функцій.

У процесі тестування було перевірено часткову функціональність модуля, наведено перелік випробувань деяких головних функціональних можливостей.

Під час тестування програмного модуля було встановлено, що функціонал програмного модуля відповідає встановленим вимогам. Підкреслимо, що всі функції, про які було заявлено, розроблені в межах модуля.

4 ОХОРОНА ПРАЦІ

4.1 Аналіз умов праці на робочому

На робочому місці оператора ПК згідно виникають небезпечні та шкідливі фактори: підвищений рівень шуму, несприятливі мікрокліматичні умови, недостатній рівень освітленості, шкідливі речовини, підвищений рівень електромагнітних випромінювань радіочастот, висока напруга електричної мережі, статична електрика та інші. Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. При систематичному впливі виробничих факторів, які не відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працюючих та можуть виникнути професійні захворювання органів зору, руху, нервової системи. Таким чином, вивчення умов праці на робочому місці оператора ПК є необхідною умовою запобігання негативних наслідків впливу небезпечних та шкідливих факторів.

Організація робочого місця. Приміщення, в якому знаходиться робоче місце оператора ПК, загальною площею 48 м^2, і висотою стелі 3,5 м. У приміщенні знаходиться 6 робочих місць з ПК. Кожне робоче місце обладнане робочім столом, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші.

4.2 Промислова безпека на робочому

Живлення ПК здійснюється від трифазної чьотирьох електричної мережі змінного струму з глухо-заземленою нейтраллю і напругою 220 В, частотою 50 Гц. Згідно НПАОП 40.1-1.21-98 приміщення можна віднести до

категорії без підвищеної небезпеки, так як в приміщенні відсутні чинники, які викликають підвищену або особливу небезпеку.

Для створення безпечних умов праці необхідно провести ряд організаційних і технічних заходів. Згідно НПАОП 40.1-1.32-01 для запобігання ураження людини електричним струмом в приміщенні застосовується система занулення.

4.3 Виробнича санітарія у приміщенні

Робота оператора ПК за енерговитратами відноситься до категорії легких робіт. В таблиці 4.1 наведені оптимальні параметри мікроклімату в приміщеннях, де виконуються роботи операторського типу [15].

Таблиця 4.1 – Параметри мікроклімату для приміщень з ПК

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	22 – 24 °С; 40 – 60 %; до 0,1 м/с
Теплий	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	23 – 25 °С; 40 – 60 %; 0,1 – 0,2 м/с

Виміряні за допомогою приладів температура та вологість у лабораторії відповідають вказаним у таблиці для теплого періоду року. Слід зазначити, що для нормалізації параметрів мікроклімату слід використовувати у приміщеннях кондиціювання повітря, або забезпечити подачу свіжого повітря системами вентиляції.

Лабораторія, де виконується розробка конструкції модуля, має наступні характеристики:

– площа приміщення 48 м^2 (8×6 м);

– висота – 3,5 м;

– кількість робочих місць – 6 шт.;

– обладнання – стіл з ПК і периферією – 6 шт.

Приміщення, відповідно до ДНАОП 0.00-1.31-99, має забезпечувати 6 м^2 площі та 20 м^3 обсягу на одне окреме робоче місце з ПК [15]. Площа приміщення 48 м^2 та об'єм 168 м^3, на кожне робоче місце приходится 8 м^2 площі і об'єм 28 м^3, тобто вимога виконана.

Приміщення з ПК повинні мати природне і штучне освітлення відповідно до ДБН В.25-28-2006 «Природне і штучне освітлення». Природне світло повинно проникати через бічні світлові прорізи, зорієнтовані, як правило, на північ або північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5 %.

Рівень загального штучного освітлення приміщення можна перевірити за допомогою методу питомої потужності, викладеної в [15].

Розрахункова формула методу:

$$W = \frac{W_{\sum}}{S}, \tag{4.1}$$

де W – питома потужність, Вт/м^2;

S – площа приміщення, м^2;

$W_{\sum}$ – загальна потужність освітлювальної установки Вт, яка розраховується за формулою:

$$W_{\sum} = W_{св} \cdot n_{св}, \tag{4.2}$$

де $W_{св}$ – потужність одного світильника, Вт;

$n_{св}$ – кількість світильників в приміщенні.

$$W_{\sum} = 100 \cdot 4 = 400 \text{ Вт}, \quad (4.3)$$

$$W = \frac{400}{48} = 8{,}33 \text{ Вт/м}^2. \quad (4.4)$$

Питомої потужності 8,33 Вт/м^2 по таблиці Б.3 із [15] відповідає освітленість в 250 лк при мінімальній допустимої освітленості 300 лк.

Отже, для створення сприятливих зорових умов в лабораторії необхідно збільшити кількість світильників або замінити лампи в світильниках на більш потужні.

4.4 Пожежна безпека виробничого приміщення

Пожежна безпека – стан об'єкта, при якім виключається можливість пожежі, а у випадку його виникнення запобігає вплив на людей небезпечних факторів пожежі й забезпечується захист матеріальних цінностей.

Пожежна безпека забезпечується системою запобігання пожежі й системою пожежного захисту. У всіх службових приміщеннях обов'язково повинен бути «План евакуації людей при пожежі», що регламентує дії персоналу у випадку виникнення вогнища загоряння, що й указує місця розташування пожежної техніки.

Горючими компонентами у виробничому приміщенні є: перегородки, двері, підлоги, ізоляція кабелів тощо.

Протипожежний захист – це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження його поширення, а також на створення умов для успішного гасіння пожежі.

Джерелами запалювання у виробничому приміщені можуть бути електронні схеми від ПК, прилади, застосовувані для технічного обслуговування, пристрою електроживлення, кондиціювання повітря, де в

результаті різних порушень утворюються перегріті елементи, електричні іскри й дуги, здатні викликати загоряння горючих матеріалів.

У сучасних ПК дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості друг від друга розташовуються сполучні проведення, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відводу надлишкової теплоти від ПК служать системи вентиляції й кондиціювання повітря. При постійній дії ці системи являють собою додаткову пожежну небезпеку.

Енергопостачання виробничого приміщення здійснюється за допомогою трансформаторної станції та за допомогою двигун-генераторних агрегатів. На трансформаторних підстанціях особливу небезпеку представляють трансформатори які мають масляне охолодження. У зв'язку із цим перевагу слід віддавати сухим трансформаторам.

ВИСНОВКИ

У даній кваліфікаційній роботі було проведено розроблення програмного модуля кібербезпеки локальної обчислювальної мережі виробничого підприємства. Під час виконання роботи було реалізовано такі завдання:

– проаналізовано особливості захисту інформації локальної обчислювальної мережі, де було визначено актуальність даної теми та опрацьовано сучасні програмні модулі кібербезпеки, їхні переваги та недоліки;

– розроблено принципи функціонування програмного модуля, котрий реалізує та використовує стандарти, що забезпечують якісний рівень мережевої кібербезпеки;

– розроблено функціональну модель програмного модуля, в якому чітко визначили функції користувача;

– опрацьовано вхідні дані, наведено опис стандартів і протоколів, які будуть використовуватись для розв’язання задачі. Встановлено їхні переваги та недоліки;

– розглянуто засоби розроблення програмного забезпечення та обґрунтовано вибір застосованих технологій;

– окреслено загальні вимоги до програмного забезпечення, описано бібліотеки, що будуть задіяні під час розроблення програмного модуля;

– описано архітектуру програмного забезпечення. Спроєктовано діаграми класів і послідовності, а також наведено їх опис;

– у процесі тестування було перевірено часткову функціональність модуля, наведено перелік випробувань деяких головних функціональних можливостей.

– доведено, що функціонал розробленої системи відповідає встановленим вимогам. Окрім того, всі функції розроблено в межах модуля;

– прораховано штучне освітлення в дослідницькій лабораторії, де виконувалась кваліфікаційна робота.

Застосовуючи розроблений програмний модуль кібербезпеки і керування доступу до інформаційної мережі, кожна організація спроможна захистити власну корпоративну мережу і втілити це максимально просто та ефективно.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ 3008:2015 Інформація та документація «Звіти у сфері науки і техніки». Структура та правила офомрлювання. / В. Земцева; Ю. Поліщук, канд. фіз.-мат. наук; Р. Санченко, канд. техн. наук; Л. Шрамко; А. Ямчук (науковий керівник) ДП «УкрНДНЦ» від 22 червня 2015р. № 61 з 2017- 07-01.

2. Методичні вказівки з підготовки кваліфікаційної роботи для здобувачів першого (бакалаврського) рівня вищої освіти денної і заочної форми навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» / Упоряд.: І. Ш. Невлюдов, О. І. Филипенко, О. В. Токарєва, С. П. Новоселов, О. В Сичова. – Харків: ХНУРЕ, 2023. – 64 с.

3. Методичні вказівки з підготовки кваліфікаційної роботи бакалавра для студентів усіх форм навчання спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» освітньої програми «Автоматизація та комп'ютерно-інтегровані технології» / Упоряд.: І. Ш. Невлюдов, А. О. Андрусевич, О. В. Токарєва, С. П. Новоселов, О. В Сичова. – Харків: ХНУРЕ, 2022. – 55 с.

4. Технічні засоби автоматизації: Підручник / І. Ш. Невлюдов, А. О. Андрусевич, О. І. Филипенко, Н. П. Демська, С. П. Новоселов. – Кривий Ріг : Криворізький коледж НАУ, 2019. – 366 с.

5. Система захисту інформації в локальних обчислювальних мережах [Електронний ресурс] – Режим доступу: https://www.docsity.com/ua/sistema-zahistu-informaciji-v-lokalnih-obchislyuvalnih-merezhah/5129431/ - 09.04.2025р. – Загол. з екрану.

6. Захист інформації в локальних мережах [Електронний ресурс] – Режим доступу:http://elartu.tntu.edu.ua/bitstream/123456789/9429/2/Conf_

2011v1_Pletiuk_I-Zakhyst_informatsii_v_lokalnykh_75.pdf/ – 10.04.2025р. – Загол. з екрану.

8. Завдання та принципи інженерно-технічного захисту інформації. – Режим доступу: https://infopedia.su/19x8b28.html – 12.04.2025р. – Загол. з екрану.

9. Електронний підпис [Електронний ресурс]. – Режим доступу: https://maanimo.ua/helpful/elektronnij-tsifrovij-pidpis/ 13.04.2025р. – Загол. з екрану.

10. GPS із захистом LAN [Електронний ресурс]. – Режим доступу: http://um.co.ua/8/8-2/8-241198.html 13.04.2025 р. – Загол. з екрану.

11. CosmosDB [Електронний ресурс]. – Режим доступу: https://cosmos.azure.com/ 14.04.2025р. – Загол. з екрану.

12. Microsoft Azure [Електронний ресурс]. – Режим доступу: https://capweb.ua/microsoft-azure-bastion.html/ 15.04.2025. – Загол. з екрану.

13. React JS [Електронний ресурс]. – Режим доступу: https://uk.reactjs.org/ 16.04.2025р. – Загол. з екрану.

14. ASP.NET Web Application [Електронний ресурс]. – Режим доступу: https://dotnet.microsoft.com/apps/aspnet/web-apps 18.04.2025р. – Загол. з екрану.

15. Комплекс навчально-методичного забезпечення навчальної дисципліни «Організація керування умовами праці» підготовки освітнього рівня бакалавр усіх спеціальностей та усіх напрямів університету [Електронний ресурс] / ХНУРЕ; розроб.: Т. Є. Стиценко, Г. В. Пронюк, Н. М. Сердюк. – Харків, 2017. – 108 с.