Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Герасимова Максима Олеговича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Адаптивна автентифікація в системах ідентифікації та контролю доступу розподілених інформаційно-телекомунікаційних систем малого бізнесу*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ас. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Герасимову Максиму Олеговичу* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Адаптивна автентифікація в системах ідентифікації та контролю доступу розподілених інформаційно-телекомунікаційних систем малого бізнесу***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 № 1036-с

Розділ	Зміст	Термін виконання
Розділ 1	*Актуальність питання. Класифікація систем управління ідентифікацією та доступом. Аналіз та порівняння існуючих СУІД. Постановка задачі.*	10.11.2021
Розділ 2	*Вимоги до СУІД. Розробка модулю адаптивної автентифікації. Обґрунтування вибору технологій СУІД. Програма випробувань СУІД. Розробка програмної реалізації елементів СУІД.*	22.12.2021
Розділ 3	*Визначення витрат на створення КЗЗ. Розрахунок експлуатаційних витрат. Оцінка величини збитку у разі реалізації загроз. Загальний ефект від впровадження КЗЗ. Визначення та аналіз показників економічної ефективності.*	12.02.2022

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі:

Дата подання до екзаменаційної комісії:

Прийнято до виконання _____ Герасимов М.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___с., ___рис., ___табл., ___додатка, ___джерел.

Об’єкт дослідження: системи управління ідентифікацією та доступом.

Предмет дослідження: процес адаптивної автентифікації в системах управління ідентифікацією та доступом.

Мета роботи: підвищення ефективності роботи систем управління ідентифікацією та доступом для інформаційно-телекомунікаційних систем малого бізнесу.

Перший розділ кваліфікаційної роботи описує актуальність питання, системи управління ідентифікацією та доступом; аналізує існуючі системи та виконує їх порівняння.

У спеціальній частині наведено основні вимоги до систем управління ідентифікацією та доступом, та послуги безпеки до них. На їх основі виконано розробку модулю адаптивної автентифікації та обґрунтування вибору технологій системи. Розроблено основні пункти програми випробувань послуг безпеки відповідно до нормативних документів із ТЗІ. Наведено фрагменти коду програмної реалізації елементів СУІД.

В економічному розділі було розраховано витрати на створення комплексу засобів захисту та щорічні експлуатаційні витрати на його підтримку. Також було доведено економічну доцільність створення комплексу.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки під час обробки інформації в інформаційно-телекомунікаційних системах малого бізнесу.

КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, ПОСЛУГИ БЕЗПЕКИ, ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ, КЕРУВАННЯ ДОСТУПОМ

РЕФЕРАТ

Пояснительная записка: ___стр., ___рис., ___табл., ___приложений, ___источников.

Объект исследования: системы управления идентификацией и доступом.

Предмет исследования: процесс адаптивной аутентификации в системах управления идентификацией и доступом.

Цель работы: повышение эффективности работы систем управления идентификацией и доступом для информационно-телекоммуникационных систем малого бизнеса.

Первый раздел квалификационной работы описывает актуальность вопроса, системы управления идентификацией и доступом; анализирует существующие системы и выполняет их сравнение.

В специальной части приведены основные требования к системам управления идентификацией и доступом, и услуги безопасности к ним. На их основе выполнено разработку модуля адаптивной аутентификации и обоснование выбора технологий системы. Разработано основные пункты испытаний услуг безопасности в соответствии с нормативными документами ТЗИ. Представлено фрагменты кода программной реализации элементов СУИД.

В экономическом разделе было рассчитано затраты на создание комплекса средств защиты и ежегодные эксплуатационные затраты на его поддержку. Также было доказано экономическую целесообразность создания комплекса.

Практическое значение проекта состоит в повышении уровня информационной безопасности во время обработки информации в информационно-телекоммуникационных системах малого бизнеса.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ, УСЛУГИ БЕЗОПАСНОСТИ, ИДЕНТИФИКАЦИЯ, АУТЕНТИФИКАЦИЯ, УПРАВЛЕНИЕ ДОСТУПОМ

ABSTRACT

Explanatory note: ___p., ___fig., ___tab., ___additions, ___sources.

Object of study: identity and access management systems.

Subject of study: adaptive authentication process in identity and access management systems.

Project objective: improving the efficiency of identity and access management systems for information and telecommunication systems for small business.

The first section of the qualification work describes the relevance of the issue, identity and access management systems; analyzes the existing systems and performs their comparison

The special section contains the basic requirements for identification and access control systems, and security services to them. On their basis, the development of adaptive authentication module and justification of the choice of system technology is made. Developed the main points of testing security services in accordance with the regulatory documents. Presented code fragments of the software implementation of elements of the IAM system.

In the economic section, the costs of creation of trusted computer base and annual operating costs of its were calculated. The economic feasibility of creating of trusted computer base was proved.

The practical significance of the project is to increase the level of information security in automated systems.

TRUSTED COMPUTER BASE, SECURITY SERVICES, IDENTIFICATION, AUTHORIZATION, ACCESS MANAGEMENT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСТУ – державний стандарт України;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

СКБД – система керування базами даних;

СУІД – система управління ідентифікацією та доступом.

ЗМІСТ

ВСТУП

Процес інформатизації охоплює більшість сфер людської діяльності, будь то соціальна, освітня, фінансова, тощо. З розвитком технологій інформація швидко набуває значимості.

Достатньо велика кількість бізнес процесів підприємств малого бізнесу реалізуються з використанням веб-додатків. Майже усі ці додатки є частинами розподілених інформаційно-телекомунікаційних систем (ІТС). В кожній такій системі циркулює інформація, порушення цілісності та доступності якої може призвести до збитків.

Побудова системи інформаційної безпеки для захисту інформації в розподіленій ІТС не можлива без упровадження двох взаємопов'язаних процесів: ідентифікації та автентифікації. Послуга НИ «Ідентифікація та автентифікація» є необхідною умовою для реалізації багатьох інших послуг конфіденційності, цілісності, доступності та спостережності [1].

Де-факто, саме множинна автентифікація є стандартом в розподілених ІТС. Проте реалізація послуги на рівні НИ-3 «Множинна ідентифікація та автентифікація» ускладнює розробку та підтримку системи інформаційної безпеки, та взаємодію кінцевого користувача з ІТС. Саме тому в останні роки виникла тенденція використання адаптивної автентифікації – процесу ідентифікації та автентифікації користувача з застосуванням поведінкового аналізу, що визначає наскільки автентичною є спроба ідентифікації та автентифікації, та встановлює необхідний метод автентифікації для цієї спроби.

Традиційно, для захисту інформації в розподілених ІТС підприємств малого бізнесу використовується механізм парольної автентифікації користувачів. Проте аналіз існуючих трендів реалізації процесів ідентифікації та автентифікації показує поступовий перехід на системи управління ідентифікацією та доступом (СУІД), які забезпечують більш високий рівень безпеки інформації, простоту використання, підвищення ефективності роботи ІТС та зниження витрат. За період з 2020 року по

2021, капіталізація ринку систем управління ідентифікацією та доступом зросла з 12,04 до 13,92 мільярдів доларів США [2], а прогнозована вартість ринку на 2026 рік складає майже 32 мільярди доларів [3].

Незважаючи на зростаючу популярність, більшості СУІД бракує механізму адаптивної автентифікації, а самі системи поширюються під пропрієтарними ліцензіями та дорогі для підприємств малого бізнесу. Також майже усі СУІД забезпечені механізмами збору телеметрії. Тому існує необхідність у створенні системи управління ідентифікацією та доступом, яка б поєднувала в собі простоту інтеграції, низьку вартість підтримки та обслуговування, та можливість використання адаптивної автентифікації.

РОЗДІЛ 1. СТАН ПИТАТАНЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

Майже в кожній інформаційно-телекомунікаційній системі циркулює інформація, порушення цілісності та доступності якої може спричинити значні збитки власнику інформації, або її розпоряднику. На сучасному етапі розвитку суспільства, кількість загроз інформаційній безпеці збільшується з кожним днем, і причиною тому є загальна інформатизація усіх сфер нашого життя. Винятком не є і підприємства малого бізнесу: достатньо велика кількість бізнес процесів реалізуються з використанням веб-сервісів та веб-додатків.

Згідно з 2019 Data Breach Investigations Report, 43% жертв кібератак в США – представники малого бізнесу [4]. A Fundera показує, що кількість кібератак на підприємства малого бізнесу США у 2020 році збільшилось на 424% у порівнянні з 2019 роком [5]. Також, у звіті від National Cyber Security Alliance зазначено, що 60% компаній виходять з бізнесу після кібератаки [6]. Причина таких високих показників – використання спрощених механізмів парольної автентифікації – 63% випадків витоку даних сталося через використання слабких чи вкрадених паролів та відсутність багатофакторної автентифікації [7].

Для захисту інформації в розподілених ІТС від несанкціонованого доступу (НСД) використовуються комплекси засобів захисту (КЗЗ) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації [8]. Різновидом КЗЗ, що стрімко набирає популярність у підприємств малого та середнього бізнесу – це системи управління ідентифікацією та доступом. У загальному розумінні, СУІД – це система бізнес-процесів для управління ідентифікаційними даними та процесами ідентифікації й автентифікації. Така система складається з організаційної політики та спеціальних програмних і/або програмно-апаратних засобів.

Більшості сучасних СУІД бракує механізму адаптивної автентифікації, а самі системи поширюються під пропрієтарними ліцензіями та дорогі для підприємств малого бізнесу.

1.2 Системи управління ідентифікацією та доступом

Система управління ідентифікацією та доступом – це комплекс засобів захисту, що дозволяє виконувати ідентифікацію та автентифікацію користувачів, управління даними користувачів та процесами ідентифікації й автентифікації як на рівні політик безпеки, так і на рівні реалізації процесів. Для забезпечення контролю доступу до інформаційних ресурсів в СУІД використовується диспетчер доступу [9].

Узагальнено, СУІД складається з трьох основних компонентів (рис. 1.1):

– підсистема управління ідентифікацією – виконує ідентифікацію та автентифікацію користувачів, а також дозволяє керувати даними користувачів;

– підсистема управління доступом – дозволяє керувати процесами ідентифікації та автентифікації, та сесіями користувачів;

– диспетчер доступу – виконує контроль доступу суб'єктів до інформаційних ресурсів, та реєстрацію подій.

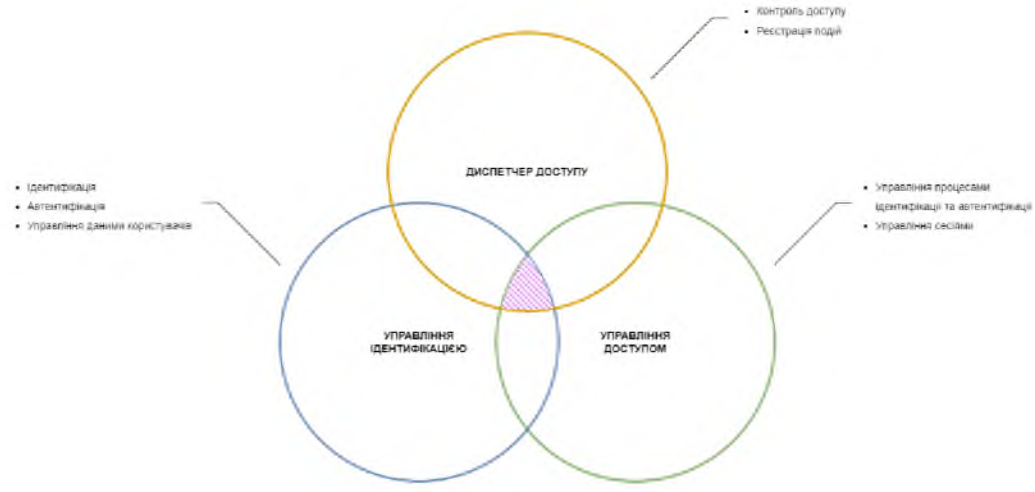

Рисунок 1.1 – Система управління ідентифікацією та доступом

Типова система управління ідентифікацією та доступом складається з:

– веб-серверу, що забезпечує комунікацію між системою та користувачем з використанням протоколу HTTP;

– сховища ідентифікаційних даних, що зберігає дані, які використовуються для ідентифікації та автентифікації користувачів. Це сховище може належати федеративному постачальнику ідентифікаційних даних у разі використання протоколу Oauth2;

– пре-процесінгу запиту користувача, що виконує перевірку запиту згідно з набором правил (політикою безпеки), встановлених адміністратором системи;

– сховища даних користувачів, що зберігає такі користувацькі дані, як інформацію про привілеї, налаштування, тощо;

– пост-процесінгу запиту користувача, що виконує перевірку запиту згідно з набором правил (політикою безпеки), встановлених адміністратором системи, та згідно з привілеями користувача;

– додаткових механізмів багатофакторної автентифікації та/або процесів перевірки особистості користувача, встановлених адміністратором системи.

Структурну схему типової системи управління ідентифікацією та доступом наведено у Додатку Д.

Системи управління ідентифікацією та доступом допомагають організаціям відповідати галузевим вимогам й економити витрати за рахунок мінімізації часу, необхідного для вирішення проблем, пов'язаних з обліковими записами користувачів. Управління ідентифікацією та доступом стандартизує і навіть автоматизує критичні аспекти управління ідентифікацією, автентифікацією і авторизацією, економлячи час і гроші і знижуючи риски для бізнесу.

1.3 Класифікація систем управління ідентифікацією та доступом

Для того, щоб у подальшому виконати порівняльний аналіз систем управління ідентифікацією та доступом, необхідно їх класифікувати.

Однією з ознак, за якими можна класифікувати системи управління ідентифікацією та доступом, є фактори, на підставі яких виконується автентифікація. У загальному випадку розрізняють такі фактори автентифікації (рис. 1.2):

– фактор знання – те, що користувач знаєте, може бути будь-якими обліковими даними автентифікації, що складаються з інформації, якою володіє користувач, включаючи персональний ідентифікаційний номер (PIN), ім'я користувача, пароль або відповідь на секретне питання;

– фактор володіння – те, що у користувача є, може бути будь-яким посвідченням, ґрунтується на предметах, якими користувач може володіти і носити з собою, включаючи апаратні пристрої, такі як токен безпеки або мобільний телефон, використовуваний для прийому текстових повідомлень або запуску застосування автентифікації, яке може генерувати одноразовий пароль або PIN-код;

– фактор інгерентності – те, чим користувач є, зазвичай ґрунтується на якій-небудь формі біометричної ідентифікації, включаючи відбитки пальців, розпізнавання особи, сканування сітківки ока або будь-яку іншу форму біометричних даних;

– фактор місцеположення – може бути менш конкретним за попередні, але фактор місцезнаходження іноді використовується як доповнення до інших факторів. Місце розташування можна визначити з достатньою точністю за допомогою пристроїв, оснащених системою глобального позиціонування, або з меншою точністю шляхом перевірки мережевих адрес і маршрутів. Фактор місця розташування зазвичай не може використовуватися для автентифікації сам по собі, але він може доповнювати інші фактори, надаючи можливість виключити деякі запити. Наприклад, він може завадити зловмисникові, що знаходиться у видаленій географічній зоні, видати себе за користувача, який зазвичай входить в систему тільки зі свого дому або офісу в країні розташування організації;

– фактор часу – час автентифікації, сам по собі недостатній, але він може бути додатковим механізмом для відсіювання зловмисників, які намагаються отримати доступ до ресурсу в той час, коли цей ресурс недоступний для авторизованого користувача. Він також може використовуватися разом з місцем розташування. Наприклад, якщо користувач останній раз проходив автентифікацію опівдні в Україні, спроба автентифікації з Китаю через годину буде відхилена на основі поєднання часу і місця розташування.

Рисунок 1.2 – Фактори автентифікації

Крім цього, залежно від кількості факторів та вимог щодо захисту інформації, сучасні системи можуть реалізовувати наступні методи автентифікації (рис. 1.3):

– однофакторна – автентифікація, що здійснюється з використанням одного фактору (частіше за все – паролю);

– багатофакторна – автентифікація, що здійснюється з використанням двох або більшої кількості факторів;

– строга – автентифікація, під час якої використовується інформація без розкриття цієї інформації. Як правило, реалізується за допомогою асиметричних криптографічних алгоритмів.

Рисунок 1.3 – Метод автентифікації

Ще однією з ознак є наявність механізму адаптивної автентифікації, оскільки лише деякі з сучасних систем управління ідентифікацією та доступом мають подібний функціонал.

Також необхідним показником є можливість самостійного встановлення і налаштування СУІД, або ж використання за моделлю «програма як послуга» (англ. Software as a Service, SaaS) – модель, при якій постачальник програмного забезпечення самостійно встановлює і керує їм, надаючи доступ замовникам через мережу Інтернет.

Останніми, але не менш важливим із показників є тип ліцензії коду програмного забезпечення та наявність телеметрії.

1.4 Огляд існуючих СУІД

Для оцінки придатності до використання, в роботі розглянуто одні з найбільш популярних на сьогоднішній день [10] систем управління ідентифікацією та доступом:

– Okta (рис. 1.4) – це хмарна платформа, що дозволяє користувачам отримувати доступ до усіх програм, використовуючи для цього тільки один логін/пароль [11]. Один логін для доступу, наприклад, до Slack, Zoom, Gmail і Figma. При цьому Okta дозволяє робити це з комп'ютера, планшета або телефону. При цьому адміністратор може віднести користувача до певної групи усередині Okta, щоб надати доступ тільки до потрібного набору програм і сервісів. Має бібліотеку з тисячами готових інтеграції з різноманітними застосунками. Є однією з найпопулярніших систем. Використовується такими компаніями, як LinkedIn, Hubpost, T-Mobile і Hewlett Packard. Фактори автентифікації, які використовуються: знання, володіння, інгерентності. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;

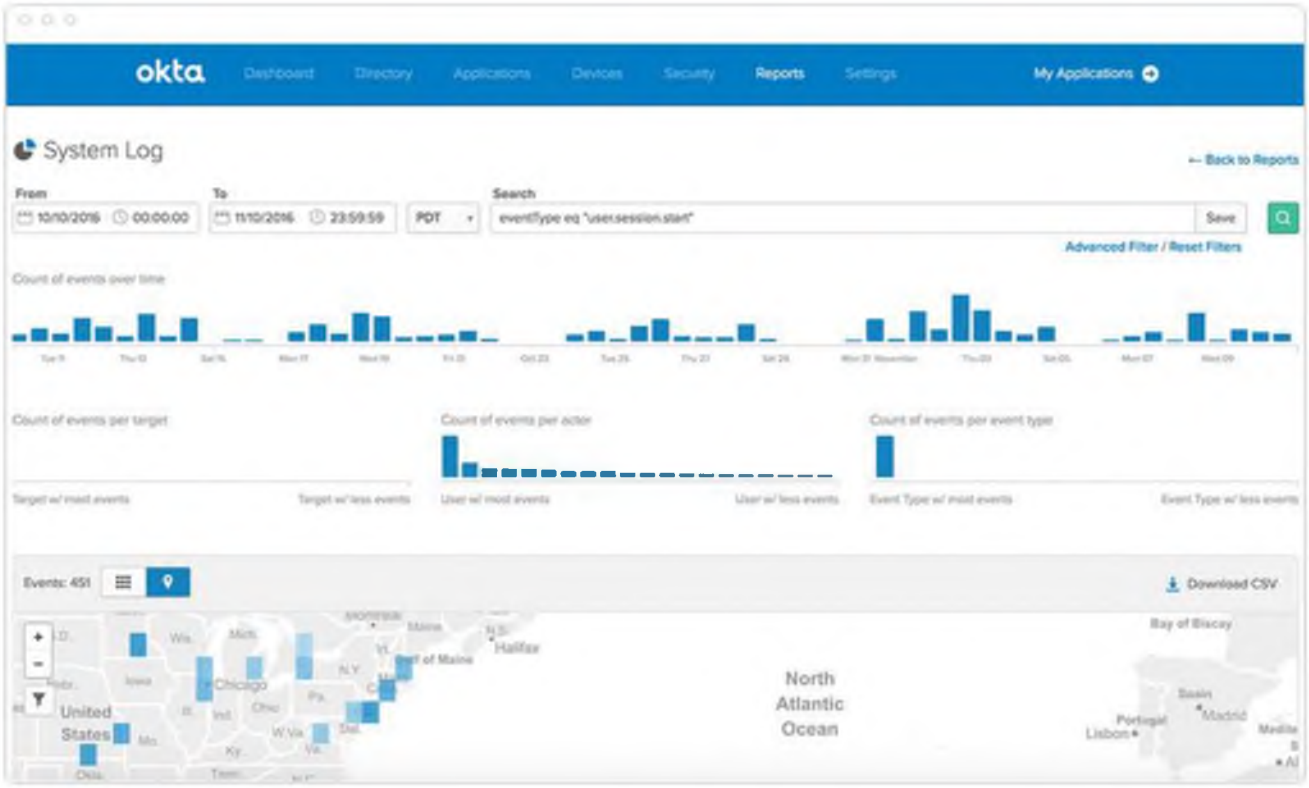

Рисунок 1.4 – Інтерфейс адміністратора СУІД Okta

– OpenIAM (рис. 1.5) – це платформа з відкритим вихідним кодом для управління доступом, дозволами і серверами федерації [12]. Складається з двох основних модулів: Identity Governance та Web Access Manager, що мають загальну інфраструктуру, завдяки чому система постає перед клієнтом як цілісне програмне забезпечення, а не набір окремих сервісів. Поширюється як по підписці, так і окремо для самостійної установки і налаштування. Використовується такими компаніями, як WarnerMedia та Deutsche Bank. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;

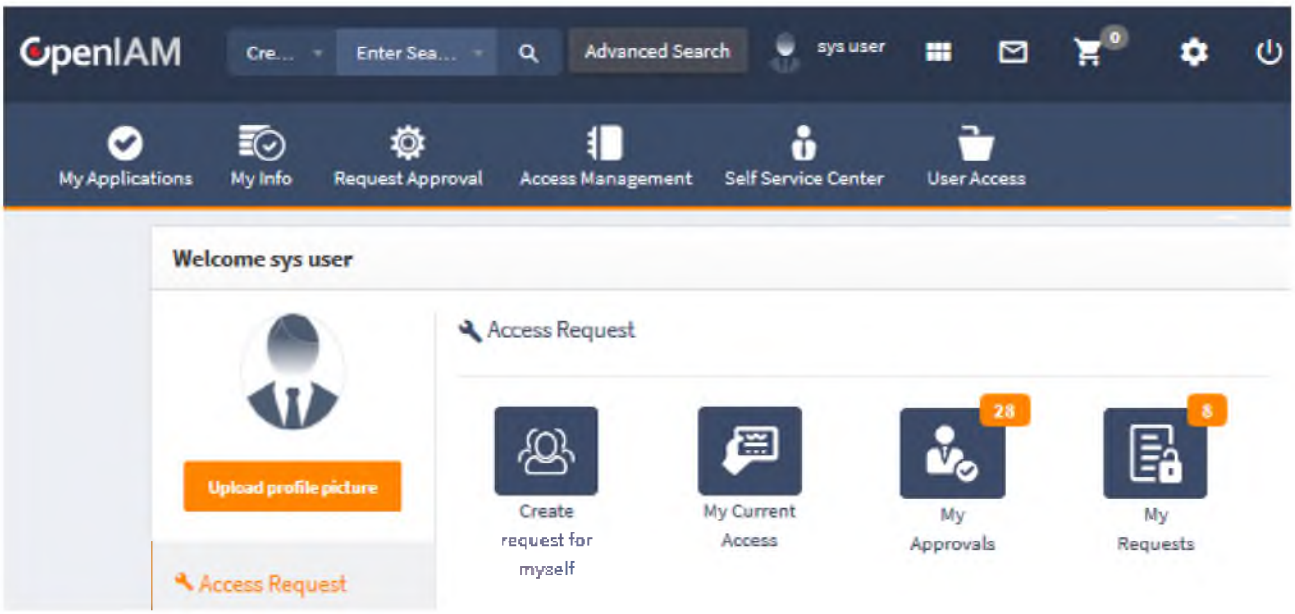

Рисунок 1.5 – Інтерфейс адміністратора СУІД OpenIAM

– Auth0 (рис. 1.6) – це платформа управління ідентифікацією, спрямована на полегшення для розробників інтеграції платформи із застосуваннями [13]. Є набором окремих API і інструментів для реалізації SSO і управління користувачами. Поставляється в декількох варіантах для різних сценаріїв: B2C (система для автентифікації звичайних користувачів за допомогою ідентифікатора і пароля, а також OAuth2), B2B (система для автентифікації ділових партнерів за допомогою SAML, LDAP і AD), B2E (система для автентифікації співробітників усередині організації). Із закритим вихідним кодом, поширюється по підписці. Є безкоштовні варіанти для невеликих проектів і некомерційних організацій. Популярний програмний засіб, інтегрований в інфраструктуру таких компаній, як Mazda, AMD і Pfizer. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;

– Ory Kratos – це хмарна система управління користувачами [14]. Вона забезпечує вхід і реєстрацію користувачів, багатофакторну автентифікацію і зберігання інформації про користувачів за допомогою API. Вона повністю налаштовується, підтримує широкий спектр протоколів, таких як Google Authenticator, і зберігає інформацію про користувачів за допомогою схеми JSON.

Ory Kratos реалізує усі необхідні потоки, такі як вхід і вихід з системи, активація облікового запису, багатофакторна автентифікація, управління профілями і сесіями, помилки, з якими стикається користувач, і методи відновлення облікового запису. Поширюється як по платній підписці, так і окремо для самостійної установки і налаштування. З відкритим вихідним кодом. Використовується такими компаніями, як Sainsbury's, Tinkoff Group і Segment. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна;

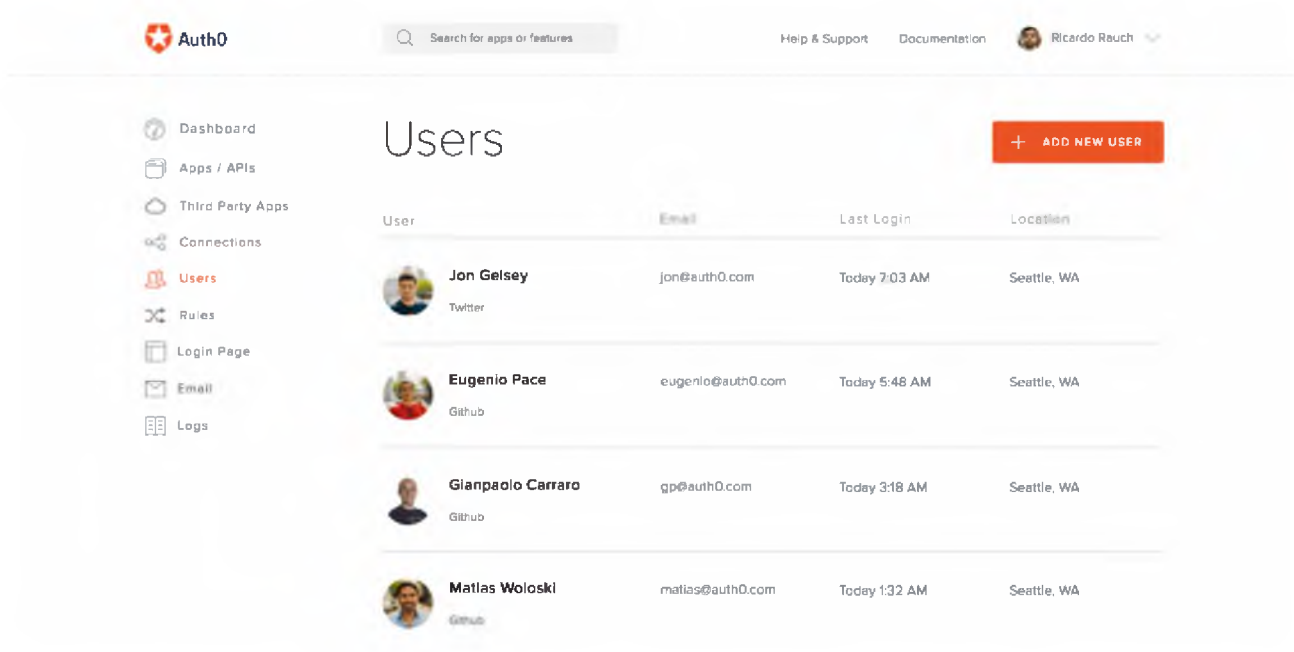

Рисунок 1.6 – Інтерфейс адміністратора СУІД Auth0

– Keycloak (рис. 1.7) – це система управління ідентифікацією і доступом з відкритим вихідним кодом для сучасних застосувань і сервісів [15]. Вона дозволяє додати автентифікацію з мінімальними витратами. Система з відкритим кодом для реалізації SSO з можливістю управління доступом. Основні функції: User Federation (зв'язування цифрової особистості користувача та її атрибутів, що зберігаються у кількох різних системах управління ідентифікацією), Identity Brokering (створення довірчих відносин із зовнішнім постачальником ідентифікаційних даних), Social Login (схема автентифікації, що дозволяє отримати доступ до різних незалежних сервісів з одними даними автентифікації за допомоги соціальних мереж). Поширюється безкоштовно для самостійної установки і

налаштування. Використовується такими компаніями, як Gympass і Backbase. Фактори автентифікації, які використовуються: знання, володіння. Методи автентифікації, які можуть бути реалізовані: однофакторна, багатофакторна.

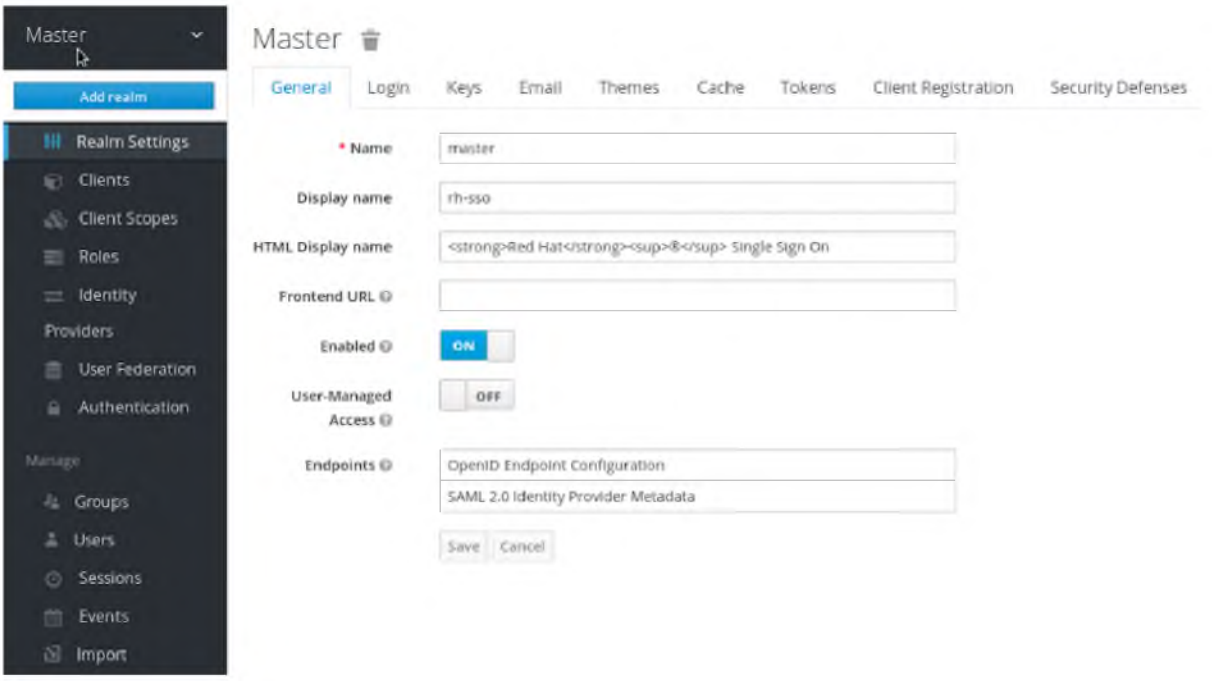

Рисунок 1.7 – Інтерфейс адміністратора СУІД Keycloak

1.5 Порівняння систем управління ідентифікацією та доступом

Порівняння систем ідентифікації та контролю доступу наведено в таблиці 1.1.

Таблиця 1.1 – Порівняння СУІД:

Характеристика	Система				
	Okta	OpenIAM	Auth0	Ory Kratos	Keycloak
Фактор знання	+	+	+	+	+
Фактор володіння	+	+	+	+	+
Фактор інгерентності	+	-	-	-	-
Фактор місцеположення	-	-	-	-	-

Продовження таблиці 1.1:

Характеристика	Система				
	Okta	OpenIAM	Auth0	Ory Kratos	Keycloak
Фактор часу	-	-	-	-	-
Однофакторна автентифікація	+	+	+	+	+
Багатофакторна автентифікація	+	+	+	+	+
Строга автентифікація	-	-	-	-	-
Адаптивна автентифікація	+	-	+	-	-
SaaS	+	+	+	+	-
Можливість самостійного встановлення та налаштування	-	+	-	+	+
Телеметрія	+	+	+	+	+
Тип ліцензії	Пропрієтарний	GNU GPL v3 (з відкритим кодом)	Пропрієтарний	Apache 2.0 (з відкритим кодом)	Apache 2.0 (з відкритим кодом)

Майже кожна з систем поставляється за моделлю «програма як послуга», тоді як програмних засобів для самостійного встановлення/налаштування значно менше.

Використання моделі SaaS прискорює інтеграцію з ІТС замовника, проте є залежність від інфраструктури сторонньої компанії та її захищеності, завдяки чому

виникають додаткові ризики, пов'язані з конфіденційністю, доступністю та цілісністю:

– було зламано 5 камер в офісі Okta [16];

– сервіси Auth0 були недоступні в ході DDoS атаки на DNS провайдера DNSimple [17].

Також більшість систем мають закритий початковий код, що підвищує їх кінцеву вартість і веде за собою загрози безпеці інформації:

– CVE-2020-5263 – Auth0 Insufficiently Protected Credentials [18];

– CVE-2021-32641 – Auth0 Improper Neutralization of Input During Web Page Generation («Cross-site Scripting») [19];

– CVE-2021-28113 – Okta Command Injection [20].

Механізм адаптивної автентифікації присутній лише у декількох системах, і доступний як платна послуга. Також більшість СУІД мають закритий вихідний код, що підвищує їх кінцеву вартість, а відсутність стороннього аудиту кодової бази може стати причиною появи додаткових вразливостей. А ті системи, що доступні безоплатно та мають відкритий код, є складними в конфігурації, ресурсномісткими, мають багато надлишкового функціоналу, та збирають телеметрію.

СУІД з відкритим початковим кодом значно менше, ніж пропрієтарних; такі програмні засоби, як OpenIAM і Keycloak мають стару кодову базу, написану на мові Java. Такі системи потребують багато ресурсів для функціонування, та є важкими в експлуатації для невеликих організацій, що не потребують СУІД рівня великих організацій.

Ory Kratos написаний на сучасній та швидкій мові Golang, проте як і раніше досить складний в налаштуванні і експлуатації, хоча і має певні переваги в порівнянні з ПЗ на Java: споживає менше ресурсів за рахунок своєї архітектури і використання мови Golang, показує більш високу ефективність і відмовостійкість, більш конфігурований і безпечний (код протестований на 79%, а в розробці застосовуються найсучасніші підходи по забезпеченню безпеки). Проте у Kratos є більш істотні недоліки, ніж складність: навіть при тому, що це – система з

відкритим кодом, в ньому присутній збір телеметрії, а для імплементації керування доступом на основі ролей потрібне підключення стороннього ПО.

1.6 Висновки

На практиці, у багатьох випадках необхідна система, яку можна інтегрувати в інформаційно-телекомунікаційну систему малого бізнесу з мінімальними зусиллями й витратами, та за найкоротший термін. Деякі існуючі СУІД надають готові конфігурації, проте вони є лише наочним прикладом роботи програмного засобу, а не готовою та безпечною системою для роботи в реальних умовах.

Таким чином, існує необхідність у створенні системи управління ідентифікацією та доступом, яка б поєднувала в собі простоту інтеграції SaaS продуктів і доступність open-source програмного забезпечення.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Вимоги до системи управління ідентифікацією та доступом

Перелік послуг, необхідних для реалізації системи управління ідентифікацією та доступом:

– НИ «Ідентифікація та автентифікація» – політика послуги поширюється на усіх користувачів системи та логічні диски на внутрішніх носіях бази даних.

В системі управління ідентифікацією та доступом, реалізація захисту від несанкціонованого доступу повинна спиратися на відповідні адміністративні заходи та програмно і/або програмно-технічні засоби, спрямовані на ідентифікацію та автентифікацію користувачів. В розподілених інформаційно-телекомунікаційних системах частіше за все використовуються такі ідентифікатори користувачів, як унікальне ім'я користувача або електронна адреса. Для автентифікації користувачів необхідна реалізація однофакторного та багатофакторного методів автентифікації.

Взаємодія з системою, що використовує багатофакторну автентифікацію, є ускладненою для кінцевого користувача. Існує ризик, що користувачі не будуть використовувати багатофакторну автентифікацію замість однофакторної, або зовсім відмовляться від використання системи. Chubb Cyber Risk Survey 2019 Executive Summary показує, що лише 30% користувачів продовжують використовувати багатофакторну автентифікацію, якщо є можливість використовувати однофакторну [21]. Задля забезпечення високого рівню послуги НИ «Ідентифікація та автентифікація» та комфортної взаємодії користувача з системою існує необхідність в доповненні типової СУІД модулем адаптивної автентифікації.

Для захисту від несанкціонованого доступу даних автентифікації користувачів, що зберігаються на внутрішніх носіях баз даних, система управління ідентифікацією та доступом повинна забезпечувати криптографічний захист даних;

– КО «Повторне використання об’єктів» – політика послуги поширюється на сторінки оперативної пам’яті.

Задля забезпечення гарантій, що у разі повторного використання ресурсів системою, інший користувач або процес не отримає доступ до даних, що зберігаються в розділюваних об’єктах, СУІД повинна забезпечити очищення цих самих об’єктів в оперативній пам’яті;

– НР «Реєстрація» – політика послуги поширюється на усіх користувачів системи, системне та прикладне ПЗ.

Для контролю подій в системі, СУІД повинна забезпечувати реєстрацію та аналіз таких подій:

1) усі події, що пов’язані з фунціоналом системи (створення облікового запису, зміна даних облікового запису, відновлення доступу до облікового запису, тощо);

2) помилки в роботі веб-серверу;

3) помилки в роботі бази даних;

4) зміна конфігурації веб-серверу;

5) зміна політики безпеки.

Кожен запис повинен мати мітку часу та унікальний ідентифікатор події. Усі події, що пов’язані з взаємодією з користувачем, також повинні мати адресу користувача та його унікальний ідентифікатор в системі;

– ДЗ «Гаряча заміна» – політика послуги поширюється на сторонні бібліотеки ПЗ.

Адміністратор системи повинен мати можливість виконувати модернізацію системи без повторної інсталяції чи перериванні в обслуговуванні;

– ЦО «Відкат» – політика послуги поширюється на послідовність операцій над захищеними об’єктами (ідентифікаційними даними).

Система повинна забезпечити цілісність даних у разі порушення роботи бази даних при виконанні операцій читання, запису та видалення над ідентифікаційними даними;

– КВ «Конфіденційність при обміні» – політика послуги поширюється на мережеві з'єднання.

Взаємодія з користувачами через незахищене середовище потребує захисту об'єктів інформації від несанкціонованого ознайомлення;

– ЦВ «Цілісність при обміні» – політика послуги поширюється на мережеві з'єднання.

Взаємодія з користувачами через незахищене середовище потребує захисту об'єктів інформації від несанкціонованої модифікації;

– НВ «Ідентифікація і автентифікація при обміні» – політика послуги поширюється на мережеві з'єднання.

Робота з розподіленими постачальниками ідентифікаційних даних потребує однозначної ідентифікації стороннього джерела та можливості для цього джерела ідентифікувати СУІД перед наданням ідентифікаційних даних користувача.

2.2 Обґрунтування вибору моделі автентифікації

Для моделей автентифікації введено такі позначення:

– X – користувач;

– B – клієнт (браузер, мобільний додаток, тощо);

– S_p – сервер;

– A – ознаку автентифіковано;

– n – унікальне значення;

– H – хеш-функція;

– C – процес шифрування;

– P_k – k-й застосунок.

Розглянуто такі моделі автентифікації [22]:

– автентифікація за паролем. Ця модель заснована на тому, що користувач повинен надати серверу унікальний ідентифікатор (наприклад, username або поштовий адрес) U_n та пароль P_s для успішної ідентифікації та автентифікації в системі.

Відрізняють три різновиди моделі. Базова модель буде мати вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_p;\ S_p(A) \rightarrow B \rightarrow X$$

Другий різновид моделі відрізняється від базового, де U_n та P_s передаються у відкритому вигляді, наявністю шифрування, та виглядає так:

$$X(C(U_n), P_s(U_n)) \rightarrow B \rightarrow S_p;\ S_p(A) \rightarrow B \rightarrow X$$

Третім різновидом є двостороння модель з використанням хеш-функції, коли сервер надсилає клієнту унікальне значення n, а клієнт передає значення хешу паролю користувача, визначене з використанням вказаного n. Має такий вигляд:

$$X \rightarrow B \rightarrow S_p;\ S_p(n) \rightarrow B \rightarrow X;\ X(U_n, H(n, P_s) \rightarrow B \rightarrow S_p;\ S_p(A) \rightarrow B \rightarrow X$$

– автентифікація з застосунком. Ця модель заснована на тому, що користувач повинен надати застосунку унікальний ідентифікатор (наприклад, username або поштовий адрес) U_n та пароль P_s для успішної ідентифікації та автентифікації в системі. Має наступний вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow P_k(S_p);\ P_k(S_p(A)) \rightarrow B \rightarrow X$$

– автентифікація с сертифікатом.

Для цієї моделі введено такі позначення: сервер автентифікації – CA, сертифікат користувача – $C_a(k)$, що включає k атрибутів та підписаний CA – $C_a(k, CA)$, секретний ключ – K_s.

Тоді модель має такий вигляд:

$$X(C_a(k), K_s) \rightarrow CA;\ CA(C_a(k, CA) \rightarrow X;\ X(C_a(k, CA) \rightarrow S_p;\ S_p \rightarrow CA;\ S_p(A) \rightarrow B \rightarrow X$$

Модель є більш надійною, однак труднощі з розповсюдженням та підтримкою сертифікатів роблять цю модель автентифікації складно реалізованою.

– багатофакторна автентифікація. Ця концепція поєднує два або більше фактори автентифікації. Для входу в систему користувачеві необхідно надати дані кількох типів. Наприклад, те, що він знає (пароль), та те, чім він володіє (біометричний показник, або пристрій для генерації одноразового паролю). Наявність двох факторів дозволяє значною мірою підвищити рівень безпеки.

Модель має наступний вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow P_k(S_p);\ P_k(S_p, R) \rightarrow X;\ X(T(K_s, t))) \rightarrow B \rightarrow P_k(S_p)$$

де R – запит додаткових факторів автентифікації, $T(K_s, t)$ – токени, що генеруються на основі додаткових факторів автентифікації та поточного часу.

– автентифікація за ключами доступу. Ця модель використовується для автентифікації пристроїв, сервісів чи застосунків при зверненні до веб-сервісів – WS, які зберігаються на хмарному сервері – S_{ws}. Засобом автентифікації є ключ доступу K_a – довільний рядок символів, який генерується сервером S_{ws}. Модель має такий вигляд:

$$X(U_n, P_s) \rightarrow B \rightarrow S_{ws};\ S_{ws}(K_a) \rightarrow X;\ X(K_a) \rightarrow P_k(S_{ws})$$

Більш складним варіантом цієї моделі є модель автентифікації по ключам для незахищених з'єднань. Цей варіант включає в себе два ключа: відкритий ключ K_o та секретний ключ K_s. K_o використовується для ідентифікації клієнта, а K_s дозволяє згенерувати підпис. Ця модель має такий вигляд:

$$X(K_o) \rightarrow B \rightarrow S_{ws};\ S_{ws}(n) \rightarrow B \rightarrow X;\ X(H(n, K_s) \rightarrow B \rightarrow S_{ws}$$

Після встановлення з'єднання, сервер S_{ws} надсилає клієнту унікальне значення n, а клієнт, у свою чергу, повертає хеш цього значення, визначений з використанням K_s. Це дозволяє уникнути передачі усього ключа в оригінальному вигляді і підвищує надійність з'єднання.

– автентифікація за токенами. Ця модель автентифікації використовується в розподілених мережах з технологією Single Sign-On (SSO), де додаток SP делегує функцію автентифікації постачальникові ідентифікаційних даних IP. Прикладом є вхід у додаток з використанням облікового запису соціальної мережі. У даній моделі токен доступу $T(P_i)$ генерується $IP(P_i)$, де P_i – параметри токену. Модель має наступний вигляд:

$$X(K_o) \rightarrow B \rightarrow IP;\ IP(n) \rightarrow B \rightarrow X;\ X(H(n, K_s) \rightarrow B \rightarrow IP;\ IP(T(P_i)) \rightarrow X;\ X(T(P_i)) \rightarrow SP$$

Інтелектуальний підхід для вибору варіантів моделі автентифікації базується на створенні правил вибору. У якості інтелектуального інструменту вибору використовуються основані на цих правилах експертні системи. Варіант моделі автентифікації формується в автоматичному режимі при обробці профілів користувачів за правилами вибору. Але для СУІД ІТС малого бізнесу підхід до формування правил може бути спрощений та представлений як правила переходу між моделями. Ці правила можуть бути реалізовані окремим модулем адаптивної автентифікації.

2.3 Розробка модулю адаптивної автентифікації

Для виконання адаптивної автентифікації, необхідно прийняти рішення за яким алгоритмом модуль буде працювати. В роботі пропонується принцип триколірного маркування облікових записів користувачів. Кожному запису присвоюється «колір» – ціле число, що позначає рівень довіри до користувача:

– рівень 3 «червоний» – для автентифікації користувача буде використано багатофакторний метод автентифікації;

– рівень 2 «жовтий» – для автентифікації користувача буде використано однофакторний метод автентифікації;

– рівень 1 «зелений» – для автентифікації користувача буде використано однофакторний метод автентифікації.

Приклад доповнення СУІД модулем адаптивної автентифікації наведено на рисунку 2.1.

Після реєстрації, кожному користувачеві призначається «червоний» рівень. Цей рівень буде перевірятися модулем адаптивної автентифікації кожен раз при автентифікації користувача (рис. 2.2).

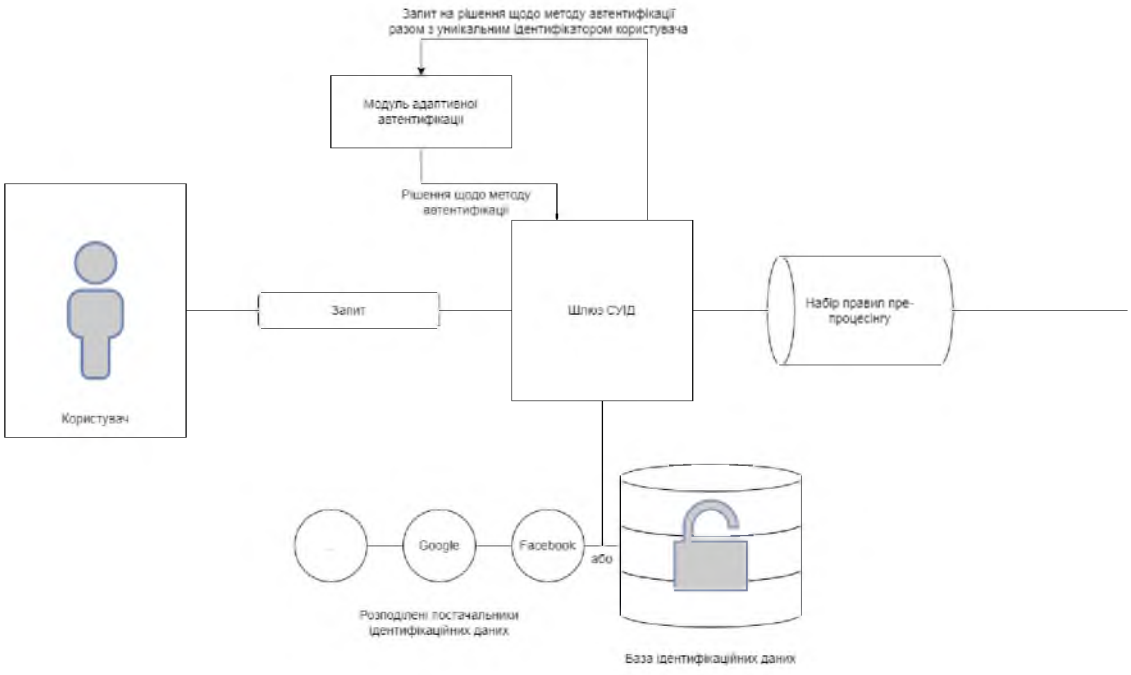

Рисунок 2.1 – Фрагмент структурної схеми СУІД з модулем адаптивної автентифікації

При кожному запиті на автентифікацію, буде розглянуто п’ять параметрів, на основі яких буде винесено рішення щодо методу автентифікації (встановлення рівню довіри):

– цифровий відбиток пристрою користувача;

– поточний рівень довіри;
– дата створення останньої сесії;
– проміжок часу типової сесії користувача;
– поточне місцеположення.

Незалежно від поточного рівню довіри користувача, буде встановлено «червоний» рівень, якщо запит на автентифікацію надходить з користувацького пристрою, якого не має в переліку відомих пристроїв користувача.

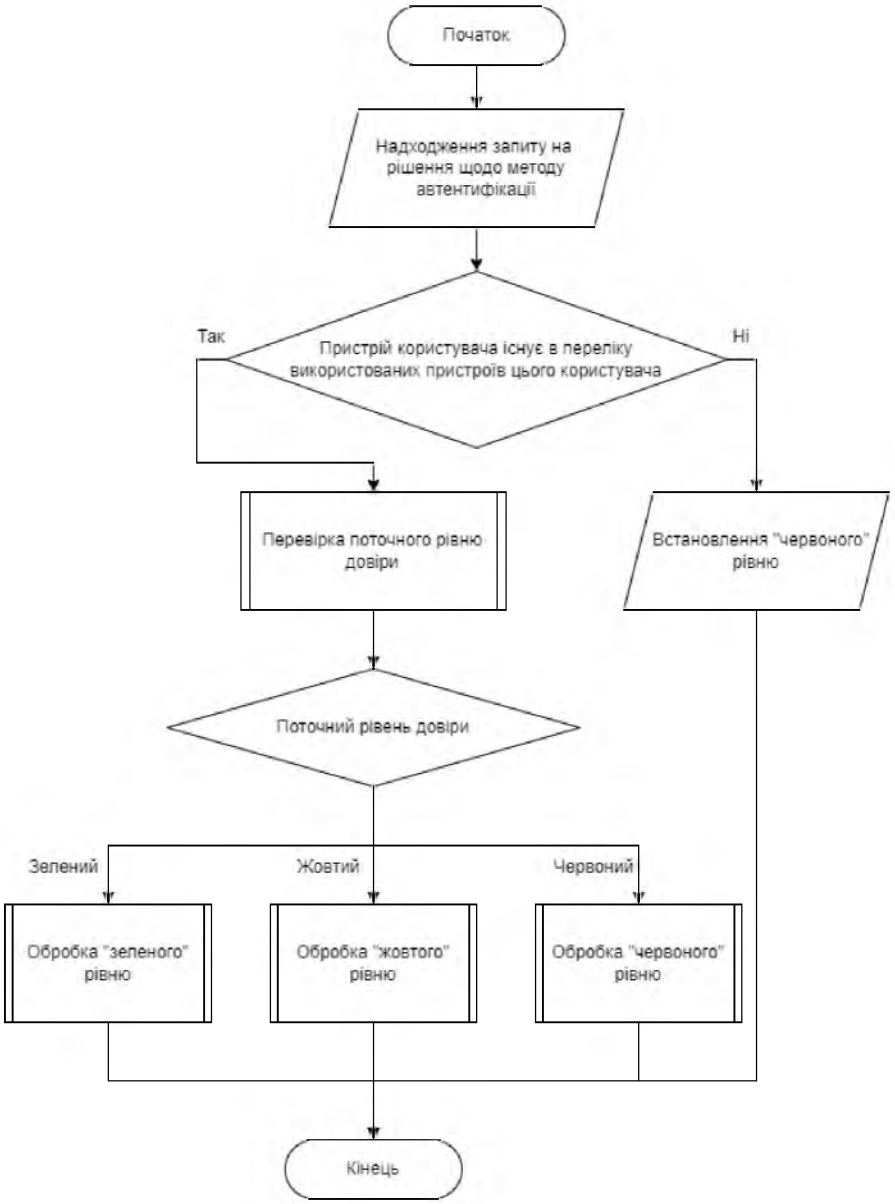

Рисунок 2.2 – Алгоритм роботи модулю адаптивної автентифікації

Алгоритм роботи кожного з рівнів відрізняється часовими параметрами та строгістю цих перевірок:

– «зелений» рівень (рис. 2.3):

Рисунок 2.3 – Алгоритм обробки запиту користувача при «зеленому» рівні довіри

Етапи роботи алгоритму:

1) виконується пошук та перевірка в базі даних інформації про дату створення останньої сесії користувача. Цей запис повинен бути створений не більше одного тижня тому від поточної дати;

2) виконується пошук та перевірка в базі даних інформації про типовий часовий проміжок сесії користувача від її створення до завершення. Поточний запит на автентифікацію не може бути за межами проміжку, визначеного запитом до бази даних, більш ніж на одну годину;

3) виконується пошук та перевірка в базі даних інформації про місцеположення користувача підчас останньої сесії. Поточне місцеположення користувача повинно бути у межах міста, визначеного запитом до бази даних.

– «жовтий» рівень (рис. 2.4):

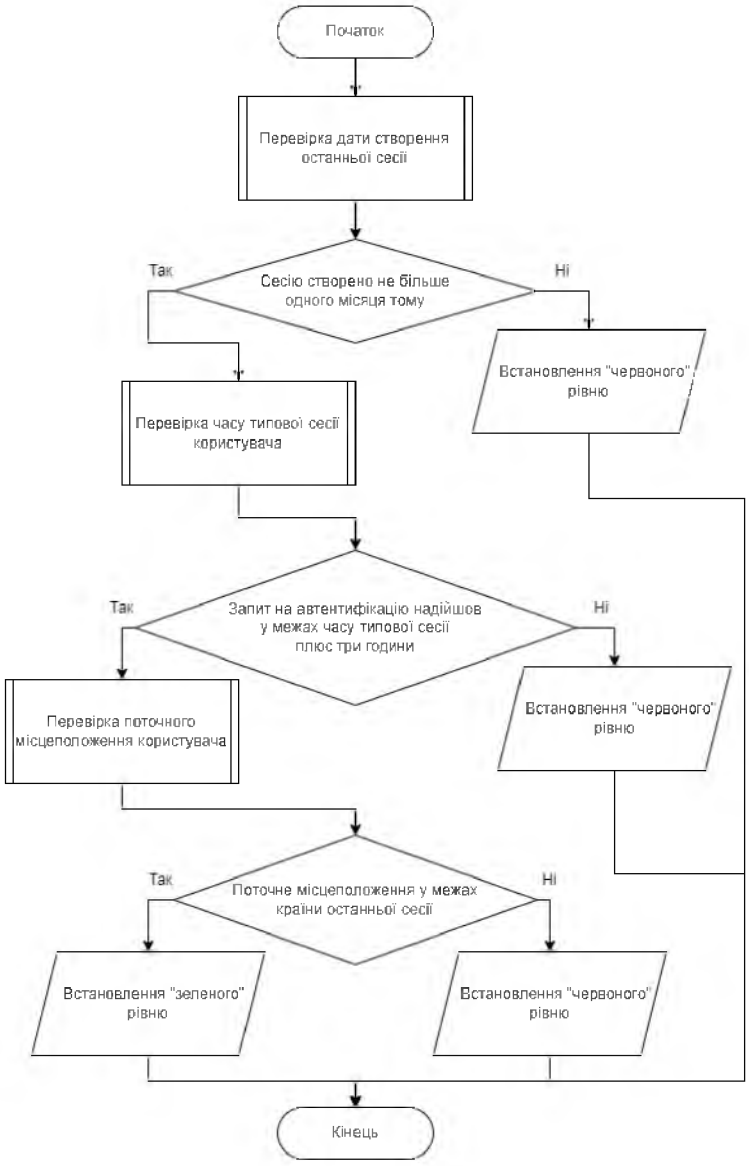

Рисунок 2.4 – Алгоритм обробки запиту користувача при «жовтому» рівні

Етапи роботи алгоритму:

1) виконується пошук та перевірка в базі даних інформації про дату створення останньої сесії користувача. Цей запис повинен бути створений не більше одного місяця тому від поточної дати;

2) виконується пошук та перевірка в базі даних інформації про типовий часовий проміжок сесії користувача від її створення до завершення. Поточний

запит на автентифікацію не може бути за межами проміжку, визначеного запитом до бази даних, більш ніж на три години;

3) виконується пошук та перевірка в базі даних інформації про місцеположення користувача підчас останньої сесії. Поточне місцеположення користувача повинно бути у межах країни, визначеної запитом до бази даних.

– «червоний» рівень (рис. 2.5):

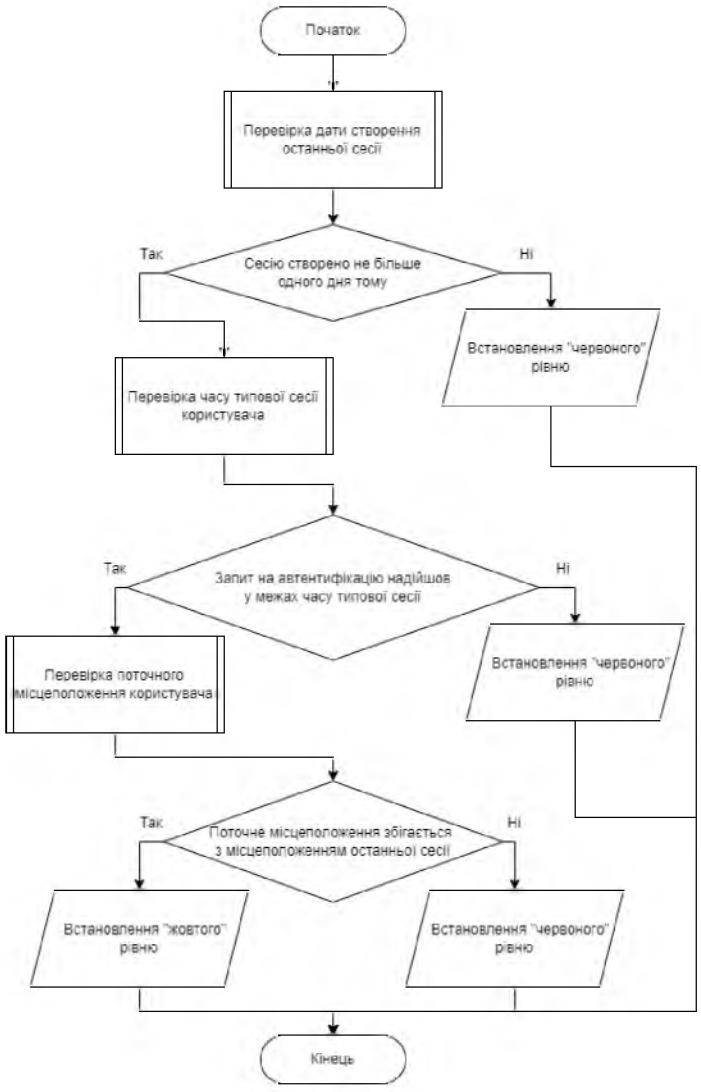

Рисунок 2.5 – Алгоритм обробки запиту користувача при «червоному» рівні

Етапи роботи алгоритму:

1) виконується пошук та перевірка в базі даних інформації про дату створення останньої сесії користувача. Цей запис повинен бути створений не більше одного дня тому від поточної дати;

2) виконується пошук та перевірка в базі даних інформації про типовий часовий проміжок сесії користувача від її створення до завершення. Поточний запит на автентифікацію не може бути за межами проміжку, визначеного запитом до бази даних;

3) виконується пошук та перевірка в базі даних інформації про місцеположення користувача підчас останньої сесії. Поточне місцеположення користувача повинно збігатися з останнім відомим місцеположенням, визначеним запитом до бази даних.

2.4 Обґрунтування функціональної схеми СУІД

Система управління ідентифікацією та доступом з підтримкою адаптивної автентифікації (рис. 2.6) відрізняється від типової СУІД наявністю:

– служби адаптивної автентифікації – програмний модуль або окремий сервіс, що виконує перевірку рівню довіри при автентифікації користувача. Ця служба отримує запити від служби ідентифікації та автентифікації, та виносить рішення щодо методу автентифікації, проводячи аналіз показників із запиту користувача та сховища ідентифікаційних даних;

– служби пошуку аномалій – програмний модуль або окремий сервіс, що виконує періодичну перевірку останнього часу сесії користувача, аналізує типовий час сесії користувача та розташування клієнтського пристрою. Взаємодіє лише зі сховищем ідентифікаційних даних, змінюючи рівні довіри для користувачів.

Також до складу СУІД з підтримкою адаптивної автентифікації входять:

– шлюз – веб-сервер, через який користувач взаємодіє із системою. Виконує початкову перевірку запитів та маршрутизацію цих самих запитів для подальшої їх обробки;

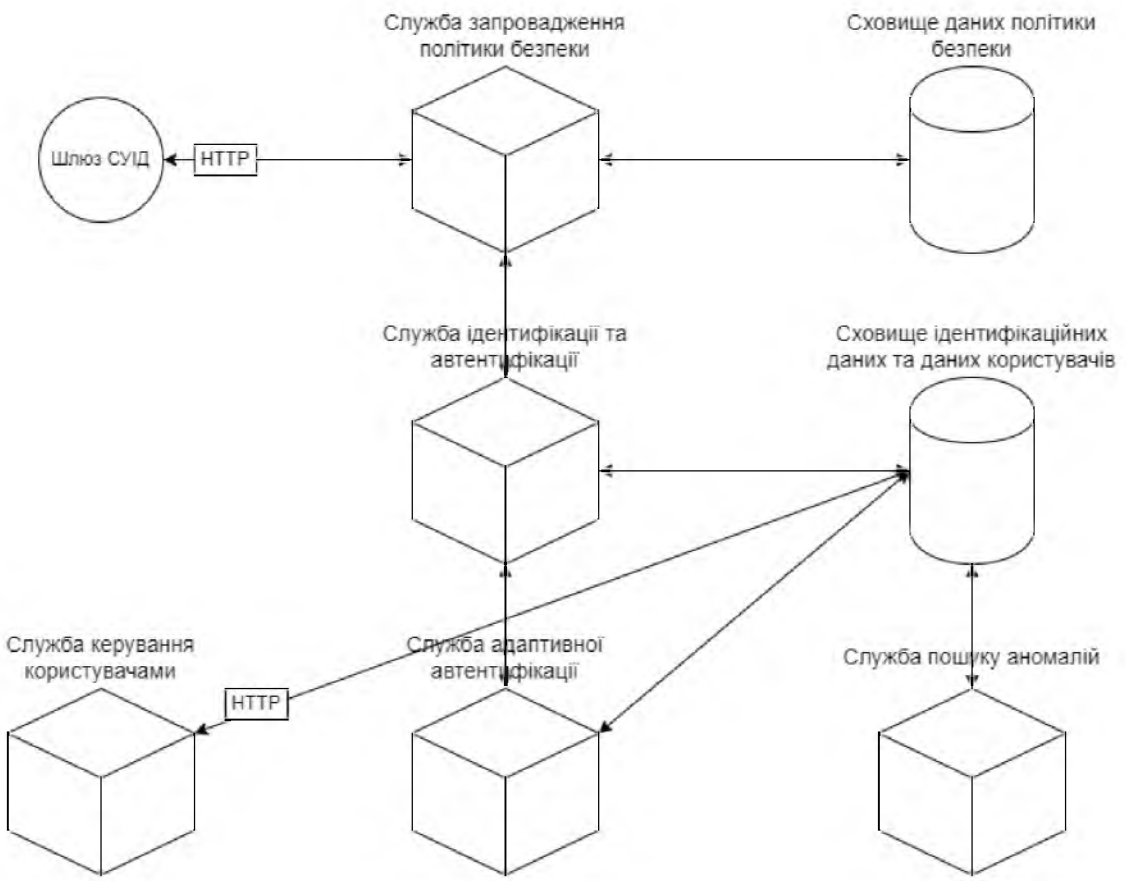

Рисунок 2.6 – Функціональна схема СУІД

– служба запровадження політики безпеки – програмний модуль або окремий сервіс, що виконує пре- та пост-процесінг запитів користувачів, перевіряючи їх згідно з набором правил (політикою безпеки);

– сховище даних політики безпеки – об’єктне сховище, що зберігає файли політики безпеки у форматі JSON;

– сховище ідентифікаційних даних та даних користувачів – СКБД, що забезпечує безпечний доступ та зберігання даних користувачів;

– служба керування користувачами – окремий сервіс, що надає доступ адміністраторові системи до засобів керування даними користувачів.

Точкою взаємодії користувача з системою ідентифікації та автентифікації є шлюз, що являє веб-сервіс, який використовує протокол HTTP. Цей сервіс виконує початкову валідацію вхідних даних та ведення журналу вхідних запитів та вихідних відповідей.

Після надходження запиту до шлюзу та проходження процесу валідації, запит користувача передається до служби запровадження політики безпеки. Ця служба взаємодіє із об'єктним сховищем даних політики безпеки, яке зберігає файли політики – набір правил валідації, обробки та підготовки даних, що подається у вигляді файлу у форматі JSON. Служба запровадження політики безпеки виконує обробку запиту згідно з визначеними правилами та передає запит користувача до служби ідентифікації та автентифікації.

Служба ідентифікації та автентифікації – центральна складова системи, що виконує обробку запиту користувача у контексті визначеної задачі, будь то реєстрація, вхід в систему чи відновлення доступу. Взаємодіє із сховищем ідентифікаційних даних та даних користувачів. У ході обробки запиту та автентифікацію викликає службу адаптивної автентифікації, передаючи унікальний ідентифікатор користувача, отриманий із сховища ідентифікаційних даних, та контекст – час надходження запиту, місцеположення користувача, цифровий відбиток пристрою, що використовує користувач.

Служба адаптивної автентифікації виконує перевірку автентичності запиту, перевіряючи його контекст на основі рівню довіри до користувача, виходячи з інформації про попередні запити, яку служба отримує через взаємодію зі сховищем ідентифікаційних даних та даних користувачів. У результаті перевірки, служба оновлює рівень довіри до користувача та повертає до служби ідентифікації та автентифікації рішення щодо методу автентифікації, яке буде визначено новим рівнем довіри.

На цьому етапі служба ідентифікації та автентифікації може запросити багатофакторну автентифікацію у користувача, або ж виконати його запит в залежності від рішення служби адаптивної автентифікації. У любому випадку, відповідь буде передано до служби запровадження політики безпеки, яка виконає обробку відповіді згідно зі встановленими правилами. Цю відповідь буде передано до шлюзу та відправлено користувачеві.

Окремим сервісом є служба пошуку аномалій, що взаємодіє із сховищем ідентифікаційних даних та даних користувачів. Цей сервіс виконує періодичну перевірку та оновлення записів в базі даних у разі знаходження застарілих сесій чи змін у місцезнаходженні користувача. Ця служба працює окремо не взаємодіючи з іншими модулями, та не виконуючи обробку запитів користувачів.

Також окремим сервісом є служба керування користувачами, яка надає доступ адміністраторові системи до засобів керування даними користувачів. Взаємодіє зі сховищем ідентифікаційних даних та даних користувачів, та має веб-інтерфейс адміністратора. Працює окремо, не виконуючи обробку запитів звичайних користувачів. Самостійно виконує ідентифікацію та автентифікацію адміністраторів з використанням строгого методу автентифікації і асиметричної криптографії.

Схему необхідно реалізувати програмно. Програмно-апаратна реалізація не підходить у даному випадку, тому що вона потребує закупівель дорогих технічних засобів, що неприпустимо для малого бізнесу.

2.5 Обґрунтування вибору мови програмування для реалізації СУІД

Вибір мови програмування може підвищити якість кінцевого продукту та рівень безпеки й надійність програмного засобу в цілому. Мови програмування розглядалися за наступними критеріями:

– збирання сміття – автоматичний процес управління пам’яттю, коли спеціальний процес періодично звільняє пам’ять, видаляючи об’єкти, які вже не потрібні. Забезпечує очищення розділюваних об’єктів. Реалізує послугу «Повторне використання об’єктів» на рівні КО-1;

– статична типізація – кожна змінна пов’язується з певним типом даних, який не може бути змінено пізніше;

– екосистема – модульна архітектура та велика кількість існуючих бібліотек значно пришвидшують розробку програмного забезпечення. Модульна

архітектура забезпечує можливість оновлення окремих компонентів системи без переривання обслуговування, реалізує послугу «Гаряча заміна» на рівні ДЗ-1;

– довгострокова підтримка платформи – заморожування випуску нових функцій для стабільного релізу програмного засобу з корегуванням помилок та закриттям вразливостей у вигляді окремих патчів. Таких підхід використовується для забезпечення стабільності та безперервності роботи програмних засобів на базі цієї платформи.

– підтримка засобів ведення та аналізу журналів реєстрації подій – наявність стандартного механізму запису подій чи можливість використання сторонніх засобів реалізує послугу «Реєстрація» на рівні НР-2.

Згідно з перерахованими критеріями було підібрано такі мови програмування:

– Golang – компільована мова програмування з підтримкою багатопоточного програмування. Має сувору статичну типізацію та збиральник сміття, що використовує алгоритм триколірного маркування. Програмне забезпечення, написане мовою Golang, має модульну архітектуру та підтримує використання сторонніх бібліотек (пакетів). Довгострокова підтримка стабільної версії платформи – один рік з моменту релізу;

– Typescript – мова програмування зі статичною типізацією, що транслюється в Javascript. Як і Javascript, ця мова може бути використана для розробки веб-сервісів на платформі Node.js. Має збиральник сміття за алгоритмом роботи схожий на збиральник сміття з напівпросторовим копіюванням Роберта Хелстеда. Використовує модульну архітектуру пакетів, довгострокова підтримка платформи – 3 роки;

– Java – об’єктно-орієнтована мова програмування зі статичною типізацією. Має п’ять різних імплементацій збиральника сміття та потужну систему пакетів для забезпечення модульної архітектури програмного забезпечення. Довгострокова підтримка платформи – 8 років.

Усі три мови програмування можуть забезпечити достатньо швидку, стабільну та безпечну роботу програмного забезпечення, проте було обрано саме Typescript, тому що:

– Java - мова для розробки програмного забезпечення enterprise-рівня, що потребує більше ресурсів для роботи, ніж інші розглянуті варіанти;

– розробка на мові Java більш складна та вимагає високої кваліфікації розробників, що позначиться як на самому процесі розробки, так і на подальшому супроводі і підтримці продукту;

– Golang - відносно нова мова програмування, тому з економічної точки зору буде доволі складно забезпечити постійну підтримку програмного забезпечення на необхідному рівні.

– Golang має найменший строк підтримки стабільної версії, що позначиться на стабільності та безпеці програмного забезпечення, та буде потребувати більшої кількості коштів для підтримання робочого стану системи;

– модель роботи платформи Node.js, що заснована на подієвому циклі, забезпечує найменше споживання ресурсів. Це веде до зниження витрат для підприємства.

2.6 Обґрунтування вибору технології зберігання даних

Для зберігання даних в СУІД обрано реляційну систему керування базами даних (СКБД). СКБД – комплекс програм та засобів, призначених для створення баз даних, підтримання їх в актуальному стані та організації санкціонованого доступу до них [23].

Такий вибір зроблено тому, що реляційні бази даних призначені для збереження структурованих даних, а мова SQL є зрілою технологією з великою кількістю документації та підтримкою. Також перевагою реляційних СКБД є підтримка контролю доступу: адміністратор СКБД може надавати конкретним користувачам системи права на запис, читання та видалення даних окремо.

Використання реляційних систем керування базами даних захищає від втрати та пошкодження даних завдяки дотриманню ACID.

ACID (Atomicity, Consistency, Isolation, Durability) – набір властивостей СКБД, дотримання яких гарантує, що транзакції в базі даних не накладаються одна на одну, де транзакція – група послідовних операцій, яка є логічною одиницею роботи з даними.

Властивості ACID (рис. 2.7):

– атомарність – кожна транзакція розглядається як єдине ціле. Вона може або повністю провалитися, або повністю завершитися. Тобто якщо одну з операцій транзакції буде відхилено, то будуть відхилені усі інші зміни у межах транзакції. Атомарність перешкоджає частковому оновленню бази даних у кожній ситуації, включаючи помилки, збої та відключення електроенергії;

– узгодженість – в базу даний можна записати тільки достовірні дані, що відповідають усім визначеним правилам, будь то обмеження, тригери, чи каскади. Якщо вхідні дані не відповідають вимогам, до базу даних буде повернено у стан, що був до початку транзакції. Узгодженість запобігає пошкодженню бази даних некоректною транзакцією;

– ізольованість – незакінчені транзакції залишаються ізольованими, та жодні проміжні зміни не будуть видимі за межами транзакції. Ізольованість гарантує, що усі транзакції виконуються безпечно та незалежно;

– довговічність – дані зберігаються системою навіть при збої. Тобто при порушенні працездатності системи результати завершених транзакцій буде записано після відновлення робочого стану бази даних.

Дотримання цих властивостей реалізує послугу «Відкат» на рівні ЦО-1.

Обрано систему керування базами даних PostgreSQL, оскільки вона надає можливість шифрування даних на різних рівнях та забезпечує гнучкість у захисті даних від несанкціонованого доступу у результаті крадіжки серверу бази даних, несумлінного персоналу чи незахищених мереж.

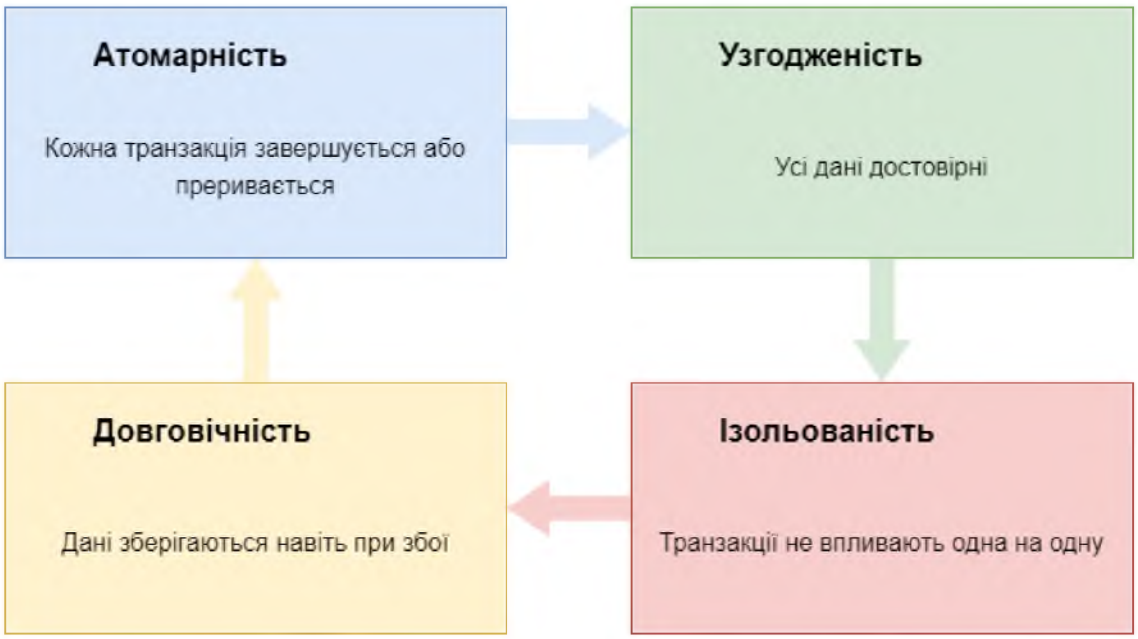

Рисунок 2.7 – Властивості ACID

СКБД PostgreSQL має такі функції:

– криптографічне перетворення паролів – збереження паролів користувачів бази даних у вигляді хешів, тому адміністратор не зможе визначити пароль користувача та використати його для доступу до інформації;

– шифрування стовпців – криптографічне перетворення конкретних стовпців таблиці за допомоги блокових шифрів. При запиті інформації з такого стовпця клієнт повинен надати ключ для дешифрування. Дешифрування виконується на сервері, а потім дані відправляються клієнту;

– шифрування сховища даних – блокове шифрування дискового простору на рівні файлової системи або блокового пристрою. Даний механізм безпеки забезпечує захист інформації від читання лише коли файлову систему не змонтовано;

– криптографічний захист мережевих з'єднань – можливість використання протоколу SSL або SSH тунелів.

Задля забезпечення конфіденційності даних обрано такі опції налаштування СКБД PostgreSQL:

– захист інформації, що зберігається на внутрішніх носіях серверу СКБД завдяки прозорому шифруванню блокових пристроїв інфраструктурою ядра Linux

Device Mapper (dm-crypt). Шифрування з використанням блокового шифру AES-256, режиму XTS та розміру ключа в 512 біт;

– захист паролів користувачів СКБД завдяки хешуванню цих паролів хеш-функцією SHA-256 та використанню механізму автентифікації SCRAM.

Набір функцій криптографічного захисту інформації СКБД PostgreSQL реалізує захист даних автентифікації для послуги НИ «Ідентифікація та автентифікація».

Використання реляційної бази даних та мови SQL відкриває потенційний вектор атак – SQL-ін'єкції, що використовує шкідливий SQL-код для маніпуляцій над базою даних щоб отримати доступ до інформації, яка не призначалася для відображення.

Успішна атака може привести до несанкціонованого читання таблиць, їх видалення, та отримання зловмисником адміністративних прав на базу даних. Можливість такої атаки виникає, коли розробники програмного забезпечення створюють динамічні запити до баз даних, котрі використовують введені користувачем дані (рис. 2.8):

```
const userIdentity: Identity = await db.one(`
    SELECT *
    FROM identities
    WHERE identities.id = '${req.query.identityId}'
`);
```

Рисунок 2.8 – Приклад вразливого коду

В даному прикладі використовуються дані, що надає користувач, у тому вигляді, у якому вони є. Тобто якщо користувач передасть замість параметру «identityId» SQL код – його буде виконано. Наприклад, якщо користувач передасть такий рядок, як «'b7131f77-6933-4100-b409-8e7d644fc02b'; DROP TABLE identities; —», то ці дані буде інтерпретовано як два запроси до бази даних (рис. 2.9):

```
SELECT *
FROM identities
WHERE identities.id = 'b7131f77-6933-4100-b409-8e7d644fc02b';

DROP TABLE identities;
```

Рисунок 2.9 – Інтерпретація шкідливого коду СКБД

Основним та найпоширенішим методом захисту від SQL-ін'єкцій є підготовлені вирази з прив'язкою змінних (параметризовані запити) [24]. Для створення такого запиту, розробникові необхідно спочатку визначити SQL-запит, а потім передати кожен параметр окремо. Такий стиль кодування дозволяє СКБД відрізняти код запиту від даних незалежно від того, які саме дані передає користувач (рис. 2.10):

```
const userIdentity: Identity = await db.one(`
    SELECT *
    FROM identities
    WHERE identities.id = '$<identityId:value>'
`, { identityId: req.query.identityId });
```

Рисунок 2.10 – Приклад параметризованого запиту

2.7 Обґрунтування вибору протоколу передачі даних

Взаємодія як з користувачами, так і з іншими системами в розподіленому оточенні виконується через незахищене середовище – мережу Інтернет. У такому оточенні не можливо гарантувати, що третя сторона не зможе отримати доступ до інформації, що передається. Тому повинні використовуватися криптографічні перетворення інформації, щоб мінімізувати ризик несанкціонованого доступу та модифікації даних.

Стандартом для отримання даних з веб-ресурсів є протокол HTTP. Його розширення, HTTPS, використовується для захисту інформації від

несанкціонованого доступу та модифікації. Основою розширення HTTPS є криптографічний протокол TLS, що використовує:

– асиметричне шифрування для автентифікації – для автентифікації серверу клієнт використовує відкритий ключ серверу для шифрування даних, що використовуються для узгодження спільного секретного ключа. Сервер може створити секретний ключ тільки у разі, якщо він може розшифрувати ці дані за допомогою свого закритого ключа. Для автентифікації клієнта сервер використовує відкритий ключ клієнта для розшифрування даних, які відправляє клієнт на етапі рукостискання. Обмін повідомленнями, що було зашифровано секретним ключем, завершує етап автентифікації. Обмін відкритими ключами виконується шляхом обміну цифровими сертифікатами, що видаються третьою стороною;

– симетричне шифрування для забезпечення конфіденційності – під час процесу рукостискання, клієнт та сервер узгоджують алгоритм шифрування та спільний секретний ключ, що буде використовуватися під час сесії. Усі повідомлення, що передаються між клієнтом та сервером, буде зашифровано з використанням встановленого алгоритму та ключа, що забезпечує конфіденційність повідомлення навіть у разі його перехоплення. Оскільки протокол TLS використовує асиметричне шифрування під час передачі спільного ключа, то з таким підходом відсутня проблема розподілу ключів.

– коди автентичності повідомлень для забезпечення цілісності – за допомоги секретного ключа, який було встановлено на етапі рукостискання, та хеш-функції створюється чек-сума повідомлення, що передається разом із ним у зашифрованому вигляді.

Розширення протоколу HTTPS разом з протоколом TLS реалізує послугу КВ-2 «Базова конфіденційність при обміні» та ЦВ-2 «Базова цілісність при обміні».

Використання сертифікатів TLS реалізує послугу НВ-2 «Автентифікація джерела даних».

2.8 Програма випробувань СУІД

Оцінка ефективності комплексу засобів захисту виконується згідно з положенням про державну експертизу в сфері технічного захисту інформації [25]. Експертиза технічних та програмних засобів проводиться шляхом випробувань. Для того, щоб виконати випробування, необхідно розробити програму та методику випробувань.

Основні пункти програми випробувань:

– перевірка можливості реєстрації користувача з наданням дійсних даних та відображення цієї події в журналі реєстрації;

– перевірка можливості реєстрації користувача з наданням недійсних даних та відображення цієї події в журналі реєстрації;

– перевірка можливості повторної реєстрації користувача та відображення цієї події в журналі реєстрації;

– перевірка можливості входу для користувача з різними рівнями довіри без порушення факторів володіння, місцеположення та часу, та відображення цієї події в журналі реєстрації;

– перевірка можливості входу для з різними рівнями довіри з порушенням фактору володіння (зміна цифрового відбитку клієнтського пристрою), та відображення цієї події в журналі реєстрації;

– перевірка можливості входу для користувача з різними рівнями довіри з порушенням фактору місцеположення (зміна місцеположення відносно останньої сесії), та відображення цієї події в журналі реєстрації;

– перевірка можливості входу для користувача з різними рівнями довіри з порушенням фактору часу (спроба входу у незвичний для користувача час), та відображення цієї події в журналі реєстрації;

– перевірка можливості відновлення доступу до облікового засобу;

– перевірка можливості виконання SQL-коду;

– перевірка очищення сторінок оперативної пам’яті;

– перевірка шифрування даних СКБД;

– перевірка можливості оновлення системи без переривання обслуговування;

– перевірка відміни послідовності операцій над даними у рамках транзакції;

– перевірка можливості використання незахищеного протоколу обміну даних.

Деякі з пунктів програми випробувань стосуються програмного коду та потребують періодичного тестування. Види тестування програмного забезпечення можна класифікувати за:

– ступенем автоматизації:

1) ручне тестування – процес ручної перевірки програмного забезпечення на помилки;

2) напівавтоматизоване тестування – процес перевірки програмного забезпечення, що поєднує ручне та автоматизоване тестування. Використовується тоді, коли не має можливості автоматизувати усі тести;

3) автоматизоване тестування – процес перевірки програмного забезпечення на помилки з використанням програмних засобів для виконання тестів та перевірки їх результатів.

– знанням системи:

1) тестування білої скриньки – метод перевірки програмного забезпечення, коли тестування виконується із знанням внутрішньої побудови програмного засобу;

2) тестування сірої скриньки – метод перевірки програмного забезпечення, коли тестування виконується із частковим знанням внутрішньої побудови програмного засобу;

3) тестування чорної скриньки – метод перевірки програмного забезпечення, коли тестування виконується без знання внутрішньої побудови та принципу роботи програмного засобу.

– ступенем ізольованості компонентів:

1) компонентне тестування – метод перевірки програмного забезпечення, що полягає в окремому тестуванні кожного компоненту коду засобу, де компонент - найменша частина програми, що може бути протестована;

2) інтеграційне тестування – метод перевірки програмного забезпечення, що полягає в тестуванні взаємодії поєднання окремих компонентів програми;

3) системне тестування – метод перевірки програмного забезпечення, що полягає в тестуванні системи, яка пройшла інтеграційне тестування, на відповідність усім вимогам, висунутим до програми.

Для контролю працездатності та узгодженості окремих компонентів програмного засобу пропонується використання автоматизованого компонентного тестування методом білої скриньки - перевірка правильності роботи окремих модулів та послуг безпеки згідно з вимогами до програмного засобу.

Для перевірки роботи системи та відповідності вимогам пропонується автоматизоване інтеграційне тестування методом чорної скриньки - перевірка основного функціоналу системи з симуляцією взаємодії з реальним користувачем.

2.9 Розробка програмної реалізації елементів СУІД

Шлюз визначає інтерфейс для взаємодії з користувачем – набір маршрутів веб-серверу та методів, що обробляють запити користувачів на цих маршрутах.

Фрагмент коду реалізації шлюзу СУІД наведено на рисунку 2.11.

Маршрути, що призначені для отримання даних від клієнтів виконують валідацію вхідних даних згідно з наборами правил, що визначені за допомогою схеми даних. Валідація вхідних даних є одним з базових механізмів безпеки програмних засобів, який підвищує стабільність та відмовостійкість сервісу. Правильно налаштована валідація вхідних даних допомагає захиститися від таких атак, як переповнення буферу, SQL-ін’єкції та XSS-атаки.

```
export async function selfService(instance: FastifyInstance): Promise<void> {
  const controller = setupDIContainer();

  instance.route({
    method: 'GET',
    url: '/v1/self-service/login',
    schema: {
      response: InitLoginFlowRes,
    },
    handler: controller.initLoginFlow,
  });

  instance.route({
    method: 'POST',
    url: '/v1/self-service/login',
    schema: {
      body: CompleteLoginFlowBody,
      querystring: FlowQuery,
      response: CompleteLoginFlowRes,
    },
    handler: controller.completeLoginFlow,
  });
}
```

Рисунок 2.11 – Фрагмент коду реалізації шлюзу СУІД

Для валідації використано бібліотеку AJV – засіб перевірки об’єктів даних на відповідність до структури, визначеної за допомогою схеми JSON. Повністю відповідає специфікації RFC 8927.

Фрагмент коду реалізації JSON схеми для валідації вхідних даних шлюзом СУІД наведено на рисунку 2.12.

```
export const CompleteLoginFlowBody = {
  description: 'Request body schema for completeRegistrationFlow method',
  type: 'object',
  required: ['csrf_token', 'method', 'password', 'traits'],
  properties: {
    csrf_token: {
      description: 'Anti-CSRF token',
      type: 'string',
    },
    method: {
      description: 'Login method',
      type: 'string',
    },
    password: {
      description: "User's password",
      type: 'string',
    },
    password_identifier: {
      description: 'Email or username of the user trying to login',
      type: 'string',
    },
  },
} as const;
```

Рисунок 2.12 – Фрагмент коду реалізації JSON схеми

Запит користувача, що пройшов етап валідації, потрапляє до сервісу запровадження політики безпеки. Даний сервіс виконує пре- та пост-процесінг запиту згідно з наборами правил, що визначає адміністратор системи управління ідентифікацією та доступом.

Фрагмент коду реалізації сервісу запровадження політики безпеки наведено на рисунку 2.13.

```
export class PolicyServiceImpl implements PolicyService {
  public constructor(
    private readonly enforcer: PolicyEnforcer,
    private readonly objectStorage: ObjectStorage,
  ) {}

  public async preCompleteLoginFlow(req: FastifyRequest): Promise<void> {
    const policy = await this.objectStorage.preCompleteLoginFlowPolicy();

    const validate = this.enforcer.compile(policy);
    if (!validate(req)) {
      throw new PreCompleteLoginFlowError();
    }
  }

  public async postCompleteLoginFlow(res: FastifyResponse): Promise<void> {
    const policy = await this.objectStorage.postCompleteLoginFlowPolicy();

    const validate = this.enforcer.compile(policy);
    if (!validate(res)) {
      throw new PostCompleteLoginFlowError();
    }
  }
}
```

Рисунок 2.13 – Фрагмент коду реалізації сервісу запровадження політики безпеки

Правила зберігаються у сховищі даних політики безпеки у вигляді JSON файлів.

Фрагмент коду реалізації файлу політики безпеки наведено на рисунку 2.14.

```
{
   "version":"2021-11-10",
   "statement":{
      "sid":"show_hide_header",
      "effect":"hide",
      "actions":[
         "headers:hide_header"
      ],
      "resource":"request",
      "conditions":[
         {
            "string_equals":{
               "headers":"x-origin-id"
            }
         }
      ]
   }
}
```

Рисунок 2.14 – Фрагмент коду реалізації файлу політики безпеки

Після проходження через сервіс запровадження політики безпеки, запит користувача потрапляє до сервісу ідентифікації та автентифікації, який виконає його обробку, при необхідності звертаючись до сервісу адаптивної автентифікації.

Фрагмент коду реалізації сервісу автентифікації наведено на рисунку 2.15.

```
export class AuthServiceImpl implements AuthService {
  public constructor(
    private readonly flowsRepository: FlowsRepository,
    private readonly identitiesRepository: IdentitiesRepository,
    private readonly adaptiveAuthService: AdaptiveAuthService,
  ) {}

  public async completeLoginFlow(req: FastifyRequest): Promise<LoginFlow> {
    const flowData = await this.flowsRepository.getFlow(req.query.flow);

    const flowContext = await this.identitiesRepository.createContext(flowData);

    const authMethod = await this.adaptiveAuthService.getAuthMethod({
      ...flowContext,
      ...req,
    });

    return {
      ...flowContext,
      method: authMethod,
    };
  }
}
```

Рисунок 2.15 – Фрагмент коду реалізації сервісу автентифікації

Сервіс адаптивної автентифікації, у свою чергу, виконую обробку контексту запиту згідно із зазначеним алгоритмом.

Фрагмент коду реалізації сервісу адаптивної автентифікації наведено на рисунку 2.16.

```
export class AdaptiveAuthServiceImpl implements AdaptiveAuthService {
  public constructor(
    private readonly devicesRepository: DevicesRepository,
    private readonly identitiesRepository: IdentitiesRepository,
  ) {}

  public async getAuthMethod(ctx: FlowContext): Promise<AuthMethod> {
    const deviceFingerprint = this.devicesRepository.getDeviceFingerprint(ctx);
    const deviceAlreadyUsed = await this.devicesRepository.checkIfUsed(
      deviceFingerprint,
    );

    if (deviceAlreadyUsed) {
      await this.identitiesRepository.setColor(COLORS.RED);
      return { method: COLORS.RED };
    }

    await this.identitiesRepository.checkLastSession(ctx);
    await this.identitiesRepository.checkCurrentSession(ctx);
    await this.identitiesRepository.checkLocation(ctx);

    const method = this.getColor(ctx);
    await this.identitiesRepository.setColor(method);

    return { method };
  }

  private getColor = (ctx: FlowContext) => {
    switch (ctx.currentColor) {
      case COLORS.GREEN:
        return COLORS.GREEN;
      case COLORS.YELLOW:
        return COLORS.GREEN;
      case COLORS.RED:
        return COLORS.YELLOW;
    }
  };
}
```

Рисунок 2.16 – Фрагмент коду реалізації сервісу адаптивної автентифікації

2.10 Висновки спеціальної частини

У спеціальній частині наведено вимоги до системи управління ідентифікацією та доступом, та функціональні послуги до них згідно з НД ТЗІ 2.5-004. Для їх тестування розроблено та наведено основні пункти програми випробувань згідно з НД ТЗІ 2.7-009-09.

На основі наведених вимог виконано розробку модулю адаптивної автентифікації та обґрунтування функціональної схеми СУІД та вибору технологій системи.

Отримані результати були використані для розробки програмної реалізації системи управління ідентифікацією та доступом з модулем адаптивної автентифікації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

Мета економічного розділу – техніко-економічний аналіз ефективності та обґрунтування доцільності створення КЗЗ – системи управління ідентифікацією та доступом з модулем адаптивної автентифікації.

Економічно доцільним слід вважати, якщо витрати на створення КЗЗ не перевищують збитків від реалізації загрози порушення безпеки.

3.2 Визначення витрат на створення КЗЗ

По-перше, необхідно визначити трудомісткість створення комплексу засобів захисту.

Трудомісткість створення КЗЗ визначається тривалістю виконання кожної операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{\text{тз}} + t_{\text{вт}} + t_{\text{ад}} + t_{\text{мд}} + t_{\text{к}} + t_{\text{тп}} + t_{\text{д}} \quad \text{годин}, \qquad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на створення КЗЗ;

$t_{\text{вт}}$ – тривалість вибору технологій, що використовуються в КЗЗ;

$t_{\text{ад}}$– тривалість аналізу документації до обраних технологій;

$t_{\text{мд}}$– тривалість створення моделі даних;

$t_{\text{к}}$– тривалість створення кодової бази КЗЗ;

$t_{\text{тп}}$– тривалість тестування функціональних послуг;

$t_{\text{д}}$– тривалість документального оформлення.

Таким чином трудомісткість створення КЗЗ дорівнює:

$$t = 8 + 8 + 16 + 16 + 100 + 16 + 16$$

$$t = 180 \text{ год.}$$

Розрахуємо витрати на створення КЗЗ. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн,} \qquad (3.2)$$

де $K_{рп}$ – витрати на створення КЗЗ;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення КЗЗ.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб}, \text{ грн,} \qquad (3.3)$$

де t – загальна тривалість створення КЗЗ, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 120 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 180 \text{ год} \cdot 120 \text{ грн/год,}$$

$$З_{зп} = 21600 \text{ грн.}$$

Витрати машинного часу визначаються за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \text{ грн,} \qquad (3.4)$$

де t – трудомісткість створення КЗЗ на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{ грн,} \qquad (3.5)$$

де P – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$С_{мч} = 0{,}5 \cdot 1 \cdot 1{,}68 + (7100*0{,}3)/1920 + (1500*0{,}1)/1920 \text{ грн,}$$

$$С_{мч} = 2{,}02 \text{ грн.}$$

Отже, витрати на створення КЗЗ за формулою 3.2 становлять:

$$К_{рп} = 21939{,}6 \text{ грн.}$$

В результаті розрахунків, вартість створення КЗЗ становить – 21939,6 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$K = K_{рп} + K_{аз} \text{ грн}, \quad (3.6)$$

де $К_{рп}$ – вартість створення КЗЗ, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення, тис. грн.

Необхідно придбати наступне апаратне забезпечення:

- сервер HP DP360p G8 (9000 грн)

Відповідно до цього, вартість апаратного забезпечення становить 9000 грн.

Таким чином, згідно з формулою 3.6:

$$K = 21939,6 + 9000 = 30963,6 \text{ грн.}$$

3.3 Розрахунок експлуатаційних витрат

Річні поточні витрати на функціонування КЗЗ розраховуються за формулою 3.7:

$$C = C_в + C_к + C_{ак} \text{ грн}, \quad (3.7)$$

де $C_в$ – вартість оновлення та модернізації системи ($C_в$ = 1500 грн.);

$C_к$ – витрати на керування системою в цілому;

$C_{ак}$ – витрати, викликані активністю користувачів ($C_{ак}$ = 8000 грн.).

Витрати на керування КЗЗ розраховується за формулою 3.8:

$$C_к = C_н + C_а + C_з + C_{св} + C_{ел} + C_о + C_{тос} \text{ грн}, \quad (3.8)$$

Витрати на навчання персоналу та користувачів складають $C_н$ = 0 грн.

Річний фонд амортизаційних відрахувань становить з урахуванням терміну експлуатації серверу у 8 років складає $С_а$ = 9000 / 8 = 1125 грн.

Річний фонд заробітної плати інженерно-технічного персоналу:

$$С_з = З_{осн} + З_{дод} \text{ грн}, \quad (3.9)$$

Основна заробітна плата одного спеціаліста з інформаційної безпеки складає 19200 грн на місяць. Додаткова заробітна плата – 10% від основної. Виконання роботи щодо налаштування КЗЗ потребує залучення спеціаліста на 0,5 ставки.

Отже, за формулою 3.9:

$$С_з = (19200*12 + 19200*12*0,1)*0,5 = 126720 \text{ грн.}$$

Ставка ЄСВ складає 22%:

$$С_{єв} = 126720 * 0,22 = 27878,4 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою, розраховується за формулою 3.10:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ грн}, \quad (3.10)$$

де $Р$ – потужність апаратури;

$F_р$ – річний фонд робочого часу;

$Ц_е$ – тариф на електроенергію.

Отже, за формулою 3.10:

$$С_{ел} = 0,8 * 8760 * 1,68 = 11773,44 \text{ грн.}$$

Витрати на залучення сторонніх організацій становлять 0 грн.

Витрати на адміністрування та сервіс становлять 2% від вартості капітальних витрат:

$$C_{тос} = 30963,6 * 0,02 = 619,27 \text{ грн.}$$

Витрати на керування КЗЗ за формулою 3.8:

$$C_к = 0 + 1125 + 126720 + 27878,4 + 11773,44 + 0 + 619,27$$
$$C_к = 168116,11 \text{ грн.}$$

Річні поточні витрати за формулою 3.7:

$$C = 1500 + 168116,11 + 8000$$
$$C = 177616,11 \text{ грн.}$$

3.4 Оцінка величини збитку у разі реалізації загроз

Мета оцінки – визначення обсягів матеріальних збитків, що розраховуються виходячи з ймовірності реалізації загрози та можливих матеріальних втрат від неї.

Упущена вигода розраховується за формулою 3.11:

$$U = П_п + П_в + V \text{ грн,} \qquad (3.11)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників, грн;

$П_в$ – вартість відновлення працездатності (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ і V, використовуються формули 3.12, 3.13, 3.14 відповідно:

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п \text{ грн}, \quad (3.12)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн}, \quad (3.13)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \text{ грн}, \quad (3.14)$$

де $F_г$ – річний фонд часу роботи організації;

$О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.15 і 3.16 відповідно:

$$П_{ви} = \frac{\sum Зс \cdot Чс}{F} \cdot t_{ви} \text{ грн,} \qquad (3.15)$$

де F – місячний фонд робочого часу;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$Ч_с$ – чисельність співробітників атакованого вузла.

$$П_{пв} = \frac{\sum Зо \cdot Чо}{F} \cdot t_в \text{ грн,} \qquad (3.16)$$

де F – місячний фонд робочого часу;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$Чо$ – чисельність обслуговуючого персоналу.

Вихідні дані для розрахунків наведені у таблиці 3.1:

Таблиця 3.1 – Вихідні дані для розрахунку збитків від реалізації загроз:

Умовні позначення	Величина
$t_п$	8 год
$t_в$	3 год
$t_{ви}$	6 год
$З_о$	19200 грн
$З_с$	15000 грн
$Ч_о$	1 особи
$Ч_с$	8 осіб
$О$	1500000 грн
$П_{зч}$	2000 грн
I	1 шт
N	15 шт
F	176 год
$F_г$	2080 год

Результати розрахунків наведено у таблиці 3.2.

Таблиця 3.2 – Результати розрахунків збитків від реалізації загроз:

Умовні позначення	Результат, грн
$П_п$	5454,54
$П_{ви}$	4090,9
$П_{пв}$	872,72
$П_в$	6963,62
V	12259,6
U	24677,76

Загальний збиток атаки на вузол розраховується за формулою 3.17:

$$B = \sum i \times \sum n \times U \quad (3.17)$$

Таким чином, загальний збиток дорівнює:

$$B = 1 * 15 * 24677,76 = 370166,4 \text{ грн.}$$

3.5 Загальний ефект від впровадження КЗЗ

Загальний ефект впровадження КЗЗ визначається з урахуванням ризиків порушення інформаційної безпеки за формуло 3.18:

$$E = B \cdot R - C \text{ грн,} \quad (3.18)$$

де В – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Економічний ефект становить:

$$E = 370166,4 * 0,6 - 177616,11 = 44483,73 \text{ грн.}$$

3.6 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки додаткового прибутку приносить одна одиниця капітальних інвестицій. Розраховується за формулою 3.19:

$$ROSI = E / K, \quad (3.19)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Таким чином:

$$ROSI = 1{,}436$$

Проект вважається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції. Розраховується за формулою 3.20:

$$ROSI > (N_{деп} - N_{інф}) / 100 \quad (3.20)$$

де $N_{деп} = 10{,}24$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф} = 9{,}6$ – річний рівень інфляції, %.

Оскільки 1,436 > 0,0064, проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.21:

$$T_o = K / E = 1 / ROSI \quad (3.21)$$

Маємо:

$$T_o = 0{,}7 \text{ року.}$$

3.7 Висновки економічного розділу

У цьому розділі були проведені розрахунки:

– Капітальних витрат на створення КЗЗ (30963,6 грн);

– Річних поточних витрат (177616,11 грн).

– Економічного ефекту (44483,73 грн);

– Коефіцієнту ефективності, який перевищує річний рівень прибутковості альтернативного варіанта (1,436 > 0,0064);

– Терміну окупності капітальних інвестицій (0,7 року).

Отже, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи описано актуальність питання, системи управління ідентифікацією та доступом. Проаналізовано та порівняно існуючі системи управління ідентифікацією та доступом.

Таким чином визначено доцільність створення КЗЗ для захисту інформації в інформаційно-телекомунікаційних системах малого бізнесу.

У спеціальній частині наведено основні вимоги до СУІД та послуги безпеки до цих вимог. На базі цих вимог розроблено модуль адаптивної автентифікації та обґрунтовано вибір технологій системи управління ідентифікацією та доступом .

Для отриманих результатів розроблено основні пункти випробувань послуг безпеки відповідно до НД ТЗІ 2.7-009-99.

В третьому розділі було проведено розрахунки капітальних та річних витрат на КЗЗ. В ході розрахунків з'ясовано, що створення КЗЗ вигідне.

Отже, створення КЗЗ повністю доцільне та сприяє підвищенню рівню захисту інформації в інформаційно-телекомунікаційних системах малого бізнесу.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf.

2. Worldwide security spending in the identity access management segment from 2017 to 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.statista.com/statistics/417602/global-market-forecast-identity-and-access-management/.

3. Global Identity and Access Management Market (2021 to 2026) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.businesswire.com/news/home/20211027005721/en/Global-Identity-and-Access-Management-Market-2021-to-2026---Featuring-Centrify-Microsoft-and-Micro-Focus-Among-Others---ResearchAndMarkets.com.

4. 2019 Data Breach Investigations Report [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf.

5. 30 Surprising Small Business Cyber Security Statistics (2021) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.fundera.com/resources/small-business-cyber-security-statistics.

6. The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.

7. 2016 Data Breach Investigations Report [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf.

8. НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf.

9. НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-002-99.pdf.

10. Best Identity and Access Management (IAM) Solutions [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.esecurityplanet.com/products/best-iam-software/.

11. What is Okta? [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://support.okta.com/help/s/article/What-is-Okta?language=en_US.

12. What is OpenIAM? [Електронний ресурс] – Режим доступу до ресурсу: https://docs.openiam.com/docs-4.2.0.8/getting-started/1-what_is_openiam.

13. Auth0 Overview [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/get-started/auth0-overview.

14. Ory Kratos, Introduction [Електронний ресурс] – Режим доступу до ресурсу: https://www.ory.sh/kratos/docs/#:~:text=Ory%20Kratos%20is%20an%20API,application%20needs%20to%20deal%20with%3A&text=Admin%20APIs%3A%20Import%2C%20update%2C%20delete%20identities.

15. Open Source Identity and Access Management [Електронний ресурс] – Режим доступу до ресурсу: https://www.keycloak.org/.

16. Security camera hack exposes hospitals, workplaces, schools [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://abcnews.go.com/Technology/wireStory/security-camera-hack-exposes-hospitals-workplaces-schools-76371080.

17. Incident Report - DNS Outage due to DDoS Attack (June 3rd, 2013) [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://blog.dnsimple.com/2013/06/incident-report-20130603/.

18. CVE-2020-5263 Detail [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/detail/CVE-2020-5263.

19. CVE-2021-32641 Detail [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/detail/CVE-2021-32641.

20. CVE-2021-28113 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-28113.

21. Chubb Cyber Risk Survey 2019 Executive Summary [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.chubb.com/content/dam/aem-chubb-global/static-pages/online-you-protected-default/pdf/Chubb_Cyber_Survey.pdf.

22. МОДЕЛИ АУТЕНИФИКАЦИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ ДЛЯ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ С ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКОЙ ВЫБОРА [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://doklady.bsuir.by/jour/article/view/836/836.

23. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення [Електронний ресурс]. – 1993. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=61937.

24. SQL Injection Prevention Cheat Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html.

25. НД ТЗІ 2.7 -009-09 "Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.7-009-09.pdf.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	13	
6	А4	2 Розділ	29	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	
14	А4	Додаток Д	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ДИПЛОМ_ГерасимовМО_125м-20-2.docx

ПРЕЗЕНТАЦІЯ_ГерасимовМО_125м-20-2.docx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника
на кваліфікаційну роботу магістра на тему:

«Адаптивна автентифікація в системах ідентифікації та контролю доступу розподілених інформаційно-телекомунікаційних систем малого бізнесу»

студента групи 125м-20-2

Герасимова Максима Олеговича

Мета роботи – забезпечення достатнього рівня надійності та лояльності автентифікації клієнтів в інформаційно-телекомунікаційних системах малого бізнесу.

Тема роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток та розробка засобів інформаційної безпеки та/або кібербезпеки інформаційно-телекомунікаційних систем.

Задачі роботи (обґрунтування актуальності роботи, класифікація та аналіз систем управління ідентифікацією та доступом (СУІД), формалізація вимог до розробки, обґрунтування вибору моделі автентифікації, розробка алгоритму роботи модулю адаптивної автентифікації, обґрунтування функціональної схеми СУІД та мови програмування для її реалізації, розробка фрагментів програмної реалізації та основних пунктів випробувань) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність технічних рішень полягає у запропонованих алгоритмах модулю адаптивної автентифікації.

Практичне значення результатів проектування полягає в розробці програмної реалізації основних елементів системи.

До недоліків кваліфікаційної роботи відносяться:

– незначні неточності при описі послуг безпеки;
– недостатньо обґрунтовано вибір методу автентифікації;
– недостатньо обґрунтовано значення критеріїв оцінки рівня довіри;

– узагальнене представлення пунктів методики випробування;

– відсутність практичної перевірки ефективності запропонованих рішень.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з деякими відхиленнями від стандартів.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог положення про систему виявлення та запобіганню плагіату.

Ступінь самостійності виконання кваліфікаційної роботи висока.

За час дипломування Герасимов М.О. виявив себе фахівцем, здатним самостійно, на достатньо високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “відмінно”, а Герасимов М.О. присвоєння йому кваліфікації магістр з кібербезпеки, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини,
старший викладач _____ Олександр КРУЧІНІН

Керівник роботи,
д.т.н., професор _____ Валерій КОРНІЄНКО

ДОДАТОК Д. Структурна схема типової СУІД