ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ CYBER SURVEILLANCE ЗА ДОПОМОГОЮ ІАМ»

Виконав студент 4 курсу, групи БСД-43
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Мишко А.А
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Мишку Андрію Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо виявлення та запобігання Cyber Surveillance за допомогою IAM»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмний комплекс Keycloak;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Вступ
2. Аналіз загроз Cyber Surveillance
1.1 Аналіз актуальності та проблематики Cyber Surveillance
1.2 Поняття та різновиди Cyber Surveillance

2. Дослідження методів виявлення та запобігання Cyber Surveillance

2.1 Методи виявлення та запобігання Cyber Surveillance

2.2 Порівняння IAM-систем для виявлення та запобігання Cyber Surveillance

2.3 IAM Keycloak

3. Розробка рекомендацій щодо виявлення та запобігання Cyber Surveillance за допомогою IAM

3.1 Дослідження технічних можливостей Keycloak для виявлення та запобігання Cyber Surveillance

3.2 Розгортання та налаштування IAM та реагування на загрозу

3.3 Розробка рекомендацій щодо використання Keycloak для виявлення та запобігання Cyber Surveillance

4. Висновки

5. Перелік графічного матеріалу

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми Cyber Surveillance.	24.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	25.02.2023 р.	
3.	Аналіз методів та засобів захисту від Cyber Surveillance	4.03.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту від Cyber Surveillance.	15.03.2023 р.	
5.	Оформлення результатів дослідження.	22.05.2023 р.	
6.	Підготовка доповіді до захисту.	28.05.2023 р.	

Студент _____ Мишко А.А.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Мишка Андрія Андрійовича
на тему: «Дослідження шляхів та розробка рекомендацій щодо виявлення та запобігання Cyber Surveillance за допомогою IAM»

Актуальність: Зростаюча кількість кіберзагроз, включаючи шпигунство та незаконне збирання інформації, ставить під загрозу безпеку як індивідуальних користувачів, так і організацій.

Зловмисники постійно вдосконалюють свої методи та технології для отримання незаконного доступу до конфіденційної інформації. Тому необхідно розробляти та застосовувати ефективні рекомендації та заходи безпеки для виявлення та запобігання кібершпигунству.

Позитивні сторони:

1. На основі проведеного аналізу в роботі був розроблений комплекс рекомендацій щодо виявлення та запобігання Cyber Surveillance.
2. Було досліджено методи виявлення та запобігання Cyber Surveillance на прикладі програмного рішення IAM Keycloak.
3. Текст відображає достатню мовну грамотність та послідовність. Висновки сформульовані чітко й змістовно. Графічний матеріал презентований високою якістю. Перелік науково-технічної літератури свідчить про вміння користуватись джерелами, що стосуються теми бакалаврської роботи.

Недоліки:

1. У бакалаврській роботі бажано було б описати можливі інтеграції програмного рішення Keycloak з іншими системами для покращення безпеки.
2. Зважаючи на широкий спектр проблематики Cyber Surveillance, дослідження може не охопити всі аспекти та потенційні варіації загроз, що можуть виникнути у контексті Cyber Surveillance.
3. Враховуючи широкий спектр можливостей та модулів, які пропонує Keycloak, дослідження може бути обмежене в аналізі та описі певних функцій, що присутні в цій системі.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку добре, а студент Мишко А.А. – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект—частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Мишку А.А. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
Освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо виявлення та Запобігання Cyber Surveillance за допомогою IAM».
Бакалаврська робота і рецензія додаються.
Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Мишку А.А. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Мишко А.А.*** обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо виявлення та запобігання Cyber Surveillance за допомогою IAM. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Мишко А.А. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Мишка Андрія Андрійовича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Мишко А.А.
(прізвище та ініціали)
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 72 сторінок, 31 рисунок, 12 джерел.

Об’єкт дослідження – загрози кібер безпеки Cyber Surveillance.

Предмет дослідження – IAM Keycloak та її вплив на протидію загрозам Cyber Surveillance.

Мета роботи – розробити рекомендації щодо виявлення та запобігання загрозам Cyber Surveillance.

Методи дослідження – опрацювання літератури, аналіз експлуатаційної документації, проведення порівнянь.

В роботі приведено основні відомості про загрози Cyber Surveillance, загрози інформаційній безпеці та кіберзлочини.

Проаналізовано різні види загроз Cyber Surveillance. Досліджено методи та засоби виявлення та запобігання загрозам Cyber Surveillance.

Досліджено можливості програмного комплексу IAM Keycloak в боротьбі з загрозами Cyber Surveillance.

На основі досліджень проведених в роботі розроблено рекомендації щодо виявлення та запобігання загрозам Cyber Surveillance за допомогою IAM Keycloak.

Галузь використання – кібербезпека корпоративних інформаційних систем.

Ключові слова: ІНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗИ, КІБЕРБЕЗПЕКА, ЗАХИСТ СИСТЕМ, КІБЕРІНЦИДЕНТ, КІБЕР-ЗЛОЧИН, МЕТОДИ ТА ЗАСОБИ ЗАПОБІГАННЯ CYBER SURVEILLANCE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ — Програмне забезпечення

ІС — Інформаційна система

ELS — Системи реєстрації подій (Event Logging Systems)

IDS — Система виявлення вторгнень (Intrusion Detection Systems)

IAM — Системи контролю доступу (Identity and access management system)

SAML — Security assertion markup language

OAuth — протокол авторизації

APP — Application

ВСТУП

Актуальність роботи. Сьогодні, в умовах розвитку технологій та інтернет-технологій, зростає кількість кібератак на користувачів та компанії. Кібератаки стають все більш витонченими та складними, а також є загрозою не лише для окремих користувачів, але й для сектору бізнесу та цілих держав. Однією з таких загроз є Cyber Surveillance – збір та моніторинг електронних даних користувачів без їх згоди. Це може бути здійснене різними способами, включаючи перехоплення трафіку, використання шпигунського програмного забезпечення та інші методи. Таким чином, захист від таких атак є важливим завданням, яке потребує розробки нових методів та підходів.

Враховуючи те, що кожна людина має свої права на конфіденційність та приватність, та що бізнес та урядові організації мають обов'язок захищати конфіденційність своїх клієнтів та громадян, виявлення та запобігання Cyber Surveillance є дуже важливим завданням для багатьох організацій та користувачів. Крім того, у бізнесі та в урядових організаціях, де інформація є ключовим активом, відсутність ефективних засобів захисту може призвести до значних втрат та пошкоджень.

Тому, дослідження Cyber Surveillance та розробка методів щодо виявлення та запобігання цій загрозі є актуальним завданням, яке допоможе забезпечити захист від кібератак та зберегти конфіденційність і приватність користувачів та організацій.

Об'єкт дослідження даної дипломної роботи є Cyber Surveillance.

Предмет дослідження даної дипломної роботи є IAM Keycloak як інструмент для запобігання загрозам Cyber Surveillance.

Мета роботи полягає у проведенні дослідження, спрямованого на виявлення та запобігання кібернагляду, який є нагальною проблемою сучасного світу.

Основні завдання дослідження включають аналіз понять Cyber Surveillance та управління ідентифікацією та доступом (IAM).

Одним з головних завдань є визначення потенційних загроз, пов'язаних з Cyber Surveillance. Дослідження також передбачає докладний аналіз технічних можливостей Keycloak для виявлення та запобігання вразливостям та загрозам кібернагляду. Крім того, будуть розроблені рекомендації щодо використання системи управління ідентифікацією та доступом (IAM) Keycloak для виявлення та запобігання кібернагляду.

Основне завдання дослідження це розробка конкретних рекомендацій щодо використання системи управління ідентифікацією та доступом (IAM) Keycloak для виявлення та запобігання кібернагляду, а також визначення практичної значущості отриманих результатів. Крім цього, на основі рекомендацій будуть сформульовані напрямки для подальших досліджень, які можуть включати більш детальний аналіз методів виявлення та запобігання кібернагляду, розгляд інших інструментів, що можуть бути використані для цієї цілі, а також вивчення нових загроз у галузі кібербезпеки.

Методи дослідження включають в себе: аналіз літературних джерел та інтернет ресурсів, використання методів тестування та експерименту, також будуть використовуватись інші методи, наприклад, інтервіювання експертів з питань інформаційної безпеки.

Практичне значення одержаних результатів дослідження полягає у покращенні кібербезпеки шляхом виявлення та запобігання Cyber Surveillance, оптимізації використання IAM Keycloak та сприянні співпраці та обміну знаннями у цій галузі.

1 АНАЛІЗ ЗАГРОЗ CYBER SURVEILLANCE

1.1 Аналіз актуальності та проблематики Cyber Surveillance

У сучасному цифровому світі, де інформаційні технології використовуються масово, Cyber Surveillance стає актуальною та важливою проблемою. Ця проблематика постійно зростає і стикається з новими викликами, що вимагає постійного аналізу та пошуку рішень.

Одним з основних аспектів актуальності Cyber Surveillance є збільшення кількості та складності кібератак, що спрямовані на незаконне збирання, моніторинг та використання цифрової інформації користувачів. Зловмисники використовують різні методи та інструменти для здійснення таких атак, включаючи вторгнення в приватне життя, крадіжку ідентифікаційних даних та масовий нагляд [1].

Ці проблеми мають серйозні наслідки для індивідів, підприємств, установ та держав. Крадіжка особистих даних може призвести до ідентифікаційної крадіжки, фінансових втрат та порушення приватності. Масовий нагляд порушує основні права на конфіденційність та свободу вираження. Вторгнення в приватне життя та соціальна інженерія створюють загрозу для особистої безпеки та довіри до цифрових сервісів.

Розвиток технологій, таких як штучний інтелект, Big Data та Інтернет речей, додатково підсилює проблематику Cyber Surveillance. За допомогою цих технологій можна збирати, аналізувати та використовувати великі обсяги даних про користувачів з метою контролю та маніпулювання.

Тому дана проблема є своєчасною та актуальною на даний момент і вона потребує нових досліджень.

1.2 Поняття та різновиди Cyber Surveillance

Поняття Cyber Surveillance означає кібернетичне спостереження або кібернетичний нагляд. Це процес збору, моніторингу та аналізу цифрової інформації про індивідів, організації або системи з метою отримання конфіденційної, приватної і особистої інформації без їхнього дозволу або свідомості.

Ця загроза є серйозною, оскільки Cyber Surveillance може мати широкий спектр негативних наслідків. Перш за все, це порушення приватності та конфіденційності. Індивіди та організації мають право на захист своєї особистої інформації, але збір та моніторинг їхніх цифрових даних без їхньої згоди порушує це право. Крім того, Cyber Surveillance може призвести до витоку конфіденційної інформації, яка може бути використана для шахрайства, шпигунства, шантажу або інших злочинних дій.

Принцип використання Cyber Surveillance полягає в тому, що зловмисники або організації використовують різні технології та методи, (які буде описано більш детально в наступному розділі), такі як шпигунське програмне забезпечення, віруси, троянські програми, шпигунські пристрої або вразливості в мережах та системах безпеки для здійснення Cyber Surveillance, тобто для непомітного збору необхідної їм інформації. Вони можуть перехоплювати повідомлення, записувати клавіші, слідкувати за активністю в мережі та багато іншого [2].

Cyber Surveillance також має великий вплив на сучасний світ в багатьох сферах. Cyber Surveillance росте і розвивається разом з невгасаючим темпом розвитку технологій. Cyber Surveillance наразі використовується майже для всього і майже усюди: від кафе, ресторанів, кінотеатрів, маленьких організацій, тощо, до багато мільярдних корпорацій та цілих держав!

Випадки використання Cyber Surveillance можуть бути різноманітними як законними так і ні, як тими, що приносять користь так і навпаки. Наразі поняття

Cyber Surveillance здебільшого пов’язане зі злочинною, неправомірною, або прихованою діяльністю, яка здійснює злочин проти конфіденційності та

приватності, але Cyber Surveillance це не завжди незаконно та не завжди погано.

Навпаки, деякі активності Cyber Surveillance мають цілком легальні підстави в окремих випадках та контексті та загалом приносять користь: наприклад уряди та розвідувальні агентства можуть здійснювати Cyber Surveillance для забезпечення національної безпеки, протидії тероризму або боротьби зі злочинністю. Вони можуть моніторити комунікації, перехоплювати повідомлення або аналізувати цифрові сліди злочинців. Корпорації можуть використовувати Cyber Surveillance для контролю за діяльністю своїх співробітників, захисту своєї інтелектуальної власності або виявлення зловживань. Але й є інша сторона Cyber Surveillance: уряди та розвідувальні агентства можуть використовувати Cyber Surveillance для збору розвідувальної інформації про інші країни або політичних опонентів, або переслідування політичних дисидентів, пропаганди, тощо. Корпорації можуть застосовувати Cyber Surveillance для здійснення шпигунства на своїх конкурентів або для збору та продажу комерційної інформації. Кіберзлочинці використовують методи Cyber Surveillance для отримання фінансової вигоди, шахрайства, шпигунства або шантажування, копіювання ідентичності, тощо.

В сучасному світі вже було виявлено багато випадків не дуже законного використання та зловживання Cyber Surveillance. Наприклад, у 2013 році відомий випадок Едварда Сноудена, коли він розкрив інформацію про широкомасштабну программу кібер-шпигування американської National Security Agency (NSA). Цей випадок привернув увагу глобальної спільноти до проблеми масового моніторингу та його впливу на приватність громадян [3].

Також були випадки, коли компанії, такі як Facebook та Google, були звинувачені у зборі та використанні особистих даних користувачів для цілей реклами та персоналізованого спостереження. Ці випадки породили обговорення про прозорість та контроль за збором та використанням цифрових даних користувачів.

Крім того, деякі країни, такі як Китай, відомі своїми широкомасштабними системами Cyber Surveillance, які включають в себе відеоспостереження,

моніторинг інтернет-активності та соціальних мереж, а також використання систем розпізнавання облич та інших технологій для статистичного контролю громадян.

Cyber Surveillance - це серйозна загроза, яка все тісніше переплітається з повсякденним життям, впливаючи на приватність, безпеку та довіру в цифровому світі.

Серед актуальних загроз Cyber Surveillance найпоширенішими є:

1. Відстеження даних
2. Вторгнення в приватне життя
3. Масовий нагляд
4. Цензура та обмеження доступу
5. Соціальна інженерія
6. Крадіжка ідентифікаційних даних

Відстеження даних.

Ця загроза передбачає збір і аналіз особисто ідентифікованої інформації про користувачів з метою виявлення їхніх звичок, здібностей, зв'язків та інших характеристик. Ці дані можуть включати особисті дані, фінансові дані, місцезнаходження, комунікації та багато іншого.

Процес відстеження даних починається зі збору інформації. Це може включати використання різноманітних методів, таких як кукі, пікселі відстеження, IP-адреси, соціальні мережі, аналітичні інструменти та багато інших. Зібрані дані потім аналізуються і профілюються для створення повного образу користувача, включаючи його інтереси, звички, покупки, переглянуті сторінки, місцезнаходження та інше.

Ця інформація може використовуватись для різних цілей, включаючи націлений маркетинг, персоналізацію послуг, розробку стратегій продажу, аналіз поведінки користувачів та іншого. Однак, в контексті кібер-спостереження, відстеження даних може мати негативні наслідки.

Перш за все, відстеження даних порушує приватність користувачів, оскільки їхні особисті дані збираються без їхнього належного інформування та згоди. Це

може призвести до незаконного доступу до конфіденційної інформації та порушення особистих прав користувачів.

Крім того, відстеження даних може стати основою для розкриття конфіденційної інформації та зловживання несанкціонованим доступом до особистих даних. Ця інформація може потрапити у руки зловмисників або бути використана з метою шантажу, маніпуляції або ідентифікаційної крадіжки.

Оскільки відстеження даних може стати масовою практикою, воно також може мати вплив на демократію, свободу вираження та права людини. Масовий збір і аналіз особистих даних можуть використовуватись для створення профілів груп користувачів та контролю їхньої діяльності, що може обмежити свободу слова та впливати на політичну або соціальну активність.

Вторгнення в приватне життя [1-3].

Ця загроза передбачає можливість стежити за особистими діями та звичками користувачів з метою збору інформації про їхню приватну сферу. В контексті кібер-спостереження, вторгнення в приватне життя може мати негативні наслідки та порушити особистість користувачів.

Процес вторгнення в приватне життя починається зі збору різноманітної інформації про користувачів. Це включає моніторинг активності в Інтернеті, перегляд веб-сторінок, використання соціальних мереж, комунікацію та інші дії. Зібрана інформація потім профілюється для отримання детального образу користувачів, їхніх інтересів, звичок, зв'язків та приватних вподобань.

Вторгнення в приватне життя є порушення приватності користувачів. Збір особисто ідентифікованої інформації без належного інформування та згоди користувачів може призвести до незаконного збирання та використання їхніх особистих даних. Це порушує основні принципи приватності та може спричинити витік конфіденційної інформації.

Вторгнення в приватне життя може мати негативні наслідки для користувачів. Інформація, яка збирається про їхню приватну сферу, може бути використана з метою шантажу, маніпуляції або навіть шкоди їхнім особистим та

професійним життям. Користувачі можуть втратити довіру, відчувати страх або стати жертвами кіберзлочинів через розкриття їхньої приватної інформації.

Масовий нагляд.

Ця загроза передбачає можливість здійснювати нагляд за великою кількістю осіб або груп і збирати їхню особисту інформацію без їхньої згоди чи попередження. Масовий нагляд може порушувати принципи демократії, свободи вираження та прав людини.

Механізми масового нагляду включає моніторинг комунікацій, збір і аналіз метаданих, перехоплення повідомлень, відслідковування місцезнаходження та використання різноманітних технологій для збору інформації. Це може бути реалізовано через використання спеціального програмного забезпечення, апаратних засобів або залучення зовнішніх ресурсів.

Масовий нагляд має серйозні наслідки для осіб, які піддаються спостереженню. Це може призвести до страху, самоцензури, обмеження свободи вираження і прав людини. Зібрана інформація може використовуватися для маніпуляції, шантажу або навіть для проведення кіберзлочинів.

Одним із способів запобігання масовому нагляду є використання захисних технологій та механізмів приватності. Keycloak, як система керування ідентифікацією та автентифікацією, надає деякі технічні можливості для захисту приватності користувачів. Наприклад, вона підтримує шифрування даних, аутентифікацію з двофакторною перевіркою, керування доступом та аудиторські журнали для виявлення підозрілих активностей [4].

Цензура та обмеження доступу.

Ця загроза полягає в контролі та обмеженні доступу користувачів до певної інформації або ресурсів. Це може бути реалізовано через блокування веб-сайтів, фільтрацію контенту, обмеження доступу до певних послуг або встановлення обмежень на використання інтернету.

Механізми цензури та обмеження доступу можуть включати фільтри мережевого рівня, блек лістинг доменних імен, URL-фільтри, системи блокування

контенту та інші технології контролю доступу. Ці механізми можуть застосовуватися на рівні мережі, веб-сайту, оператора мережі або навіть державного рівня.

Цензура та обмеження доступу можуть мати серйозні наслідки для свободи слова, інформаційної вільності та прав людини. Вони можуть призводити до обмеження доступу до інформації, зниження рівня свободи вираження, зменшення рівня приватності та порушення прав людини на інформацію.

Соціальна інженерія.

Соціальна інженерія використовується для збирання інформації про користувачів з метою маніпулювання ними або впливу на їхні дії. Ця загроза базується на використанні психологічних методів та маніпуляційних технік з метою отримання конфіденційної інформації або зловживання довірою користувачів.

Соціальна інженерія може включати такі методи, як фішинг, шантаж, маніпуляцію психологічним станом користувачів, використання соціальних мереж для збору інформації тощо. Зловмисники можуть встановлювати підроблені веб-сайти або надсилати шкідливі електронні листи з метою отримання логінів, паролів або інших конфіденційних даних.

Висновок до розділу 1

У цьому розділі було детально розглянуто поняття та різновиди Cyber Surveillance. Було з'ясовано, що Cyber Surveillance означає незаконне збирання, моніторинг та використання цифрової інформації користувачів. З'ясувалися різні форми цього явища, включаючи електронний нагляд, соціальний інженерінг, кібершпигунство та інші.

Аналізуючи отриману інформацію, можна зробити висновок, що Cyber Surveillance є серйозною проблемою, що порушує приватність та безпеку користувачів в цифровому середовищі. Враховуючи швидкий розвиток технологій та зростання загроз кібербезпеці, важливо розробляти ефективні рекомендації та заходи для виявлення та запобігання Cyber Surveillance.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ CYBER SURVEILLANCE

2.1 Методи виявлення та запобігання Cyber Surveillance

Даний розділ описує різноманітні підходи та технології, які можуть використовуватися для виявлення та протидії Cyber Surveillance. Цей розділ представляє широкий огляд методів та інструментів, що можуть бути використані для виявлення активності Cyber Surveillance. Він охоплює як технічні аспекти, пов'язані з використанням різноманітних програмних та апаратних рішень, так і методи соціального аналізу та розуміння характеристик та мотивацій суб'єктів спостереження.

Засоби розглянуті у цьому розділі, є технічним виявленням Cyber Surveillance. Це включає в себе використання апаратних та програмних засобів для виявлення підозрілої активності, яка може бути пов'язана з Cyber Surveillance. Це може включати аналіз мережевого трафіку, виявлення вразливостей та зловживань, моніторинг системи безпеки та виявлення аномальної поведінки користувачів, тощо. Використання таких технічних методів дозволяє ранньо виявляти ймовірні загрози та забезпечувати захист від них [5].

У цьому розділі також будуть розглянуті сучасні тенденції та нові розробки в галузі виявлення Cyber Surveillance. Враховуючи постійний розвиток технологій та зміну підходів до кібернетичного спостереження, дослідження новітніх методів та інструментів стає ключовим для ефективного виявлення та захисту від цієї загрози. Програмні рішення, штучний інтелект, машинне навчання та аналітика даних є лише деякими з напрямків, які вивчаються з метою розробки ефективних методів виявлення Cyber Surveillance.

Отже, ці методи використовуються для аналізу мережевого трафіку, виявлення вразливостей, моніторингу систем безпеки та інших технічних аспектів, які можуть свідчити про наявність Cyber Surveillance.

Зараз я розгляну деякі з найбільш поширених технік та інструментів, що використовуються для цих цілей:

Серед таких засобів найбільш поширеними є:

1. Системи виявлення вторгнень (Intrusion Detection Systems, IDS)
2. Мережеві екрани (Firewall)
3. Системи моніторингу мережі
4. Системи реєстрації подій (Event Logging Systems)
5. Системи контролю доступу (Identity and access management system, IAM)

Розглянемо детальніше кожен із них:

1. Система виявлення вторгнень (Intrusion Detection System, IDS).

Система виявлення вторгнень є ефективним способом виявлення Cyber Surveillance та інших загроз безпеці мережі. Вона працює, аналізуючи мережевий трафік та шукати ознаки незвичайної або підозрілої активності.

Розглянемо детальніше, як працює Система виявлення вторгнень:

Моніторинг трафіку: IDS стежить за всіма пакетами даних, які переходять через мережу. Це включає як внутрішній, так і зовнішній трафік, що проходить через вузли мережі.

Правила виявлення: IDS використовує заздалегідь визначені правила та сигнатури для виявлення підозрілих дій. Ці правила можуть включати детектування відомих атак, незвичайні моделі поведінки, порушення заборонених дій та інші характеристики, що вказують на можливу загрозу.

Аналіз трафіку: IDS аналізує трафік залежно від правил виявлення. Це може бути базовим аналізом заголовків пакетів, зіставленням з відомими сигнатурами, створенням профілів поведінки або застосування складніших алгоритмів машинного навчання.

Виявлення та сповіщення: Якщо IDS виявляє підозрілу активність або можливий вторгнення, він сповіщає адміністратора або безпековий персонал про виниклий інцидент. Це може бути здійснено через систему сповіщень, журнали подій або інші канали зв'язку.

Реагування на інциденти: IDS може приймати певні заходи для забезпечення безпеки. Це може включати блокування джерела атаки, зміну налаштувань мережі для запобігання подібним атакам, збір додаткових доказів або сповіщення безпекових служб [6].

Переваги використання Системи виявлення вторгнень (IDS):

0 IDS дозволяє виявляти незвичайну або підозрілу активність, яка може бути пов'язана з Cyber Surveillance або іншими загрозами безпеці.

1 IDS може негайно сповістити про виявлені загрози, що дозволяє оперативно реагувати та запобігати подальшому пошкодженню або компрометації системи.

2 IDS працює в реальному часі, постійно моніторячи мережу і виявляючи небезпеки в режимі реального часу.

Недоліки використання Системи виявлення вторгнень (IDS):

– IDS може ідентифікувати деякі звичайні дії як підозрілі, або недооцінювати деякі загрози, що може призводити до сповіщень, які вимагають подальшого аналізу.

– Деякі атаки можуть бути розроблені з метою обходу виявлення IDS, залишаючись непоміченими.

– IDS потребує налагодження та постійного оновлення правил виявлення для забезпечення ефективності та врахування нових видів загроз.

Щоб реалізувати Систему виявлення вторгнень, необхідно мати відповідне апаратне забезпечення та програмне забезпечення, що підтримує IDS. Вона може бути реалізована як фізичний пристрій або вбудована в мережеве обладнання, таке як маршрутизатори і комутатори. Для налагодження та управління IDS можуть використовуватися спеціальні інтерфейси або програмне забезпечення.

Під час роботи Системи виявлення вторгнень вона аналізує мережевий трафік, шукає підозрілі ознаки, порушення правил або незвичайні зміни у поведінці мережі. При виявленні потенційної загрози або вторгнення, IDS сповіщає

адміністратора або безпековий персонал, щоб подальші заходи могли бути прийняті для забезпечення безпеки системи та мережі.

Використання Системи виявлення вторгнень є дійсним способом виявлення Cyber Surveillance, оскільки вона дозволяє виявляти підозрілу активність, яка може бути пов'язана зі спостереженням або зловживанням. Вона допомагає забезпечити безпеку мережі, вчасно реагувати на загрози та запобігати можливим вторгненням.

2. Мережевий екран (Firewall).

Мережевий екран (Firewall) є важливим засобом, який використовується для виявлення та захисту від різних загроз, включаючи Cyber Surveillance. Він забезпечує фільтрацію мережевого трафіку, контролює доступ до ресурсів та мережевих служб, ідентифікує та блокує підозрілу активність, що може бути пов'язана зі спостереженням або зловживанням. Давайте розглянемо детальніше, як працюють мережеві екрани та чому вони є дійсним способом виявлення Cyber Surveillance.

Коротко розглянемо роботу мережевого екрана:

Мережевий екран функціонує як посередник між внутрішньою мережею і зовнішнім середовищем, контролюючи мережевий трафік, що проходить через нього. Він застосовує різні правила та політики безпеки для перевірки пакетів даних, що надходять та виходять з мережі, і приймає рішення про те, чи дозволити чи заборонити їхню передачу. У разі виявлення підозрілої або небажаної активності, мережевий екран може вживати різних заходів для реагування на інцидент. Це може включати автоматичне блокування джерела атаки, генерацію сповіщень про інцидент і збереження журналів подій для подальшого аналізу іншими системами та/або спеціалістами з кібербезпеки.

Переваги та недоліки Мережевих екранів:

Переваги:

- Мережевий екран забезпечує захист мережі, фільтруючи трафік та блокуючи небажану активність, включаючи Cyber Surveillance.

- Він дозволяє контролювати доступ до ресурсів та мережевих служб, забезпечуючи обмеження прав доступу до чутливої інформації.
- Мережеві екрани можуть виявляти аномальну активність, шкідливі атаки та інші загрози безпеці мережі.
- Мережеві екрани можуть бути легко інтегровані з іншими системами безпеки для забезпечення комплексного підходу до виявлення загроз.

Недоліки:

3 Мережеві екрани можуть бути менш ефективними проти нових типів атак та загроз, які вони не знають або не вміють виявляти.

4 Для забезпечення ефективності Мережевих екранів необхідно постійно поновлювати їхнє програмне та апаратне забезпечення, щоб враховувати нові загрози та вразливості.

Як організації можуть розгорнути мережеві екрани та що для цього потрібно:

Апаратне обладнання: Мережевий екран може бути реалізований у вигляді фізичного пристрою, що включає спеціальні компоненти для обробки мережевого трафіку та прийняття рішень щодо передачі даних.

Програмне забезпечення: Мережевий екран може також бути реалізований у вигляді програмного забезпечення, яке встановлюється на сервер або спеціальний пристрій. Він може бути інтегрований з операційною системою або працювати самостійно [7].

Конфігурація та налаштування: Для ефективного функціонування Мережевого екрана необхідно правильно сконфігурувати його правила та політики безпеки. Це включає визначення дозволених та заборонених типів мережевого трафіку, налаштування ідентифікації та аутентифікації користувачів, налаштування правил доступу до ресурсів тощо.

Чому Мережевий екрани дієвий у виявленні Cyber Surveillance? З декількох причин:

1. Фільтрація трафіку: Мережеві екрани можуть використовувати різні методи фільтрації трафіку, такі як інспекція пакетів, правила доступу, доменні імена тощо. Це дозволяє виявляти та заблокувати небажаний мережевий трафік, що може бути пов'язаний з Cyber Surveillance (наприклад коли йде постійне звернення до незрозумілого сервера, який не має відношення до компанії).

2. Інтелектуальний аналіз: Сучасні Мережеві екрани можуть використовувати алгоритми машинного навчання та штучного інтелекту для аналізу мережевого трафіку. Вони можуть виявляти аномальну поведінку, патерни атак та інші ознаки Cyber Surveillance.

3. Інтеграція з іншими системами: Мережеві екрани можуть бути швидко інтегровані з іншими системами безпеки, такими як системи виявлення вторгнень (IDS), системи управління подіями та інші. Це дозволяє значно збільшити ефективність виявлення та реагування на потенційні загрози, а також покращити захист загалом, не тільки від Cyber Surveillance.

Усі ці аспекти роботи Мережевих екранів допомагають у виявленні та захисті від Cyber Surveillance. Вони створюють шар безпеки, який допомагає виявити та зупинити небажану активність та спостереження у мережі. Проте, варто пам'ятати, що Мережевий екран не є єдиним стовідсотковим способом захисту, і надзвичайно рекомендується використовувати його в поєднанні з іншими методами та заходами безпеки для створення комплексної системи захисту мережі.

3. Системи моніторингу мережі

Системи моніторингу мережі є важливим інструментом виявлення Cyber Surveillance та інших загроз безпеці мережі. Вони дозволяють наглядати за активністю в мережі, аналізувати мережевий трафік і виявляти підозрілу або зловісну активність. Цей спосіб є дійсним через свою здатність виявляти вразливості, аномалії та атаки, які можуть бути пов'язані з Cyber Surveillance.

Робота систем моніторингу мережі базується на зборі, аналізі та інтерпретації мережевого трафіку. Для їх ефективної роботи потрібне апаратне та програмне забезпечення, яке забезпечує збір трафіку, аналіз його характеристик, виявлення

аномалій та специфічних патернів, які можуть свідчити про наявність Cyber Surveillance.

Для реалізації Системи моніторингу мережі необхідне спеціалізоване програмне забезпечення, яке забезпечує збір і аналіз мережевого трафіку. Такі системи можуть бути реалізовані на основі фізичних апаратних пристроїв, відомих як мережеві монітори, або програмних рішень, встановлених на серверах або віртуальних машинах.

Під час роботи Системи моніторингу мережі відбувається неперервний збір і аналіз мережевого трафіку. Вона аналізує пакети даних, що протікають через мережу, шукає відхилення від типових шаблонів та поведінки. Система виявляє незвичайну активність, аномалії, спроби несанкціонованого доступу, а також інші ознаки Cyber Surveillance. При виявленні підозрілого або небажаного трафіку система генерує так звані “алерти” або сповіщення для адміністраторів мережі.

Системи моніторингу мережі реагують на інциденти шляхом вжиття відповідних заходів для зупинення або мінімізації загрози. Це може включати блокування атакуючих IP-адрес, встановлення правил фільтрації трафіку, припинення підключення до вразливих систем або сповіщення відповідальних осіб для подальшої обробки інциденту.

Однією з основних переваг Систем моніторингу мережі є їх здатність виявляти навіть хитрі та субтильні загрози, які можуть бути пов'язані з Cyber Surveillance. Вони можуть виявляти нові методи атак і зловживання, які ще не відомі антивірусним програмам або іншим захисним засобам. Крім того, вони надають можливість для виявлення внутрішніх загроз, коли власний персонал або користувачі мережі стають джерелом спостереження.

Іншою перевагою є можливість контролювати весь мережевий трафік, що проходить через систему. Це дозволяє адміністраторам мережі збирати детальну статистику, аналізувати шаблони активності, розпізнавати незвичайну поведінку та забезпечувати дотримання політик безпеки.

Однак, Системи моніторингу мережі також мають деякі недоліки. Перш за все, вони можуть створювати значні обсяги даних, що потребують збереження та обробки. Це може вимагати додаткових ресурсів та інфраструктури для збереження і аналізу мережевого трафіку.

Крім того, Системи моніторингу мережі можуть бути схильні до помилкових спрацювань, що може призводити до генерації багатьох хибних “алертів”. Це може викликати незручності для адміністраторів мережі, які повинні витрачати час і ресурси на перевірку та аналіз кожного алерту.

Використання Системи моніторингу мережі є гарним способом виявлення Cyber Surveillance через їх здатність виявляти незвичайну активність та аномалії, що можуть свідчити про вторгнення або спостереження. Вони надають адміністраторам мережі цінну інформацію про стан безпеки мережі, дозволяючи своєчасно реагувати на загрози та запобігати потенційним атакам. Завдяки цим системам організації можуть забезпечити високий рівень безпеки своїх мереж та захистити конфіденційну інформацію від небажаного доступу.

4. Системи реєстрації подій (Event Logging Systems)

Система реєстрації подій (Event Logging System) є важливим компонентом для виявлення Cyber Surveillance та забезпечення безпеки інформаційних систем. Її завданням є збір, збереження та аналіз журналів подій, що відбуваються в мережі або на окремих комп'ютерах. Система реєстрації подій реєструє різноманітні дії, які відбуваються в системі, такі як вхід в систему, виходи, запуск програм, зміни конфігурації, доступ до файлів тощо [8].

Принцип роботи Системи реєстрації подій полягає в тому, що вона збирає дані з різних джерел, таких як операційна система, додатки, мережеві пристрої, файрволи тощо, і записує ці дані в журнали подій. Кожна подія отримує часову мітку, інформацію про джерело події, тип події, параметри та додаткові деталі, які дозволяють зрозуміти, що саме сталося. Система реєстрації подій може працювати на рівні окремих комп'ютерів або на рівні мережі, де централізовано збираються журнали подій з усіх пристроїв.

Один з основних аспектів, який робить систему реєстрації подій ефективною для виявлення Cyber Surveillance, це можливість виявлення незвичайної або підозрілої активності. Система реєстрації подій збирає великий обсяг інформації про події, які відбуваються в системі, і дозволяє аналізувати ці дані для виявлення аномальних патернів або поведінки, які можуть свідчити про Cyber Surveillance. Наприклад, вона може виявити незвичайну активність з певного IP-адреси, непередбачені зміни в системних файлих, спроби несанкціонованого доступу до важливих ресурсів тощо.

Для реалізації Системи реєстрації подій необхідно мати як апаратне, так і програмне забезпечення. Апаратна складова може включати спеціалізовані сервери або пристрої, які здатні збирати великий обсяг журналів подій і забезпечувати їх збереження. Програмне забезпечення включає різноманітні системи управління журналами, які забезпечують збір, агрегацію, фільтрацію та аналіз подій. Також важливо налаштувати правила і порогові значення для виявлення підозрілої активності та належно сконфігурувати систему для відправки алертів адміністраторам безпеки у разі виявлення підозрілих подій.

Під час роботи Системи реєстрації подій відбувається неперервний процес збору, обробки та збереження журналів подій. Система реєструє кожну активність, що відбувається в мережі або на комп'ютерах, і зберігає цю інформацію відповідно до налаштувань збереження даних. Під час збору даних важливо забезпечити цілісність та конфіденційність журналів подій, оскільки це важлива інформація, яка може використовуватися для виявлення загроз безпеці.

Системи реєстрації подій можуть реагувати на інциденти в різних режимах. Деякі системи можуть надавати реального часу “алерти” адміністраторам безпеки про підозрілу або небезпечну активність. Це дозволяє оперативно реагувати на загрози та вживати заходи для їхнього усунення. Крім того, системи реєстрації подій зазвичай забезпечують можливість аналізувати історичні дані, що дозволяє виявити патерни атак, встановити причини інцидентів та побудувати стратегії запобігання майбутнім загрозам.

Переваги використання Систем реєстрації подій виявлення Cyber Surveillance включають:

1. Системи реєстрації подій дозволяють виявляти незвичайні або підозрілі події, які можуть свідчити про Cyber Surveillance. Це дозволяє оперативно реагувати на загрози та запобігати можливим атакам.

2. Системи реєстрації подій забезпечують збереження історичних журналів подій, що може бути корисно для подальшого аналізу і розслідування інцидентів. Вони створюють цифровий слід, який може бути використаний для виявлення і відновлення дій зловмисників.

3. Деякі системи реєстрації подій можуть надавати можливість моніторити події в реальному часі і отримувати алерти про підозрілу активність. Це дозволяє оперативно реагувати на потенційні загрози та запобігати їхньому поширенню.

Незважаючи на переваги, Системи реєстрації подій також мають свої недоліки:

1. Збір великого обсягу журналів подій може призвести до значного зростання обсягу даних для зберігання і аналізу. Це може вимагати значних ресурсів для зберігання і обробки даних.

2. Аналіз журналів подій може бути складним завданням, особливо при великій кількості зібраних даних. Вимагається спеціаліст з безпеки, який має знання та досвід у сфері аналізу подій, для виявлення підозрілих активностей та ідентифікації потенційних загроз.

3. Хакери та зловмисники можуть вживати заходів для обхіду системи реєстрації подій, щоб приховати свою активність або змінити записи подій.

5. Системи контролю доступу (Identity and access management system, IAM)

Системи контролю доступу (Identity and access management system, IAM) – це апаратні та програмні компоненти, що використовуються для керування доступом користувачів до різних ресурсів в комп'ютерних системах. Вони забезпечують безпеку даних шляхом ідентифікації, аутентифікації, авторизації та аудиту доступу

до цих ресурсів. Ці системи можуть бути використані як засіб виявлення кібернетичного спостереження, а також як засіб захисту від нього.

IAM-системи використовуються для керування доступом користувачів до різних ресурсів, таких як файли, бази даних, мережеві служби та інші. Ці системи дозволяють створювати та керувати ідентифікаційними записами користувачів, надавати їм права доступу до різних ресурсів та відстежувати їхню активність в системі [9].

Ідентифікація користувача – це процес визначення, хто саме входить в систему. Після успішної ідентифікації, користувач повинен бути аутентифікований, щоб підтвердити свою ідентичність та підтвердити свої права доступу до ресурсів. Авторизація пов'язана з наданням користувачу конкретних прав доступу до ресурсів в системі. І, нарешті, аудит відбувається для забезпечення збору, аналізу та зберігання інформації про активність користувачів у системі.

IAM-системи зазвичай включають в себе такі компоненти, як:

Директорії: це сховище даних, що містить інформацію про користувачів та ресурси, до яких вони мають доступ. Директорії можуть використовуватися як для зберігання даних користувачів, так і для зберігання політик доступу до ресурсів.

Механізми аутентифікації: це компоненти, що використовуються для перевірки ідентичності користувачів. Це може бути, наприклад, процес введення логіна та пароля або використання біометричних даних.

Механізми авторизації: це компоненти, що визначають права доступу користувачів до ресурсів в системі. Вони враховують політики безпеки та ролі користувачів для прийняття рішень щодо надання або відмови в доступі.

Механізми аудиту: ці компоненти відповідають за реєстрацію та збереження історії дій користувачів в системі. Вони забезпечують збір і аналіз журналів подій, що дозволяє виявляти підозрілу або небажану активність.

Під час роботи Системи контролю доступу, дані про ідентифікацію, аутентифікацію, авторизацію та аудит збираються і аналізуються для виявлення підозрілої або небажаної активності. Наприклад, система може виявити надмірну

кількість невдалих спроб входу, незвичайну активність користувачів або незвичайні зміни в правах доступу. Це може свідчити про можливість кібернетичного спостереження або зловживання доступом.

Якщо Система контролю доступу виявляє підозрілу активність, вона може прийняти певні заходи реагування. Це може включати блокування доступу користувача, сповіщення адміністратора про інцидент, виконання подальшого аналізу або автоматичне запуск інших заходів безпеки.

Системи контролю доступу мають кілька переваг у виявленні Cyber Surveillance:

1. IAM-системи збирають і аналізують дані про активність користувачів, дозволяючи виявити незвичайну або підозрілу поведінку, яка може бути пов'язана з кібернетичним спостереженням.

2. IAM-системи допомагають управляти правами доступу користувачів, забезпечуючи, що лише авторизовані особи мають доступ до ресурсів. Це зменшує ризик несанкціонованого доступу для кібернетичного спостереження.

3. IAM-системи дозволяють централізовано керувати ідентифікацією, аутентифікацією, авторизацією та аудитом в різних системах та додатках. Це спрощує процес виявлення кібернетичного спостереження та реагування на нього.

4. IAM-системи можуть бути інтегровані з іншими засобами безпеки, такими як системи виявлення вторгнень або системи моніторингу мережі, для отримання комплексного погляду на кібернетичне спостереження.

Незважаючи на переваги, системи контролю доступу також мають свої недоліки:

1 Складність впровадження: Реалізація і налагодження IAM-систем може бути складним процесом, особливо в організаціях зі складною інфраструктурою та великою кількістю користувачів.

2 IAM-системи можуть вимагати значних ресурсів, включаючи обладнання, пропускну здатність мережі та велику кількість дискового простору для зберігання даних про активність користувачів.

3 Централізоване керування IAM-системою може вимагати спеціалізованих знань та навичок, особливо в організаціях з великою кількістю користувачів та розподіленими ресурсами.

4 IAM-системи можуть видавати хибнопозитивні або хибнодійсні сповіщення про підозрілу активність, що може призвести до зайвих труднощів та витрат на перевірку та відповідну реакцію.

Використання системи контролю доступу (IAM) є гарним способом виявлення Cyber Surveillance через його здатність до виявлення підозрілої активності і аномалій у поведінці користувачів, забезпечення авторизованого доступу до ресурсів та запобігання несанкціонованому доступу, централізованого керування та моніторингу ідентифікаційних даних та активності користувачів та інтеграції з іншими системами безпеки для отримання комплексного погляду на кібернетичне спостереження.

Враховуючи ці переваги, використання системи контролю доступу (IAM) є важливим елементом в сукупності заходів з виявлення та запобігання кібернетичного спостереження. Й саме на цьому інструменті зосереджена вся увага в даній роботі.

2.2 Порівняння IAM систем для виявлення та запобігання Cyber Surveillance

Дана робота зосереджена на використанні IAM систем для виявлення та запобігання Cyber Surveillance. Тому потрібно оглянути ринок даних продуктів, та порівняти продукти між собою. Дане порівняння є необхідним для визначення найбільш ефективних і надійних рішень. Дане порівняння допоможе вибрати найкращий продукт, відповідний потребам та вимогам з точки зору безпеки та функціональності.

1. Keycloak:

Keycloak є відкритим та безкоштовним інструментом управління доступом та ідентифікацією (IAM) [10], який надає широкий функціонал для забезпечення безпеки додатків та захисту від Cyber Surveillance.

Переваги:

- Широкий спектр функціональних можливостей, включаючи ідентифікацію, автентифікацію, авторизацію та управління доступом, має багатофакторну атуентифікацію та інші розширені засоби безпеки.
- Розширюваність та гнучкість для інтеграції з іншими системами та розробкою додаткових функцій.
- Відкритий вихідний код, що дозволяє залучати спільноту розробників для вдосконалення та підтримки продукту.

Недоліки:

- Не має повного охоплення всіх можливостей, які пропонують інші корпоративні продукти.
- Вимагає певного рівня технічних знань для ефективного налаштування та використання.

2. Okta:

Okta є популярним корпоративним рішенням IAM, яке надає різноманітні засоби для управління доступом та захисту від Cyber Surveillance.

Переваги:

- Широкий набір функціональних можливостей, включаючи ідентифікацію, автентифікацію, авторизацію та моніторинг безпеки.
- Інтеграція з багатьма популярними системами та рішеннями, що полегшує їхнє використання.
- Масштабованість для використання в різних типах організацій

Недоліки:

- Вартість використання може бути високою для менших компаній або організацій з обмеженими бюджетами.

- Вимагає певного часу та ресурсів для налагодження та впровадження.

3. Microsoft Azure Active Directory (Azure AD)

Azure AD є рішенням IAM, яке надає засоби для ідентифікації, автентифікації, авторизації та управління доступом в екосистемі Microsoft та поза її межами.

Переваги:

- Глибока інтеграція з іншими продуктами та сервісами Microsoft, забезпечуючи синергію та спрощення використання.
- Багатофакторна аутентифікація та інші розширені засоби безпеки.
- Масштабованість для використання в різних типах організацій.

Недоліки:

- Вартість може бути високою, особливо для повного спектру функцій та великого обсягу користувачів.
- Обмежена гнучкість та настроюваність порівняно з відкритими або спеціалізованими рішеннями.

Вибір Keycloak для дослідження був зумовлений декількома факторами. По-перше, Keycloak є відкритим та безкоштовним продуктом з відкритим вихідним кодом, що забезпечує доступність та гнучкість для дослідження та впровадження. По-друге, Keycloak надає широкий спектр функціональних можливостей для виявлення та запобігання Cyber Surveillance, включаючи ідентифікацію, автентифікацію, авторизацію та управління доступом. Незважаючи на те, що Keycloak може не охопити весь функціонал інших корпоративних продуктів, його гнучкість та розширюваність роблять його привабливим вибором для дослідження та персоналізації під конкретні потреби організації.

Враховуючи вищезгадане порівняння, можна зробити висновок, що Keycloak є конкурентоспроможним продуктом для виявлення та запобігання Cyber Surveillance, зокрема у випадку організацій, які цінують відкритий вихідний код, гнучкість налаштування та високий рівень контролю.

2.3 IAM Keycloak

У цьому розділі буде детально розглянуто Keycloak - потужний інструмент управління ідентифікацією та автентифікацією, який успішно використовується не тільки для запобігання Cyber Surveillance, але й для забезпечення загальної безпеки різних систем, починаючи з веб-додатків закінчуючи гігантськими корпоративними мережами. Keycloak відіграє важливу роль у сучасних системах, забезпечуючи безпеку та захист інформації шляхом управління доступом користувачів до ресурсів системи.

Keycloak - це відкритий програмний засіб (Open Source), розроблений для управління ідентифікацією та автентифікацією в розподілених додатках та сервісах. Він надає масштабовану та безпечну інфраструктуру для аутентифікації користувачів, контролю доступу та керування правами [11].

Keycloak забезпечує безпеку ідентифікації та автентифікації користувачів. Він надає різноманітні методи аутентифікації, такі як логін/пароль, багатофакторна аутентифікація та використання сертифікатів. Це дозволяє підтверджувати ідентичність користувачів перед наданням доступу до системи.

Крім того, Keycloak надає засоби для керування авторизацією, що дозволяє визначити, які ресурси можуть бути доступні для кожного користувача. Він дозволяє створювати ролі, групи та політики доступу, що допомагає точно визначити рівень доступу до ресурсів та забезпечити контроль над ними.

Keycloak підтримує широкий спектр стандартів безпеки, таких як OpenID Connect, OAuth 2.0 і SAML. Це робить його сумісним із застосунками і сервісами, які використовують ці стандарти. Він дозволяє інтегрувати Keycloak з існуючими системами управління ідентифікацією та забезпечує стандартизований підхід до безпеки аутентифікації та авторизації.

Keycloak надає централізовану платформу для управління ідентифікацією та автентифікацією. Він дозволяє адміністраторам керувати користувачами, ролями, політиками доступу та іншими параметрами безпеки з одного інтерфейсу. Це робить процес управління безпекою простим та ефективним.

Keycloak побудований з урахуванням масштабованості та високої продуктивності. Він може обробляти великі обсяги запитів аутентифікації та авторизації без затримок і забезпечує високу доступність системи. Це дозволяє йому працювати з розподіленими додатками та великими мережами з високим навантаженням.Основними компонентами Keycloak є Realm (область), Клієнти, Користувачі, Ролі та Протоколи безпеки.

Realm є основним контейнером для всіх інших об'єктів Keycloak. Кожен Realm представляє собою ізольовану область, в якій зберігаються дані користувачів, клієнтів, ролей та інших об'єктів. Він визначає контекст безпеки, правила аутентифікації та авторизації для об'єктів, що належать до нього. Одна з основних переваг використання Realm полягає в тому, що вони дозволяють створювати ізольовані середовища для різних додатків або систем, що використовують Keycloak. Кожен Realm може мати власні налаштування безпеки, політики авторизації та власну базу користувачів.

Наприклад, якщо у вас є система, що використовує Keycloak для керування доступом користувачів, ви можете створити окремий Realm для кожного клієнта або додатка. Кожен Realm буде мати своїх користувачів, ролі, налаштування безпеки та політики доступу. Це дозволить вам ефективно управляти доступом до ресурсів для кожного клієнта окремо [12].

Крім того, Realmи дозволяють створювати ієрархію або відносини між собою. Наприклад, ви можете створити батьківський Realm і додаткові дочірні Realmи, які успадковують налаштування та правила доступу від батьківського Realma. Це дозволяє вам організувати багаторівневу структуру для управління доступом на різних рівнях системи.

Таким чином, Realmи у Keycloak забезпечують гнучкість, масштабованість та контроль над безпекою та доступом в системі. Вони дозволяють легко організувати та керувати безпековими просторами для різних додатків або клієнтів, забезпечуючи надійну ідентифікацію та авторизацію користувачів.

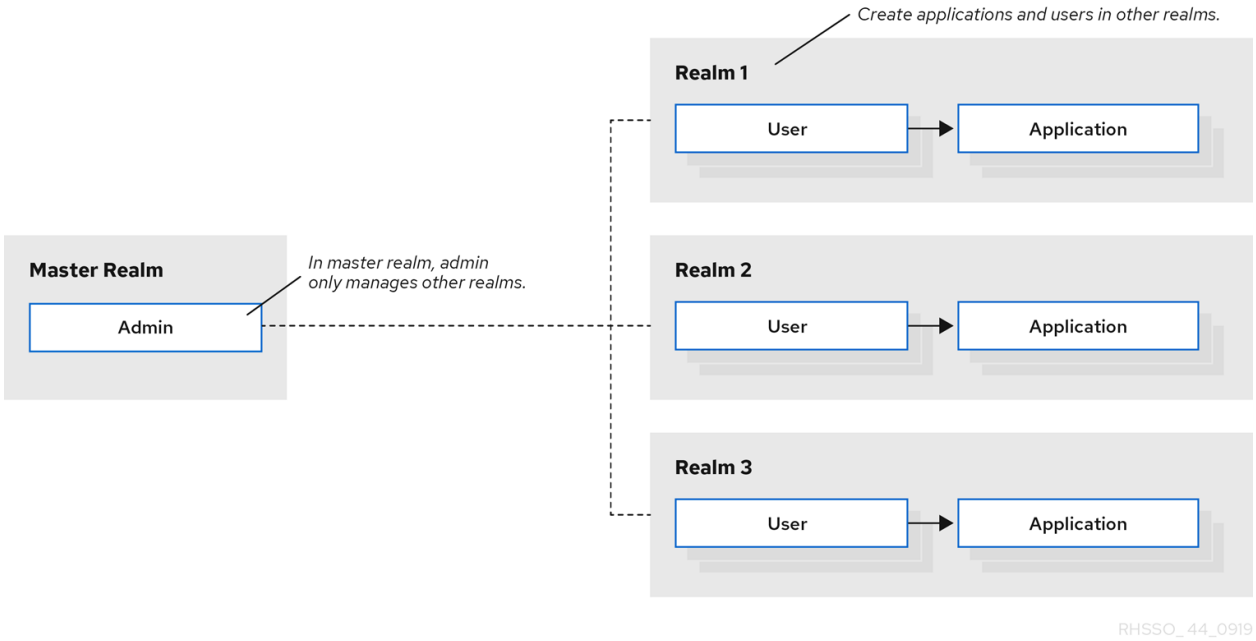

Рис. 2.1 Відносини між “Realmами”, проста схема, яка демонструє яким чином працюють “Realmи” в Keycloak

Клієнти представляють собою додатки або сервіси, які використовують Keycloak для аутентифікації та авторизації користувачів. Клієнти можуть бути веб-додатками, мобільними додатками або іншими системами, які взаємодіють з Keycloak. Клієнти реєструються в Realm і мають свої унікальні ідентифікатори та налаштування безпеки.

Клієнти можуть бути різних типів, таких як веб-додатки, мобільні додатки, API-сервіси або навіть інші системи. Кожен клієнт має унікальний ідентифікатор і налаштування безпеки, що дозволяють Keycloak ідентифікувати та авторизувати користувачів, що намагаються отримати доступ до цих додатків або ресурсів.

Один з основних завдань клієнтів у Keycloak - це здійснювати аутентифікацію користувачів. Клієнт звертається до Keycloak для отримання токенів аутентифікації, які дозволяють ідентифікувати користувача. Keycloak проводить процес аутентифікації на основі налаштувань безпеки, таких як використання ідентифікаційних постачальників, мультифакторної аутентифікації

тощо, і надає клієнту валідний токен, який далі може бути використаний для доступу до ресурсів [5-8].

Клієнти також відповідають за авторизацію доступу до ресурсів. Keycloak надає можливість налаштовувати політики авторизації для кожного клієнта, що дозволяє контролювати, які ресурси мають доступ до клієнта, які ролі або дозволи потрібні для доступу, які обмеження часу чинність і т.д.

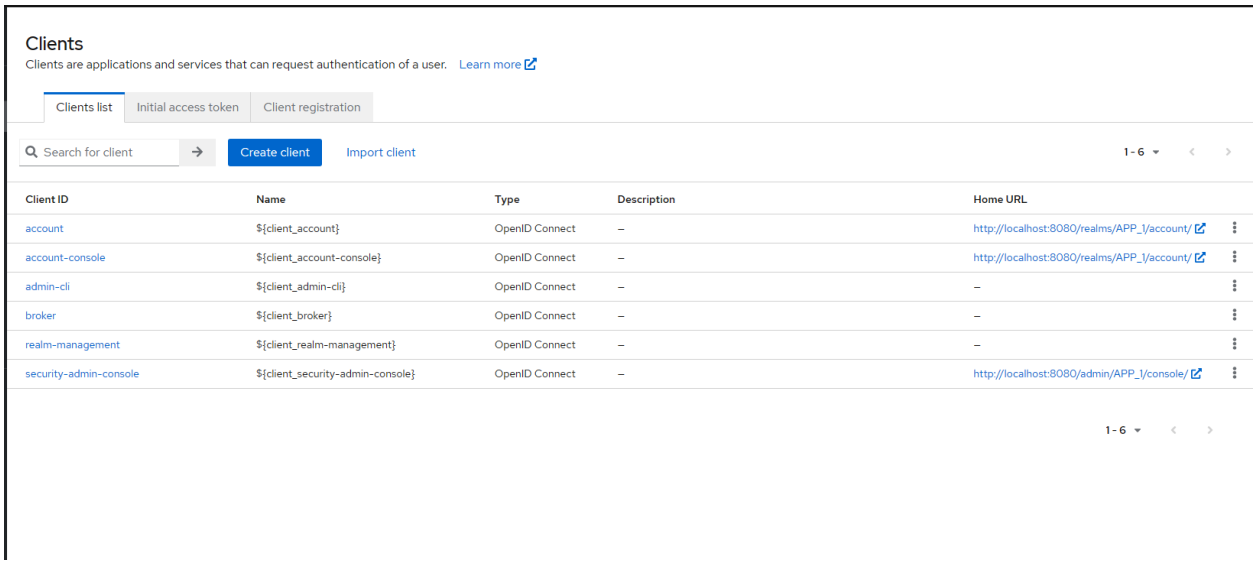

Рис. 2.2 Інтерфейс адміністрування клієнтів в Keycloak.

Користувачі є суб'єктами, які отримують доступ до додатків та ресурсів через Keycloak. Користувачі реєструються в Realm та мають унікальні ідентифікатори, аутентифікаційні дані та набір ролей, які визначають їхні права доступу.

Keycloak дозволяє створювати та управляти користувачами з різними атрибутами, такими як ім'я, електронна пошта, роль, група тощо. Користувачі можуть бути організовані у групи, які спрощують управління доступом до ресурсів для багатьох користувачів одночасно. Також, в Keycloak можна налаштовувати ролі, які надаються користувачам, що дозволяє контролювати їх права доступу до ресурсів.

Користувачі можуть проходити процес аутентифікації в Keycloak, щоб підтвердити свою ідентичність і отримати доступ до системи або додатків.

Keycloak підтримує різні протоколи аутентифікації, такі як OAuth, OpenID Connect, SAML і інші, що дають користувачам можливість використовувати різні методи для входу до системи.

Управління користувачами в Keycloak також включає можливість налаштовувати політики паролів, змінювати атрибути користувачів, надавати чи відбирати ролі, додавати до груп, встановлювати обмеження часу дії акаунтів та інші дії для забезпечення безпеки та ефективного управління доступом.

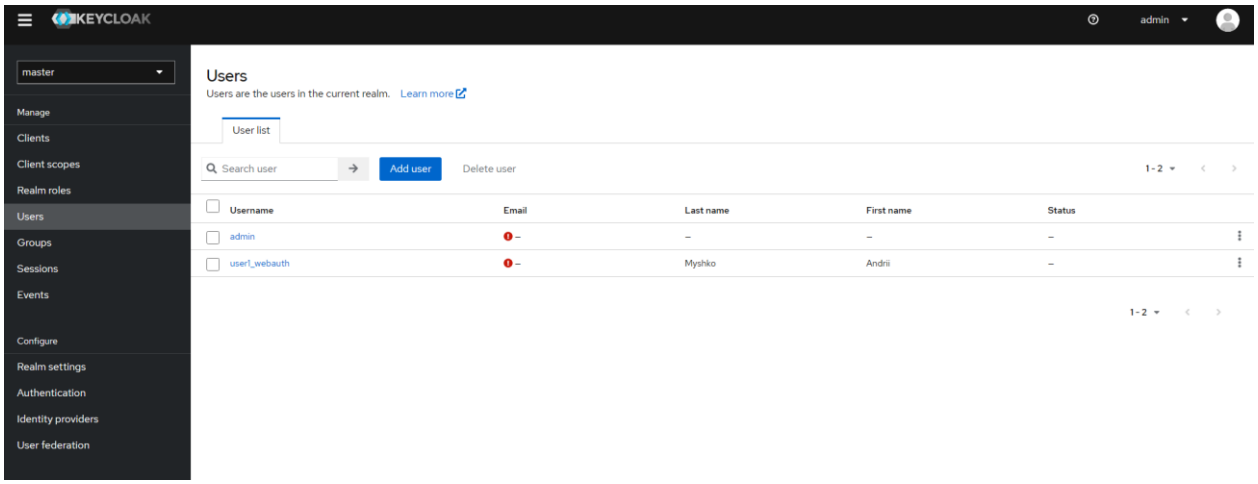

Рис. 2.3 Інтерфейс адміністрування клієнтів

Ролі використовуються для керування правами доступу користувачів. Вони дозволяють визначати групи прав, які можуть бути присвоєні користувачам. Ролі можуть мати свої обмеження та політики безпеки, що використовуються для контролю доступу користувачів до ресурсів [9-12].

Кожна роль має свій набір привілеїв, які визначають дозволи користувача на доступ до конкретних функціональностей системи або ресурсів. Наприклад, роль "адміністратор" може мати повний доступ та контроль над системою, тоді як роль "користувач" може мати обмежений доступ до певних функцій.

Ролі можуть бути надані окремим користувачам або групам користувачів. Групування користувачів за ролями спрощує управління доступом та дозволяє швидко змінювати привілеї для цілої групи користувачів замість встановлення їх індивідуально.

Крім вбудованих ролей, Keycloak також дозволяє створювати власні ролі, що відповідають унікальним потребам системи. Це дає можливість докладно налаштувати привілеї та контроль доступу до ресурсів з урахуванням специфіки додатка чи сервісу.

Ролі в Keycloak використовуються для реалізації процесу авторизації, де система перевіряє, чи має користувач необхідні ролі для доступу до ресурсу. Ролі дозволяють встановлювати права доступу на основі принципу "найменшого привілею", де користувач отримує доступ лише до тих функцій та ресурсів, які необхідні йому для виконання своїх завдань.

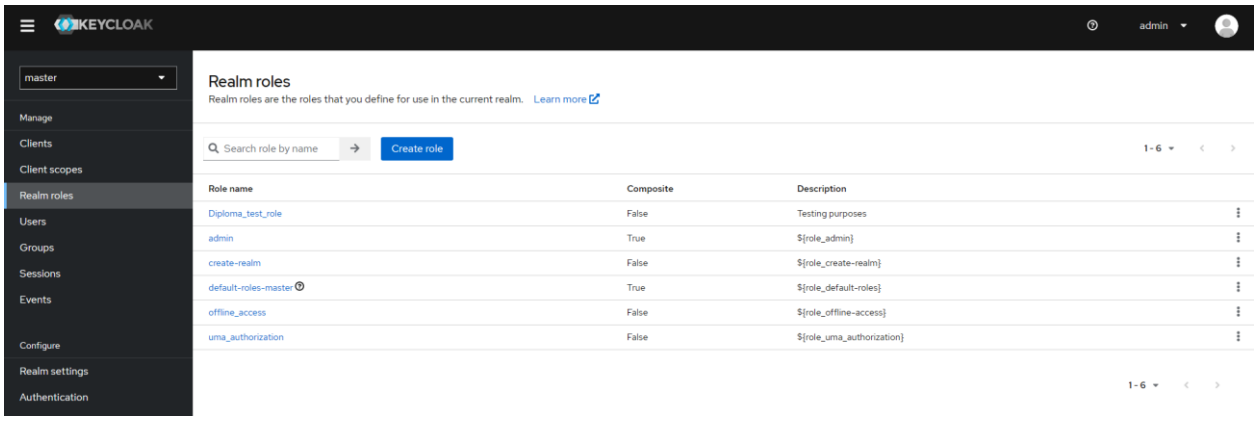

Рис. 2.4 Інтерфейс адміністрування ролей

Рис. 2.5 Інтерфейс редагування ролей, присвоєння ролей конкретним користувачам та присвоєння атрибутів конкретним ролям

Протоколи безпеки визначають правила і механізми, які використовуються для забезпечення безпеки взаємодії між Keycloak і його клієнтами. Keycloak підтримує різні протоколи безпеки, такі як OpenID Connect, SAML і OAuth, що дозволяють інтегрувати його з різними додатками та системами.

OAuth 2.0 є протоколом авторизації, який дозволяє користувачам видавати доступ до своїх ресурсів третім сторонам без необхідності надавати їм свої облікові дані. У Keycloak ви можете налаштувати сервер OAuth, де клієнти можуть зареєструватись та отримати доступ до API за допомогою токенів доступу. Користувачі можуть автентифікуватись через Keycloak і видавати токени доступу третім сторонам для обмеженого доступу до своїх ресурсів.

OpenID Connect є протоколом, який побудований на основі OAuth 2.0 і додає ідентифікацію до авторизації. Він дозволяє взаємодіяти зі стандартними ідентифікаційними постачальниками і дозволяє клієнтам отримувати інформацію про користувача після успішної аутентифікації. Keycloak може використовуватись як провайдер OpenID Connect, що дозволяє клієнтам отримувати профіль користувача та іншу інформацію після автентифікації через Keycloak.

SAML (Security Assertion Markup Language) є протоколом односторонньої автентифікації, який використовується для обміну ідентифікаційними та авторизаційними даними між сторонами. Keycloak може діяти як постачальник

ідентифікації SAML, що дозволяє інтегрувати його з системами, які підтримують SAML. Користувачі можуть автентифікуватись через Keycloak, а потім отримувати ствердження безпеки (assertions), які можна передати іншим системам для авторизації та доступу до ресурсів [10].

Процес аутентифікації та авторизації з використанням цих протоколів в Keycloak зазвичай включає наступні кроки: клієнти реєструються в Keycloak, налаштовують правила аутентифікації та авторизації, а користувачі проходять процес аутентифікації через Keycloak за допомогою вибраного протоколу. Keycloak генерує та валідує токени доступу, які можуть використовуватись для отримання доступу до ресурсів з врахуванням встановлених правил і політик безпеки.

Цей процес дозволяє системам управління доступом Keycloak надати безпеку та контроль доступу для різноманітних додатків і сервісів, використовуючи різні протоколи безпеки в залежності від потреб інтеграції.

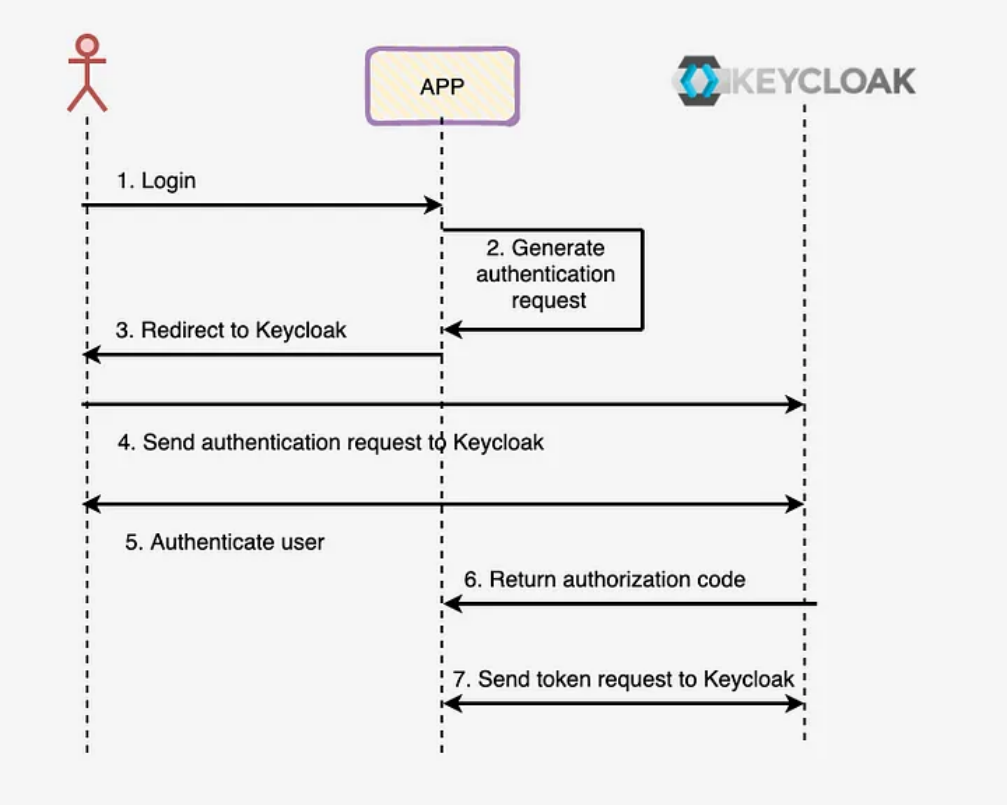

Рис. 2.6 Базова реалізація протоколу OpenID Connect в Keycloak

Зв'язок між всіма цими компонентами полягає в тому, що клієнти реєструються в Realm, а користувачі аутентифікуються через Keycloak для отримання доступу до ресурсів, заснованих на їхніх ролях та політиках безпеки. Keycloak забезпечує механізми автентифікації, авторизації та керування сесіями для забезпечення безпеки і управління доступом до системи. Протоколи безпеки використовуються для захищеної комунікації між Keycloak і клієнтами, забезпечуючи обмін інформацією про ідентифікацію та авторизацію.

Загальна архітектура Keycloak побудована навколо цих компонентів та їх взаємодії, що дозволяє розробникам легко впроваджувати потужні системи управління доступом для своїх додатків та сервісів [1-3].

Дані компоненти будуть розглянуті більш детально безпосередньо в практичній частині даного дослідження при розробці практичних рекомендацій.

Висновок до розділу 2

У цьому розділі було розглянуто методи виявлення та запобігання Cyber Surveillance і проведено порівняння різних IAM систем. За допомогою цього порівняння було отримано важливі висновки щодо ефективності та надійності цих систем у контексті боротьби з Cyber Surveillance. Дане порівняння показало, що Keycloak є потужним інструментом для управління доступом і ідентифікації. Він має відкритий вихідний код, що сприяє гнучкості та можливості налаштування під потреби організації.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ CYBER SURVEILLANCE ЗА ДОПОМОГОЮ IAM

3.1 Дослідження технічних можливостей Keycloak для виявлення та запобігання Cyber Surveillance

Keycloak надає широкий набір функцій та можливостей, що дозволяють виявляти потенційні загрози кібер-спостереження та ефективно їм протистояти. Я ретельно проаналізую ці можливості і розкрию їх потенціал в контексті виявлення та запобігання різноманітним формам Cyber Surveillance. Для дослідження можливостей Keycloak в запобіганні та виявленні Cyber Surveillance, я використаю минулий розділ, та опишу, яким чином Keycloak здатен протидіяти сучасним загрозам Cyber Surveillance [2-6].

Відстеження даних.

Keycloak використовує механізми шифрування для захисту особисто ідентифікованої інформації про користувачів. Коли дані зберігаються у базі даних або передаються по мережі, вони шифруються, що робить їх непридатними для перехоплення та читання третіми сторонами. Крім того, Keycloak надає можливість настроювати політики збору і використання даних, дозволяючи користувачам контролювати, які дані збираються і як вони використовуються.

Вторгнення в приватне життя.

Keycloak забезпечує механізми аутентифікації та авторизації, що дозволяють встановлювати рівні доступу до ресурсів. Завдяки цьому, тільки користувачі з необхідними привілеями можуть отримати доступ до конфіденційної інформації. Keycloak також дозволяє управляти згодами користувачів щодо збору і використання їхніх особистих даних, надаючи їм контроль над обсягом і способом використання їхньої інформації.

Масовий нагляд.

Keycloak надає можливість налаштування політик безпеки, які дозволяють обмежувати доступ до системи для певних груп користувачів. За допомогою правил авторизації і контролю доступу, Keycloak забезпечує здатність встановлювати, які дії можуть виконувати користувачі і які ресурси вони можуть переглядати. Це дозволяє уникнути масового нагляду, так як доступ до інформації обмежується лише до необхідного мінімуму.

Цензура та обмеження доступу.

Keycloak надає можливість налаштовувати політики контролю доступу для керування правами користувачів до ресурсів системи. Адміністратори можуть встановлювати обмеження доступу на основі ролей, груп або інших критеріїв, що дозволяє забезпечити, що лише визначені користувачі мають доступ до певної інформації або функціональності. Це допомагає запобігти небажаній цензурі та обмеженню доступу до конфіденційних даних.

Соціальна інженерія.

Keycloak звертає особливу увагу на безпеку аутентифікації, зокрема на захист від соціальної інженерії. Він надає можливість налаштовувати сильні паролі, багатофакторну аутентифікацію та інші механізми захисту від шахрайства. Keycloak також пропонує різноманітні стратегії аутентифікації, такі як використання сертифікатів, OAuth-токенів або інтеграцію з існуючими ідентифікаційними системами, що дозволяє забезпечити надійність процесу аутентифікації та унеможливити соціальну інженерію.

Крадіжка ідентифікаційних даних [9].

Keycloak використовує різноманітні механізми захисту від крадіжки ідентифікаційних даних. Він підтримує шифрування персональних даних, таких як паролі і токени доступу, що робить їх непридатними для використання зловмисниками. Крім того, Keycloak пропонує можливість встановлювати термін дії токенів доступу, вимагати багатофакторну аутентифікацію та інші механізми

безпеки, що допомагають унеможливити несанкціонований доступ до облікових записів користувачів.

3.2 Розгортання та налаштування IAM та реагування на загрозу

Встановлення та розгортання IAM Keycloak не є складною задачею. В даній роботі буде розглянутий найбільш розповсюджений та легкий спосіб розгортання - за допомогою ПЗ Docker.

Установка та налаштування Keycloak за допомогою Docker є швидким та зручним способом розгортання Keycloak. Docker забезпечує контейнеризацію, що дозволяє легко управляти залежностями, розгортати програмне забезпечення та забезпечує його ізольоване середовище.

Переваги використання Docker для запуску Keycloak полягають у простоті та швидкості розгортання. Docker дозволяє легко створювати, розгортати та управляти контейнерами з Keycloak, ізолюючи його від інших компонентів вашої системи. Це спрощує процес розгортання, оновлення та масштабування Keycloak. Крім того, Docker забезпечує переносимість, що означає, що э змога запустити Keycloak на будь-якому середовищі, де працює Docker, незалежно від операційної системи та конфігурації сервера [6-10].

Після встановлення ПЗ Docker запуск IAM Keycloak потребує лише однієї команди в терміналі.

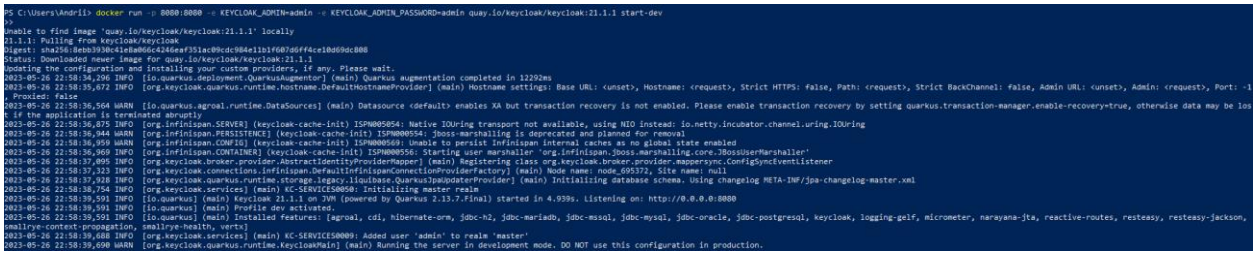

Рис. 3.1. Процес встановлення Docker-контейнеру з IAM Keycloak

Ця команда завантажує та запускає офіційний Docker образ Keycloak з Docker Hub. Параметри -p вказують на прив'язку портів контейнера до порту 8080, а -e встановлюють імена користувача та пароль для адміністративного доступу.

Після завантаження та розгортання з’явиться повідомлення про успішний старт контейнера. Наразі залишилось тільки перевірити чи дійсно контейнер з IAM Keycloak запущений та працює. Для цього потрібно перейти до веб-інтерфейсу IAM Keycloak, який розташований за адресою http://localhost:8080.

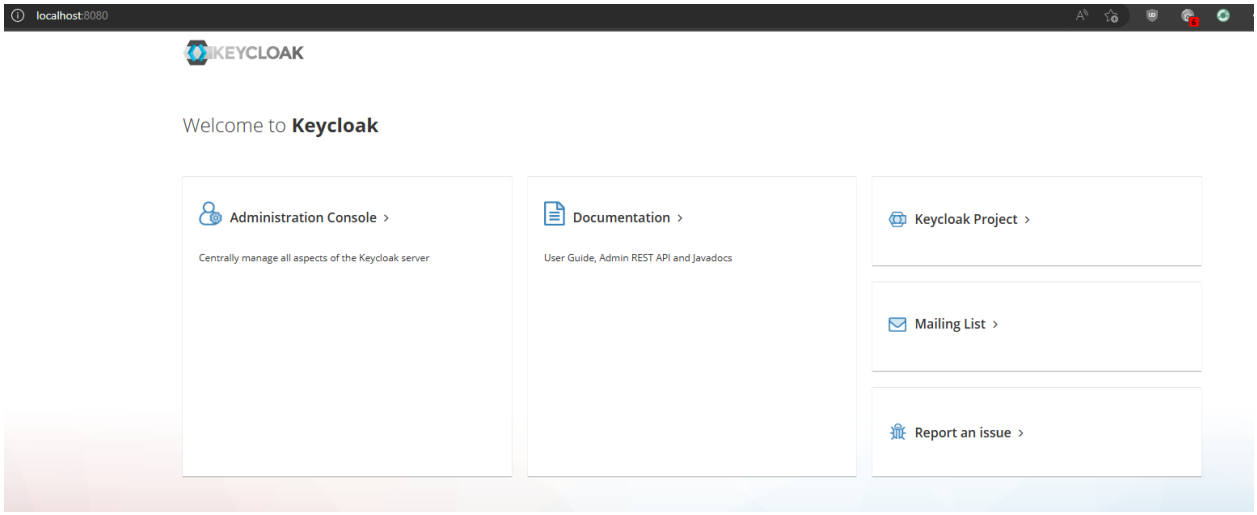

Рис. 3.2 Головний екран IAM Keycloak

Далі можна увійти в адміністративний інтерфейс Keycloak за допомогою облікових даних адміністратора, які були встановлені при установці та розгортанні контейнеру Docker, в цьому випадку - “admin”/”admin”.

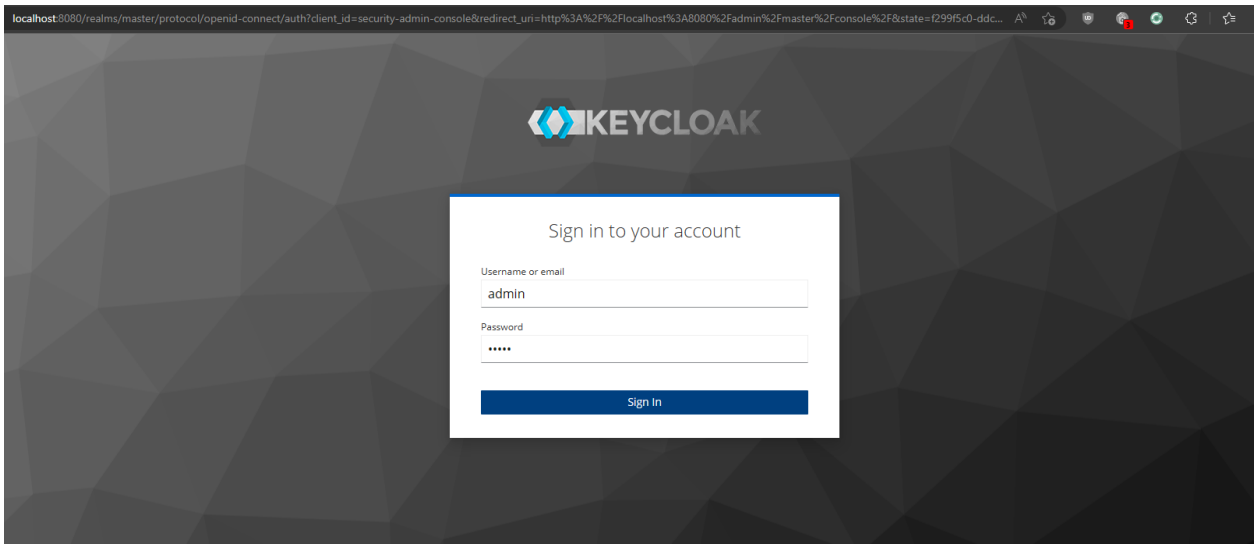

Рис. 3.3 Вікно входу Keycloak

Далі з’явиться панель адміністратора, яка дозволяє проводити глибші налаштування системи.

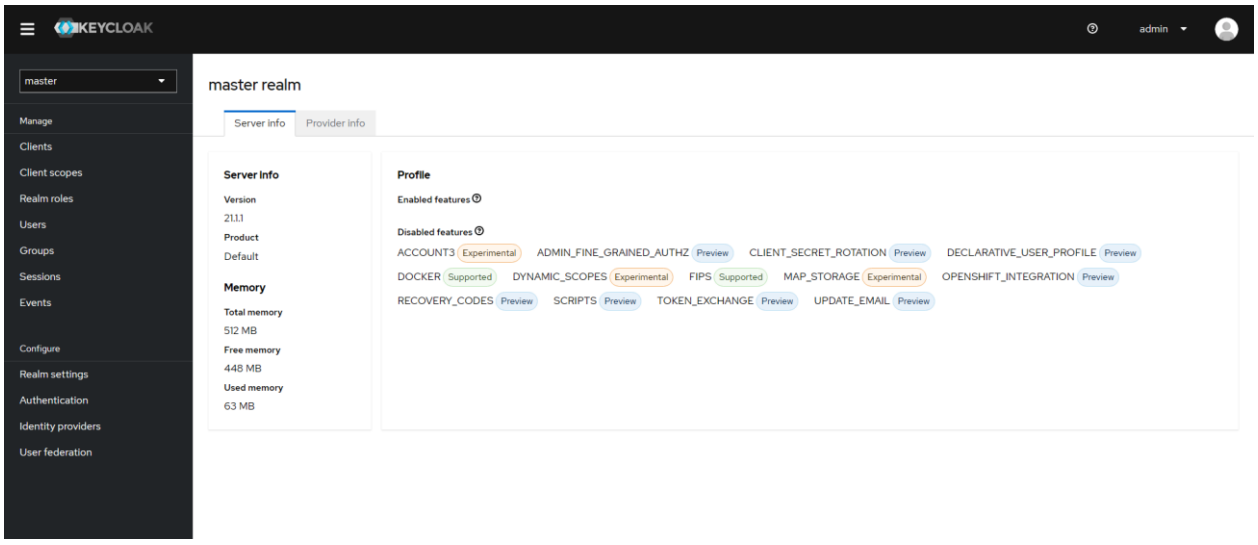

Рис. 3.4 Адміністративна панель

Після входу до адміністративної панелі, можна перейти до налаштування системи, за допомогою наступних налаштувань можна захистити систему від несанкціонованого доступу та виявляти Cyber Surveillance.

Існує певний алгоритм для налаштування системи. Алгоритм є свого роду методичною рекомендацією для стандартного розгортання. IAM Keycloak є дуже комплексним інструментом з багатоцільовим застосуванням, тому в даному дослідженні увага зосереджена на його базовому розгортанні та налашутванні, а далі, з інформації отриманої з цього дослідження, спеціаліст може легко масштабувати або змінювати конфігурацію під себе.

Отже, цей алгоритм можна розбити на чотири умовних кроки, які в свою чергу мають підкроки:

Крок 1: Налаштування аутентифікації і авторизації в Keycloak

У першому кроці потрібно налаштувати автентифікацію та авторизацію в Keycloak для системи. Це включає налаштування різних механізмів автентифікації, таких як паролі, одноразові паролі, двофакторна аутентифікація і т. д. Також потрібно визначити ролі та права доступу для користувачів.

Крок 2: Встановлення політик авторизації

Використовуючи Keycloak, потрібно встановити детальні політики авторизації для кожного ресурсу в системі. Це включає в себе визначення дозволів, областей, обмежень доступу та умов, які впливають на авторизаційні рішення.

Крок 3: Виявлення підозрілих активностей

Keycloak також надає можливості для виявлення підозрілих активностей в системі. Це може включати виявлення незвичайних спроб входу, спроб доступу до недозволених ресурсів, надмірну активність тощо. Ви можете використовувати журнали подій Keycloak та механізми аналізу журналів для виявлення таких підозрілих активностей.

Крок 4: Моніторинг та оновлення

Важливим етапом є моніторинг системи та оновлення політик авторизації на основі нових вимог та виявлених загроз. Слід систематично аналізувати журнали подій, моніторити активність користувачів та вчасно реагувати на будь-які небажані або підозрілі активності.

Отже, перший крок - це Налаштування аутентифікації і авторизації в Keycloak. Даний процес в свою чергу можна розбити на такі підкроки:

Крок 1: Створення Realm

Перший крок - створення Realm в Keycloak.

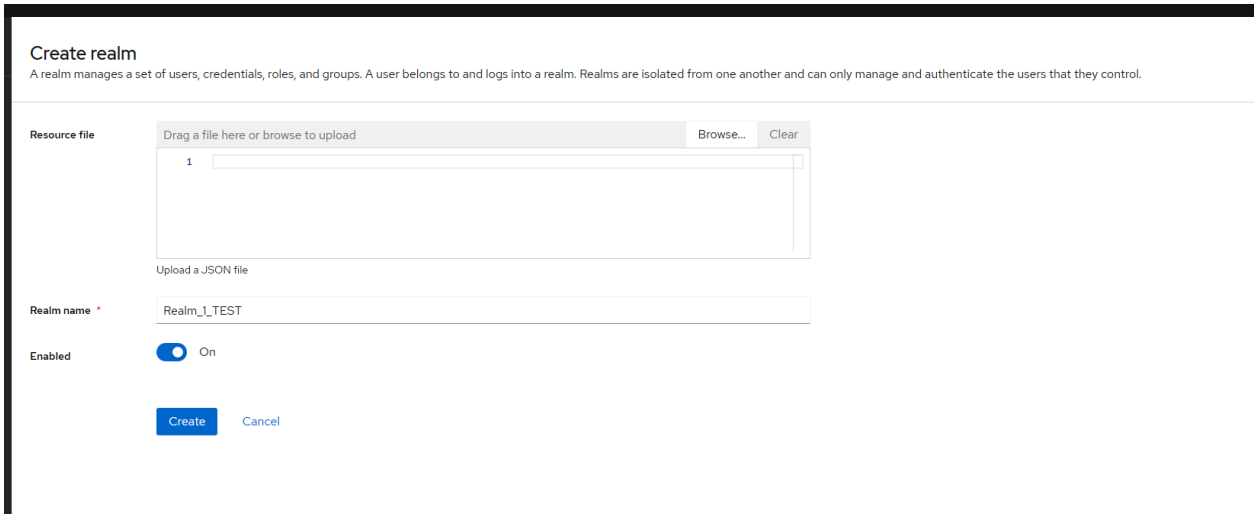

Рис. 3.5 Створення Realmy

Крок 2: Додавання користувачів

Другий крок - додавання користувачів для Realmy. Це саме ті користувачі, які будуть проходити процес аутентифікації та авторизації за предвстановленими параметрами.

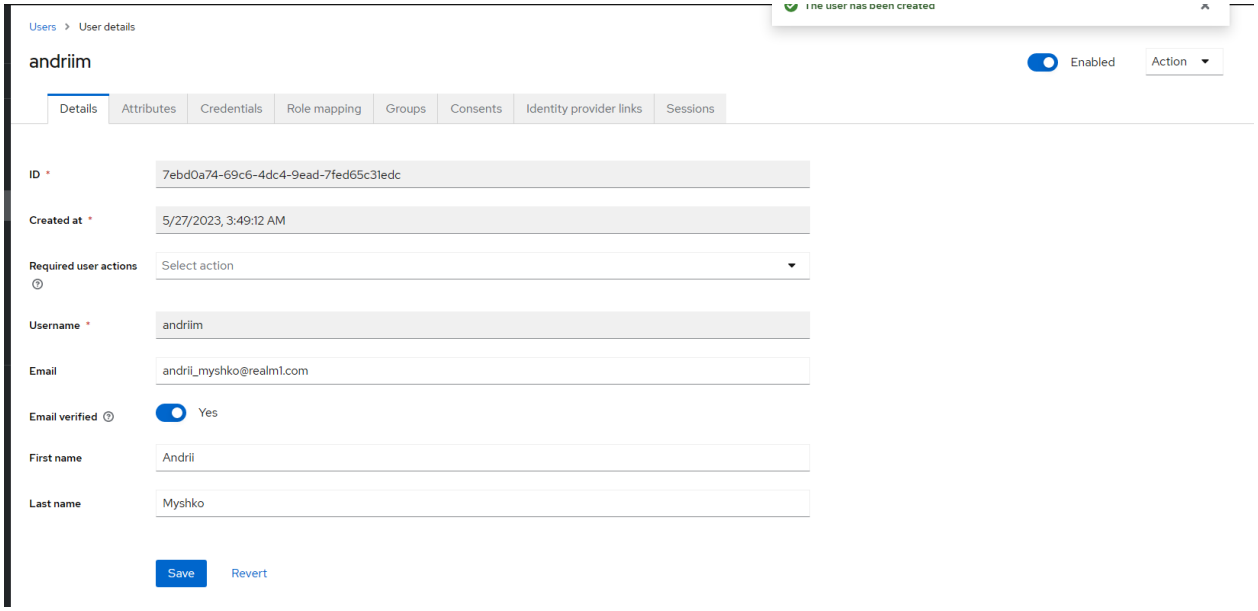

Рис. 3.6 Створення користувача

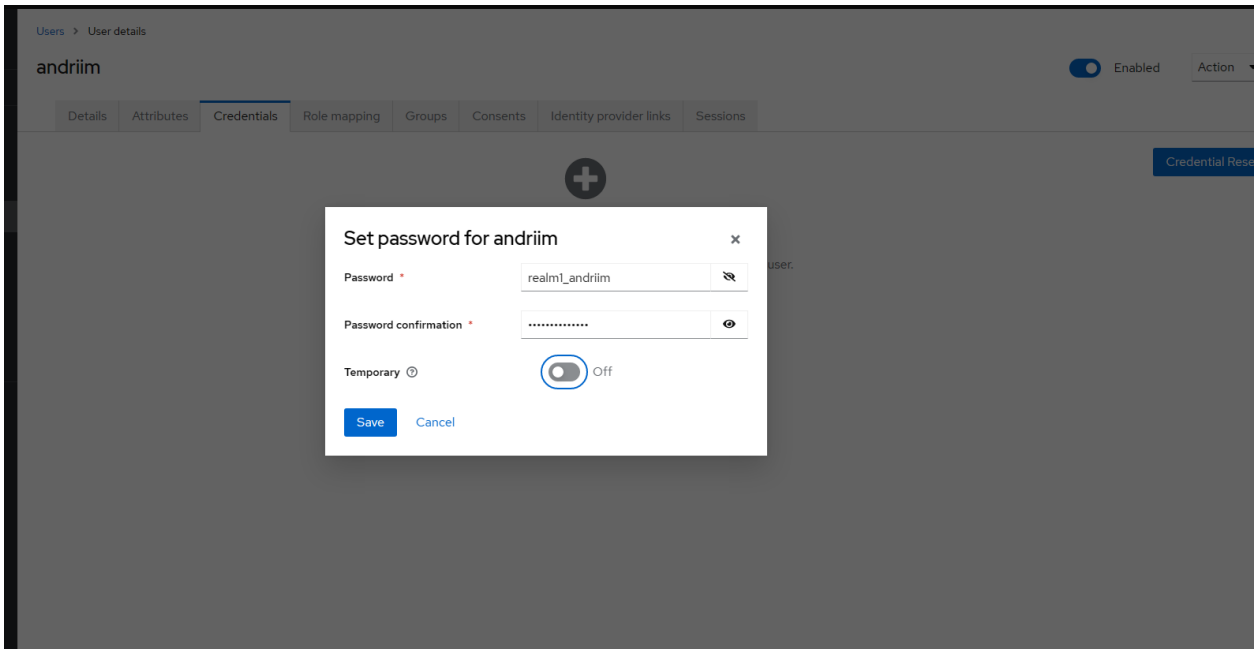

Рис. 3.7 Встановлення паролю для користувача

Після створення користувача/ів, можна перейти до наступного кроку та розподілити ролі та права доступу серед користувачів.

Крок 3: Визначення ролей та прав доступу

Третій крок - встановлення ролей та прав доступу для конкретних користувачів.

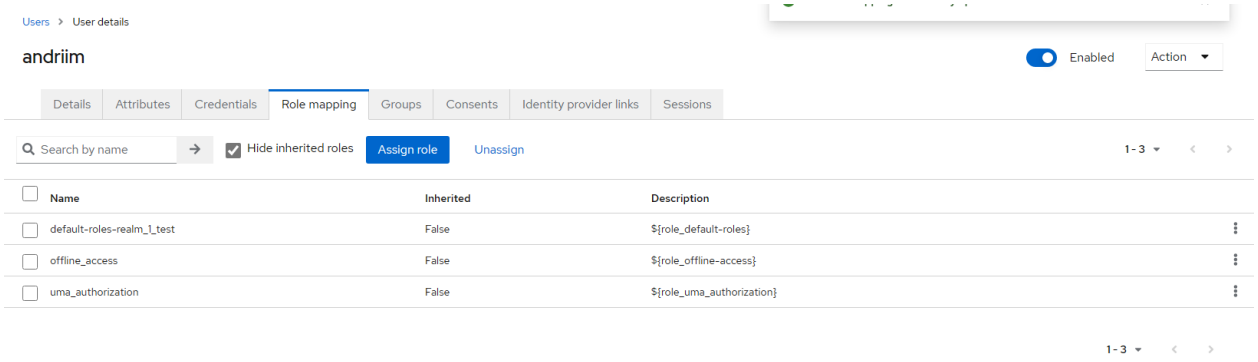

Рис. 3.8 Назначення ролей для конкретного користувача (в даному випадку назначена “default role”, яка дозволяє доступ до всього контенту Realmy, але не до адміністративних ресурсів/панелей.

Ролі дозволяють групувати користувачів за функціональністю або рівнем доступу, а права доступу визначають, які ресурси або операції можуть виконувати користувачі з конкретною роллю. Після цього кроку можна перейти до четвертого кроку, а саме налаштування клієнтів [6-10].

Крок 4: Налаштування клієнтів

Четвертий крок - налаштування клієнтів. Клієнти - це саме ті ресурси (програми/сервіси/сервіси API/Web-додатки, тощо.), які використовують Keycloak для аутентифікації та авторизації. В Keycloak можна налаштовувати клієнти, визначаючи їхні URL, налаштування безпеки, типи аутентифікації та авторизації, дозволені ролі та обмеження доступу. При налаштуванні клієнтів, Keycloak автоматично використовує HTTPS з'єднання, що гарантує цілісність та конфіденційність інформації.

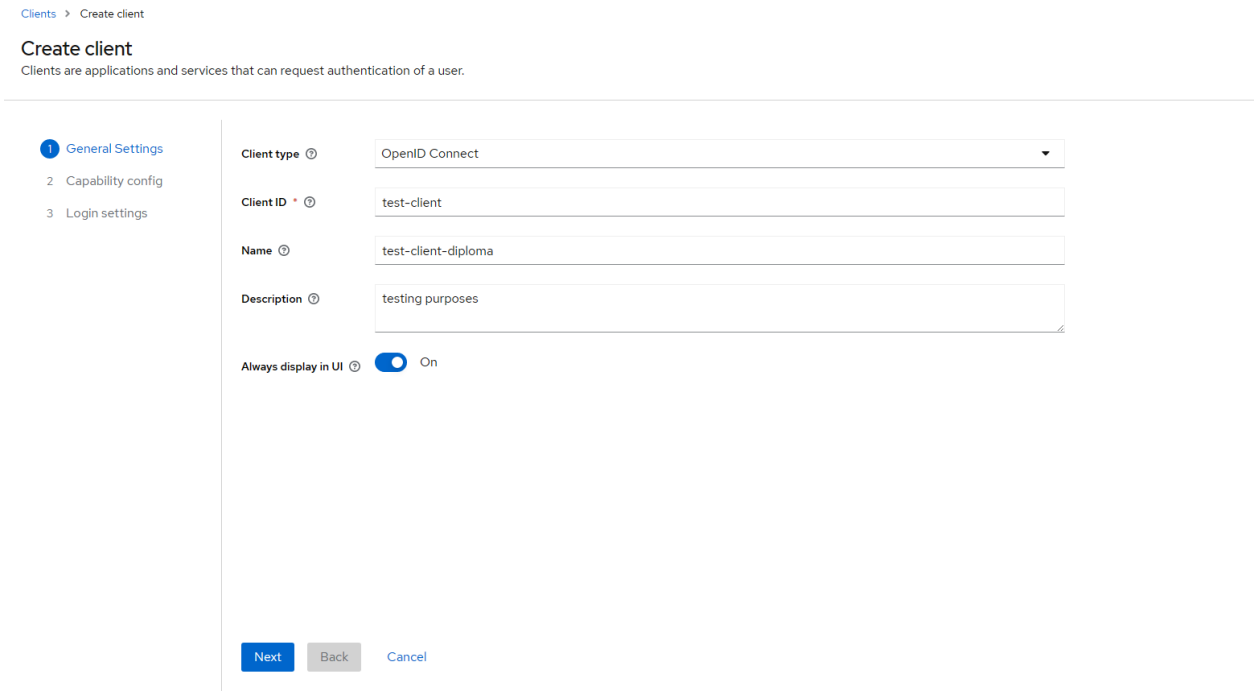

Рис. 3.9 Створення клієнту

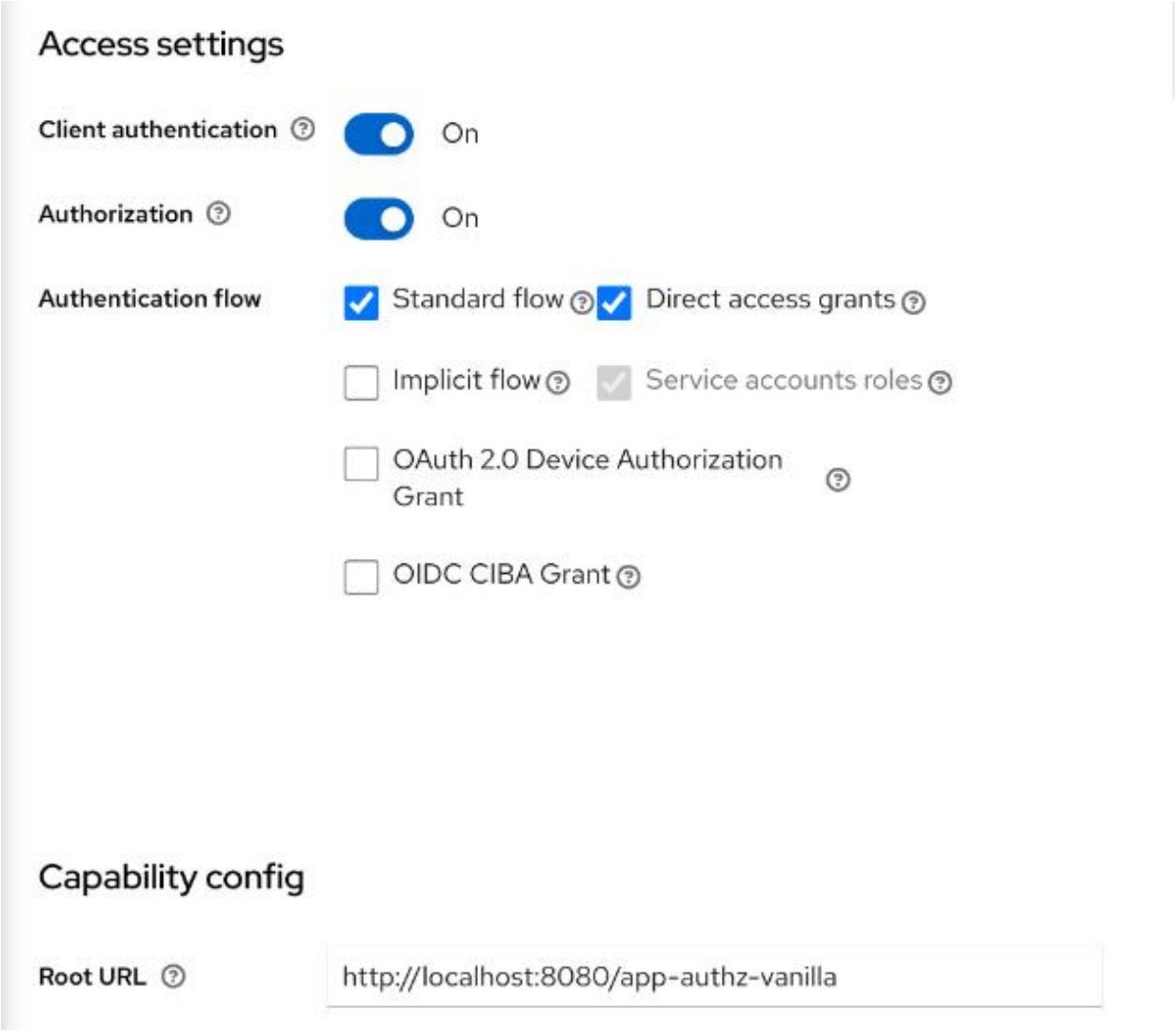

Рис. 3.10 Створення клієнту, ввімкнення аутентифікації та авторизації за протоколом OpenID Connect для уникнення публічного доступу до клієнту

Після створення клієнту можна переходити до наступного кроку.

Отже, після стартового налаштування та визначення головних суб'єктів та об'єктів системи, можна переходити до наступного, другого глобального кроку, а саме до встановлення політик/потоків авторизації:

Крок 1: Налаштування потоків аутентифікації

Keycloak надає різні потоки аутентифікації, які використовуються для перевірки ідентичності користувачів. Послідовність дій, які користувач або служба повинні виконати для автентифікації, в Keycloak називається потоком

автентифікації. Можна налаштувати потоки аутентифікації в Keycloak відповідно до вимог безпеки і встановити послідовність кроків аутентифікації. Зв'язок між Keycloak і клієнтами, які запитують у нього послуги аутентифікації, відбувається відповідно до одного з двох основних підтримуваних протоколів єдиного входу (SSO): OpenID Connect і SAML.

OpenID Connect (OIDC) є кращим методом. Це сучасний протокол, побудований на основі фреймворку OAuth 2.0. SAML - це старіший протокол аутентифікації, який завоював популярність у світі SOAP-сервісів. Він спирається на XML-документи, що містять твердження про користувача, тоді як OIDC використовує JWT (JSON Web Token) у вигляді ідентифікаційних токенів та маркерів доступу.

Формалізуючи концепції, стандартизований фреймворк OAuth 2.0, OIDC визначає чотири основні потоки, які можуть бути використані для аутентифікації користувача:

1. Потік коду авторизації для браузерних додатків, таких як SPA (Single Page Applications) або серверних додатків;
2. Implicit Flow для браузерних додатків, менш безпечний, ніж попередній, не рекомендований і застарілий в OAuth 2.1;
3. Client Credentials Grant, як і веб-сервіси, він передбачає зберігання секрету, тому клієнт повинен бути надійним;
4. Resource Owner Password Credentials Grant для клієнтів REST, таких як інтерфейси до мейнфреймів та інших застарілих систем, які не можуть підтримувати сучасні протоколи автентифікації, це передбачає обмін обліковими даними з іншою службою, це застарілий метод, тому з ним потрібно бути обережним.

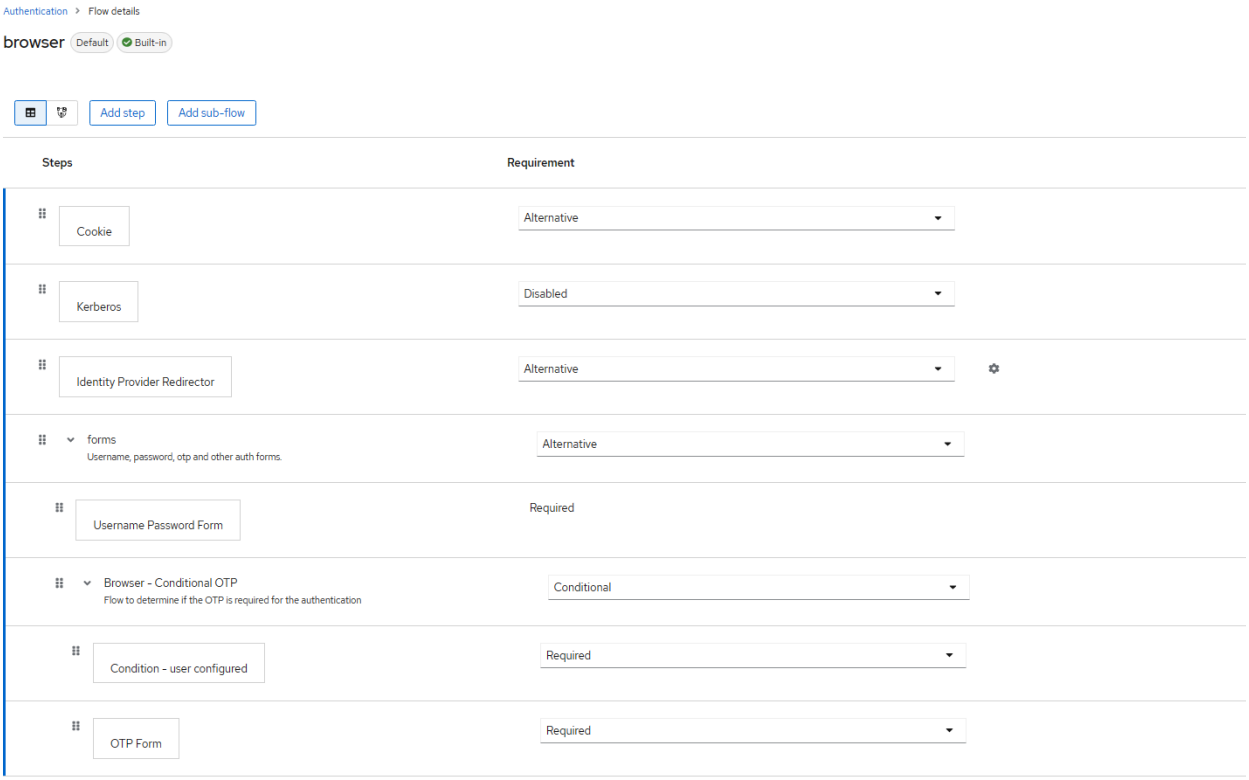

Рис. 3.11 Інтерфейс потоків аутентифікації

Так як мій клієнт є веб-додатком, то для нього застосовується правила “browser flow”, інтерфейс інтуїтивний, тут можна додавати або прибирати потрібні для процесу успішної аутентифікації кроки, що дозволить більш точно контролювати критичні ресурси/клієнти.

Крок 2: Конфігурація прав доступу

Одним з важливих етапів є налаштування прав доступу до ресурсів та застосунків. В даному кроці потрібно визначити ресурси, які потребують авторизації, встановити політики доступу до цих ресурсів та зв'язати їх з ролями користувачів.

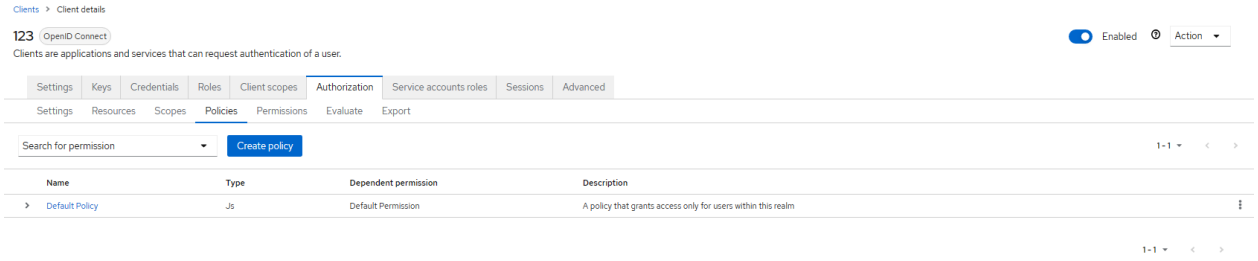

Рис. 3.12 Інтерфейс управління політиками доступу

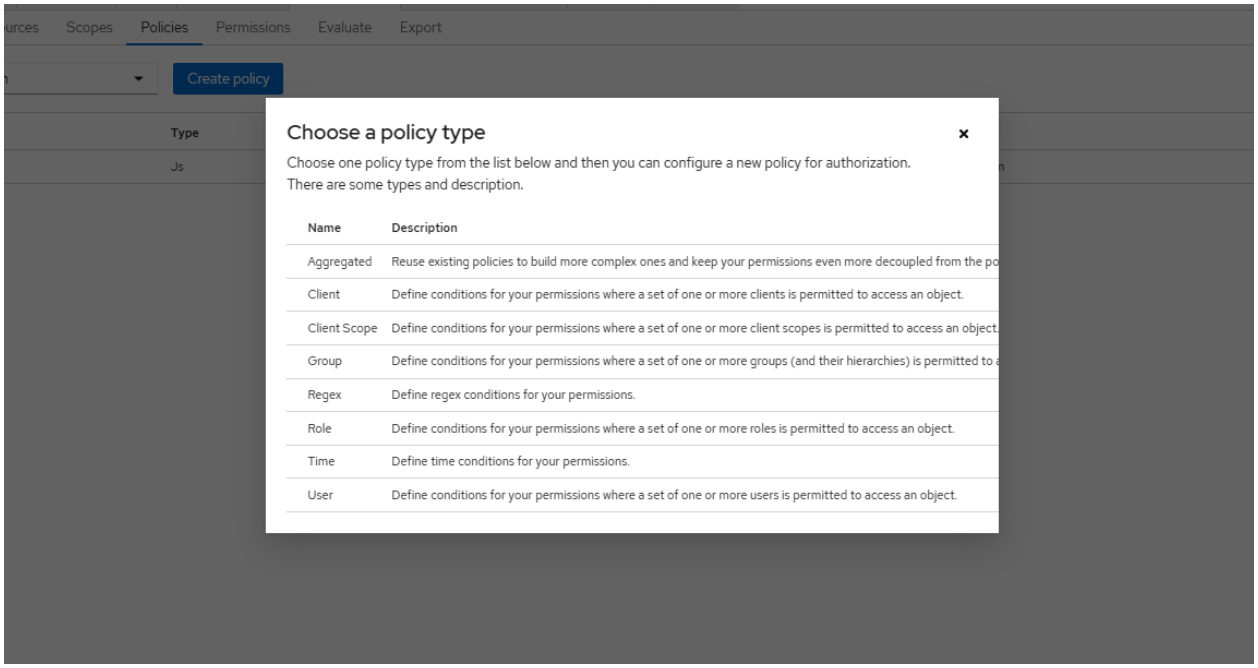

Рис. 3.13 Інтерфейс вибору потрібної політики

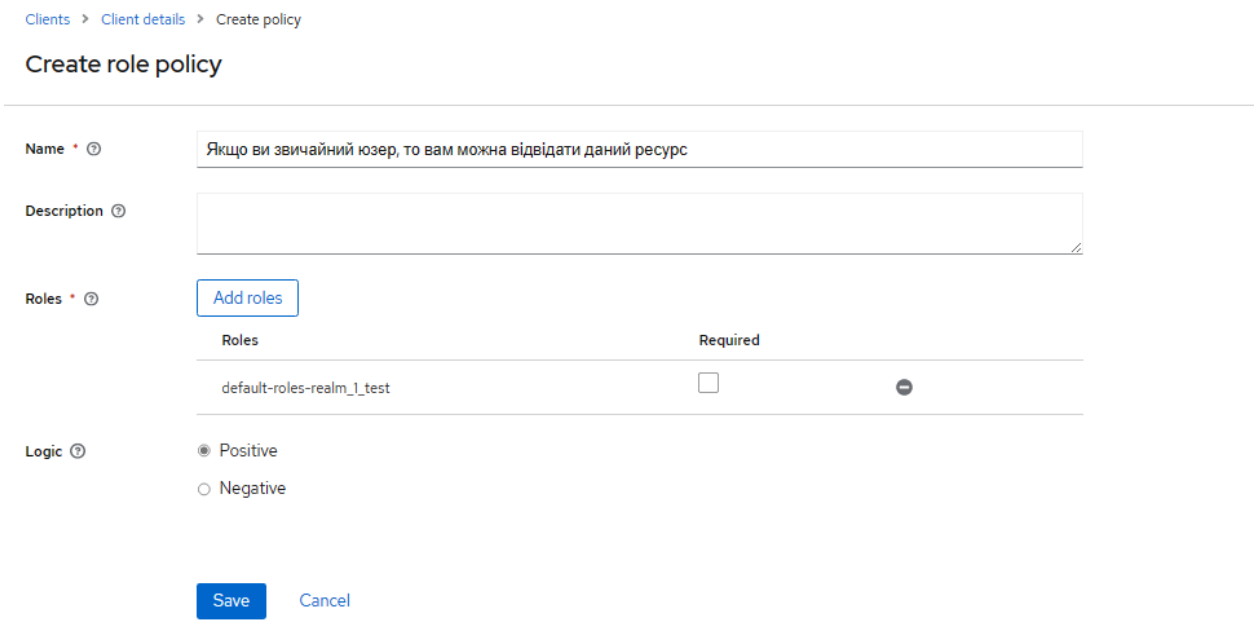

Рис. 3.14 Створення ролі

Для простої демонстрації - було створено політику доступу, за якою користувач отримає доступ до клієнту, якщо він входить в потрібну групу, в даному випадку “default-roles-Realm_1_test”, “Logic” відповідає за спрацювання Keycloak на відповідний сигнал, в даному випадку, якщо “Positive”, тобто роль користувача збігається з потрібною - користувач отримує доступ до ресурсу. Тобто був використаний метод Role-based access control (RBAC) [3-9].

Крок 3: Створення політик Realmy

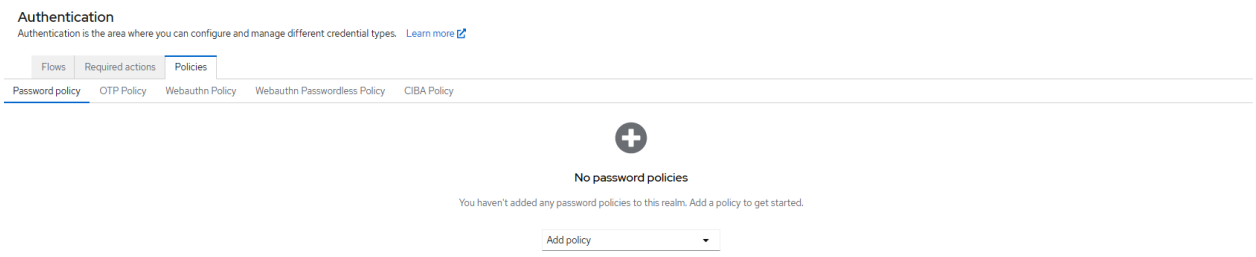

Рис. 3.15 Демонстрація вікна політик

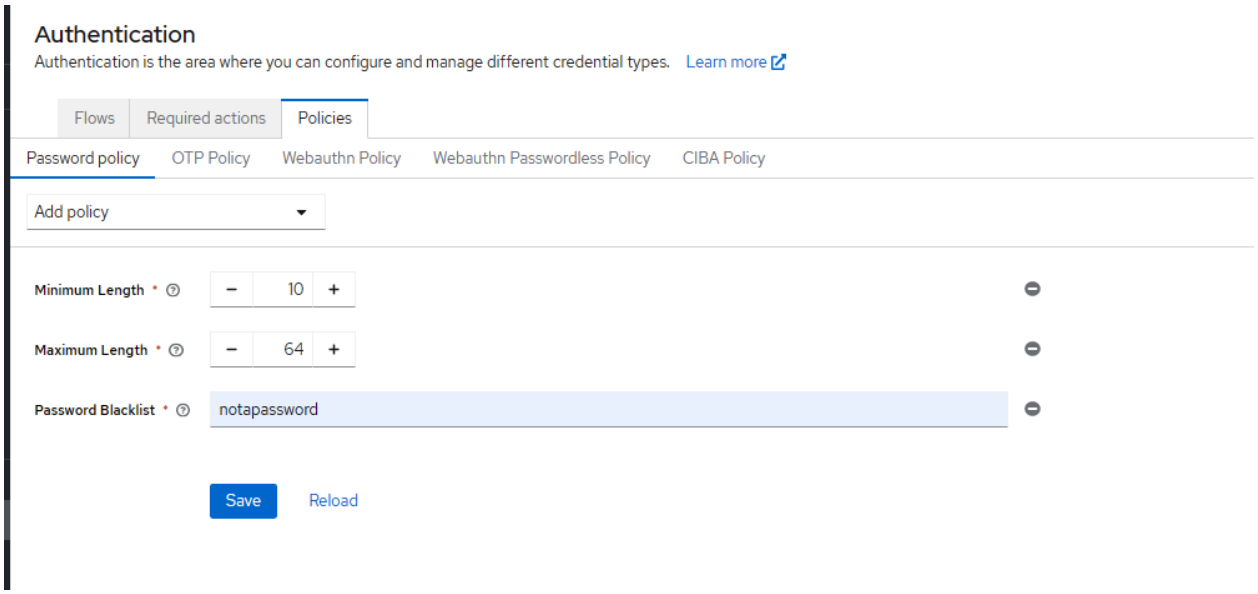

Рис. 3.16 Демонстрація створення політики для паролів, в даному випадку пароль може бути мінімум від 10 символів, та максимум 64, а також була створена заборона на конкретний набір символів “notapassword”.

Після конфігурації політик аутентифікації та авторизації можна переходити до третього кроку, а саме виявлення підозрілих активностей.

Логування подій є важливою частиною виявлення Cyber Surveillance, на щастя Keycloak має вбудований функціонал логування, за допомогою якого, спеціалісти можуть аналізувати стан системи, або виявляти підозрілі дії та небажаний доступу до тих чи інших клієнтів. В третьому кроці я хочу розглянути конфігурацію Keycloak для запуску логування.

Крок 1: Ввімкнення логування подій

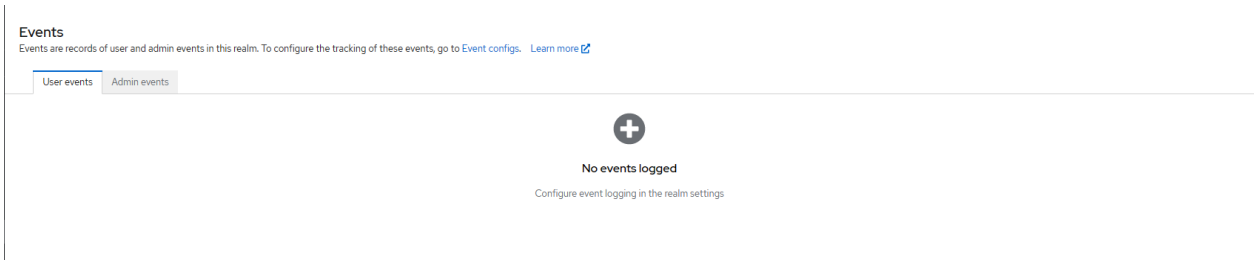

Рис. 3.17 Вікно логу подій

За замовчуванням для параметра "Зберегти події" встановлено значення OFF. Це робиться для того, щоб адміністратор вирішив сам, які події потрібно логувати.Тому зараз потрібно ввімкнути логування у налаштуваннях Realmy.

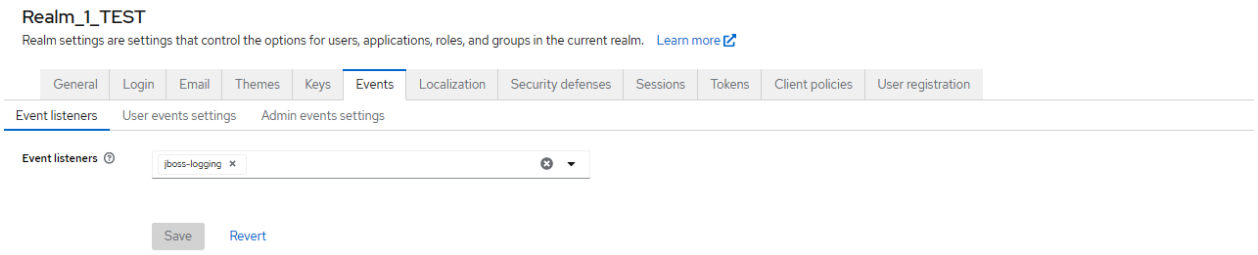

Рис. 3.18 Налаштування логування

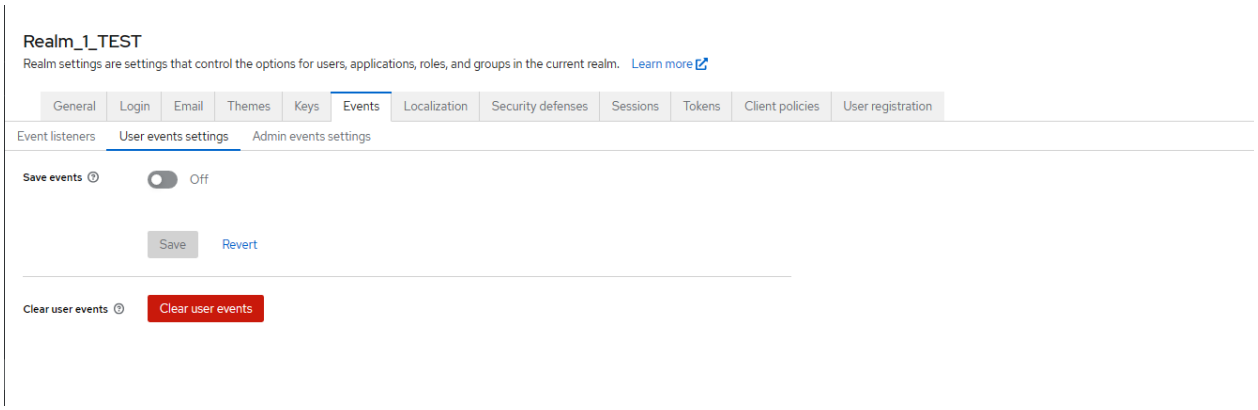

Рис. 3.19 Налаштування логування

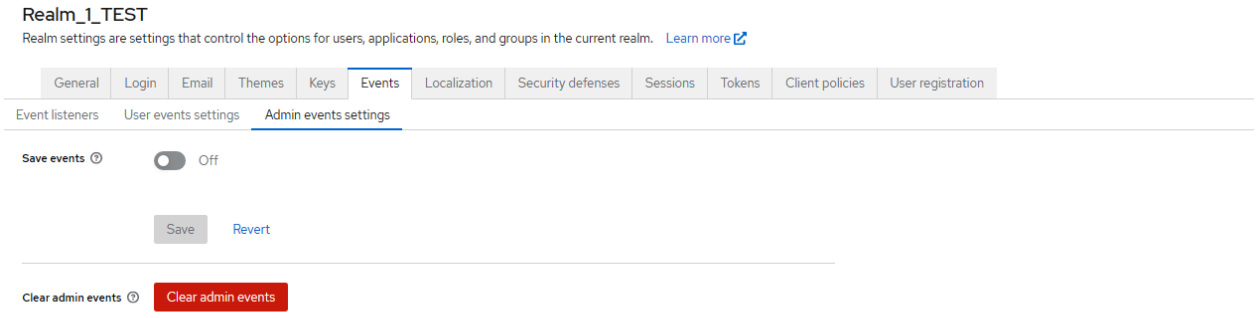

Рис. 3.20 - Налаштування логування

Після увімкнення логування, Keycloak буде реєструвати події, пов'язані з аутентифікацією, авторизацією, створенням користувачів та іншими діями, що відбуваються в системі. Спеціалісти можуть аналізувати журнали подій для виявлення підозрілих активностей або використовувати їх для аудиту та моніторингу безпеки системи.

Увімкнення логування також може вплинути на продуктивність системи, тому рекомендується обирати рівень логування з урахуванням потреб і обсягу даних, що будуть зберігатися в журналах.

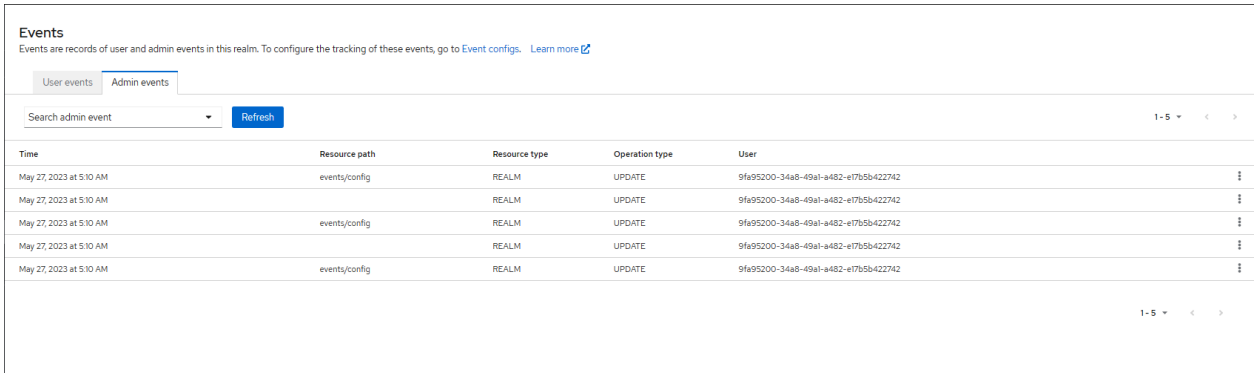

Рис. 3.21 - Демонстрація працездатності логування Keycloak

Основні події:

Login - Користувач увійшов в систему.

Register - Користувач зареєстрований.

Exit- Користувач вийшов з системи.

Code to Token - Додаток/клієнт обміняв код на токен.

Refresh Token - Додаток/клієнт оновив токен.

Події облікового запису:

Social Link - Обліковий запис був пов'язаний зі соціальним постачальником.

Remove Social Link - Соціальний постачальник був видалений з облікового запису.

Update Email - Адреса електронної пошти для облікового запису змінилася.

Update Profile - Профіль для облікового запису змінився.

Send Password Reset - Було надіслано лист для скидання пароля.

Update Password - Пароль для облікового запису змінився.

Update TOTP - Налаштування TOTP для облікового запису змінилися.

Remove TOTP - TOTP був видалений з облікового запису.

Send Verify Email - Було надіслано лист для підтвердження адреси електронної пошти.

Verify Email - Адреса електронної пошти для облікового запису була підтверджена.

Для всіх подій є відповідна подія помилки.

Після всіх виконаних кроків, система може вважатись достатньо захищеною, але є ще один, четвертий, напевно один із самих важливих кроків, який потрібно виконувати на постійній основі - Моніторинг та оновлення. Моніторинг і оновлення Keycloak є важливими аспектами забезпечення безпеки і ефективної роботи системи.

Кілька рекомендацій щодо моніторингу та оновлення Keycloak:

– Використання моніторингових інструментів, таких як системи моніторингу метрик і журналів, для відстеження працездатності Keycloak. Слід регулярно перевіряти метрики процесора, пам'яті, мережі та інших ресурсів, щоб виявити будь-які проблеми або аномалії.

– Регулярний аналіз журналів подій Keycloak, щоб виявити підозрілі або ненормальні активності. Можливі ознаки зловмисницької діяльності, такі як спроби неуспішної аутентифікації, незвичайні запити або надмірне навантаження на систему.

Оновлення:

– Регулярна еревірка наявності оновлень для Keycloak. Оновлення часто включають виправлення помилок, покращення безпеки та нові функції.

– Перед оновленням - ретельне вивчення документації та вказівок з оновлення Keycloak. Резервне копіювання конфігураційних файлів та бази даних перед початком процесу оновлення це важливо.

– Потрібно переконайтеся, що додатки та інтеграції з Keycloak сумісні з новою версією.

– Проведення тестування оновлення на тестовому середовищі перед його застосуванням до продакшн середовища. Це дозволить виявити можливі проблеми чи несправності після оновлення.

Важливо мати систему моніторингу та регулярно оновлювати Keycloak, щоб забезпечити безпеку та ефективну роботу системи аутентифікації та авторизації.

Після зазначених налаштувань, можна переглянути як Keycloak працює:

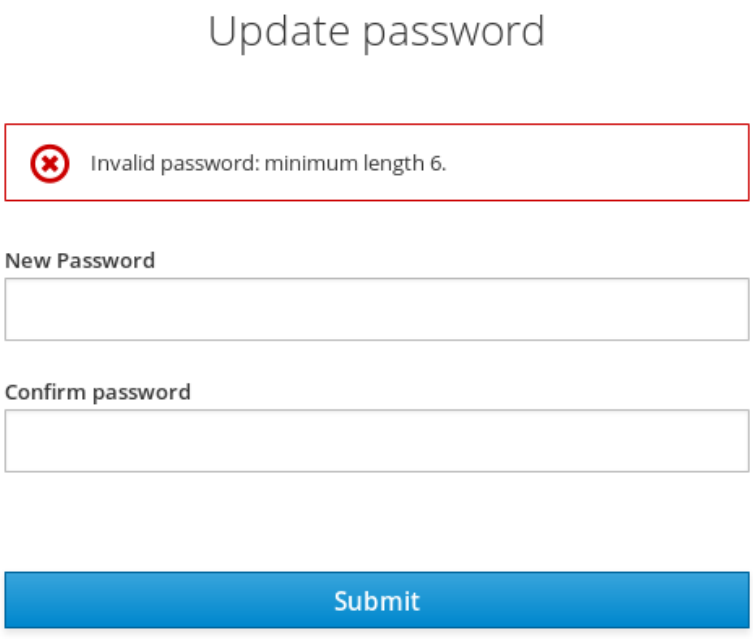

Рис. 3.22 Після налаштування політик паролів Keycloak буде вимагати зазначені параметри для паролів

Рис. 3.23 Працездатність аутентифікації

Рис. 3.24 Працездатність аутентифікації після налаштування

Event Type	Details
CODE_TO_TOKEN	Client: security-admin-console User: 5e073544-a49b-45c5-bff2-a43679d4a4e9 IP Address: 127.0.0.1 Details: +
LOGIN	Client: security-admin-console User: 5e073544-a49b-45c5-bff2-a43679d4a4e9 IP Address: 127.0.0.1 Details: +
LOGOUT	Client: User: 5e073544-a49b-45c5-bff2-a43679d4a4e9 IP Address: 127.0.0.1 Details: +

Рис. 3.25 Лог логіну та виходу з клієнту

Whitelabel Error Page

Tue Mar 17 14:49:16 UTC
There was an unexpected error (type=Forbidden, status=403).
No message available

Рис. 3.26 Сторінка помилки при відхиленні процесу аутентифікації

3.3 Розробка рекомендацій щодо використання Keycloak для виявлення та запобігання Cyber Surveillance

Отже на основі вище вказаної інформації, після опису процесів роботи Keycloak та після огляду його технічних можливостей розроблено наступні рекомендації щодо виявлення та запобігання Cyber Surveillance за допомогою Keycloak:

- Налаштування сильної аутентифікації це важливо. Використовуйте багатофакторну аутентифікацію для підвищення рівня безпеки. Вимагайте використання додаткових чинників, таких як одноразові паролі або біометричні дані, для підтвердження ідентичності користувача.
- Вимагайте від користувачів використовувати сильні паролі, що складаються з комбінації великих і малих літер, цифр та спеціальних символів. Встановлюйте політики безпеки щодо мінімальної довжини паролю та періодично змінюйте їх, або також сконфігуруйте додаткову політику, яка буде давати тимчасові паролі, по закінченню терміну дії яких будуть генеруватись нові.
- Використовуйте можливості Keycloak для точного визначення ролей і надання прав доступу. Встановлюйте строгі правила доступу до ресурсів системи, щоб обмежити привілеї користувачів тільки необхідними функціями та даними.
- Обов’язково ввімкніть журналювання та моніторинг активності користувачів, щоб виявляти підозрілу або незвичайну поведінку. Аналізуйте журнали, виявляйте спроби несанкціонованого доступу, надмірну активність або зміну звичних патернів використання системи.
- Подбайте про шифрування даних. Застосовуйте шифрування для захисту конфіденційної інформації, що зберігається в системі. Використовуйте механізми шифрування для захисту паролів, токенів доступу та інших чутливих даних в пам'яті системи і під час передачі через мережу.
- Регулярні оновлення. Регулярно оновлюйте Keycloak до останніх версій та встановлюйте виправлення для виявлених вразливостей. Слідкуйте за

офіційними повідомленнями та вразливостями, щоб швидко впроваджувати необхідні заходи безпеки.

- Проводьте навчання та тренінги серед персоналу та користувачів про загрози Cyber Surveillance, методи соціальної інженерії та крадіжки ідентифікаційних даних. Підвищення обізнаності користувачів допоможе уникнути потенційних атак та збільшити рівень безпеки системи загалом.

Висновок до розділу 3

В даному розділі було проведено дослідження технічних можливостей IAM Keycloak, включаючи його розгортання та налаштування. Практично було продемонстровано ефективність та функціональність цієї системи, що дає змогу впевнено рекомендувати його використання для запобігання та виявлення Cyber Surveillance.

ВИСНОВКИ

За результатами даної роботи була розроблена серія рекомендацій щодо виявлення та запобігання Cyber Surveillance за допомогою Identity and Access Management (IAM) Keycloak. Під час дослідження були розглянуті технічні аспекти роботи цієї системи, а також проведений огляд потенційних загроз Cyber Surveillance.

Виявлено, що Keycloak має значний потенціал у боротьбі з різними формами Cyber Surveillance, такими як відстеження даних, вторгнення в приватне життя, масовий нагляд, цензура та обмеження доступу, соціальна інженерія та крадіжка ідентифікаційних даних.

Рекомендації, що були розроблені, охоплюють кілька аспектів безпеки. Вони включають налаштування сильної аутентифікації, встановлення правил паролів, керування ролями і дозволами, моніторинг активності користувачів, шифрування даних, оновлення та патчі, а також навчання користувачів щодо Cyber Surveillance.

Ці рекомендації дозволять організаціям ефективно використовувати Keycloak для забезпечення високого рівня безпеки та захисту від загроз Cyber Surveillance. Важливо враховувати, що безпека є постійним процесом, і рекомендації повинні бути використані разом з іншими заходами безпеки для створення надійної системи безпеки.

Розроблені рекомендації є цінним доповненням до багатофункціональної системи Keycloak і можуть служити як основа для розробки стратегій виявлення та запобігання Cyber Surveillance. Їх впровадження допоможе організаціям забезпечити високий рівень безпеки та захисту персональних даних у сучасному цифровому середовищі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Keycloak Офіційний веб-сайт URL: www.keycloak.org (дата звернення: 21.03. 2023).

2. Keycloak Authentication Flows, SSO Protocols and Client Configuration URL: Keycloak Authentication Flows, SSO Protocols and Client Configuration (thomasvitale.com) (дата звернення: 21.03. 2023).

3. Keycloak Documentation URL: wjw465150.gitbooks.io (дата звернення: 21.03. 2023).

4. A deep dive into Keycloak | TechTalk URL: https://www.youtube.com/watch?v=ZxpY_zZ52kU (дата звернення: 21.03. 2023).

5. Keycloak Advanced Scenarios URL: developers.redhat.com (дата звернення: 21.03. 2023).

6. Writing Keycloak extensions: Key concepts and anti-patterns URL: https://www.zone2.tech/blog/writing-keycloak-extensions-key-concepts-and-anti-patterns (дата звернення: 21.03. 2023).

7. What is the difference between Picketlink and Keycloak? | Planet JBoss Developer URL: https://web.archive.org/web/20170405213148/http://planet.jboss.org/post/what_is_the_difference_between_picketlink_and_keycloak (дата звернення: 21.03. 2023).

8. Thorgersen, Pedro Igor Silva, Keycloak - Identity and Access Management for Modern Applications, 2021, Packt Publishing

9. Resources, scopes, permissions and policies in Keycloak URL: https://stackoverflow.com/questions/42186537/resources-scopes-permissions-and-policies-in-keycloak (дата звернення: 21.03. 2023).

10. Ertem Osmanoglu, Identity and Access Management: Business Performance Through Connected Intelligence, 2013, Syngress; 1st edition

11. Omondi Orondo PhD, Identity & Access Management: A Systems Engineering Approach, 2014, CreateSpace Independent Publishing Platform; 1st edition

12. Michael E. Whitman, Herbert J. Mattord, Management of Information Security, 2018, Cengage Learning; 6th edition

ДЕМОНАСТРАЦІЙНІ МАТЕРІАЛИ
(Презентація)