ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА НА БАЗІ ORACLE IDENTITY AND ACCESS MANAGEMENT»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Єрмак М.В.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 77 сторінок, 43 рисунків, 19 джерел.

Об'єкт дослідження – процес забезпечення управління ідентифікацією та доступом до корпоративної інформаційної системи.

Предмет дослідження – технологія управління ідентифікацією та доступом до корпоративної інформаційної системи.

Мета роботи – розробити варіант топології системи управління ідентифікацією та доступом до корпоративної інформаційної системи та рекомендації щодо застосування технології на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління захистом кінцевих точок корпоративної інформаційної системи.

В роботі проведено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено мету та завдання ідентифікації та управління доступом до корпоративної інформаційної системи. Проаналізовано існуючі технології управління ідентифікацією та доступом до корпоративної інформаційної системи.

Досліджено методи та засоби управління ідентифікацією та доступом на прикладі рішення Oracle Identity and Access Management. Визначено призначення, основні функції та склад програмного комплексу Oracle Identity and Access Management. Визначено призначення, основні функції та принципи роботи рішень Oracle Identity and Access Management.

На основі досліджень проведених в роботі розроблено варіант топології системи управління ідентифікацією та доступом до корпоративної інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Галузь використання – кібербезпека корпоративної інформаційної системи.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ІДЕНТИЦІКАЦІЯ ТА УПРАВЛІННЯ ДОСТУПОМ, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ІДЕНТИЦІКАЦІЄЮ ТА ДОСТУПОМ, ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИЦІКАЦІЄЮ ТА ДОСТУПОМ

ABSTRACT

The text part of the master's work: 77 pages, 43 figures, 19 sources.

Object of research - the process of providing identification and access management to the corporate information system.

Subject of research - technology of management of identification and access to the corporate information system.

Purpose - to develop a variant of the topology of the identification and access management system to the corporate information system and recommendations for the use of technology in the enterprise.

Research methods - study of literature on the subject, analysis of operational documentation, international standards and their comparison, modeling the process of managing the protection of endpoints of the corporate information system.

The work analyzes the problem of ensuring cybersecurity of the corporate information system and defines the purpose and objectives of identifying and managing access to the corporate information system. The existing technologies of identification and access control to the corporate information system are analyzed.

The methods and means of identity and access management are investigated on the example of Oracle Identity and Access Management solution. The purpose, main functions and composition of the Oracle Identity and Access Management software package are determined. The purpose, main functions and principles of operation of Oracle Identity and Access Management solutions are determined.

Based on the research carried out in the work developed a variant of the topology of the identity and access management system to the corporate information system and recommendations for the use of technology to manage their protection in the enterprise.

Scope - cybersecurity of corporate information system.

CORPORATE INFORMATION SYSTEM, CYBERSECURITY, IDENTIFICATION AND ACCESS MANAGEMENT, METHODS AND MEANS OF IDENTIFICATION AND ACCESS MANAGEMENT, IDENTIFICATION AND ACCESS MANAGEMENT TECHNOLOGY

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ…….. 9

ВСТУП ……..……. 10

1 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ……. 13

1.1. Сучасні технології захисту підприємства…..……..……. 13
1.2. Методи та технології забезпечення інформаційної безпеки…….. 17
1.3. Порівняння систем управління ідентифікацією та доступом (IAM)…… 23

2 АРХІТЕКТУРА ТА КОМПОНЕНТИ ДЛЯ РІШЕННЯ ORACLE IDENTITY MANAGEMENT…….…….…….. 36

2.1. Oracle Internet Directory…….…….. 36
2.2. Oracle Identity Manager Architecture……... 38
2.3. Data Base of Enterprise User Security…..…… 41
2.4. Oracle Authentication Services for Operation Systems..... 42
2.5. Oracle Directory Integration Platform …….. 44

3 РОЗРОБКА ВАРІАНТУ РІШЕННЯ ORACLE IDENTITY MANAGEMENT 50

3.1. Розробка варіанта налаштування рішення oracle identity management……..……..…. 50
3.2. Рекомендації фахівціям з кібербезпеки щодо управління ідентифікаціїєю та до ступом користувачів до інформаційної системи 74

ВИСНОВКИ…….. 76

ПЕРЕЛІК ПОСИЛАНЬ..... 77

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 78

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Єрмака Максима Володимировича
на тему: «Технологія управління ідентифікацією та доступом користувачів інформаційної системи підприємства на базі Oracle Identity and Access Management»

Актуальність:
Управління доступом та ідентифікацією користувачів корпоративної інформаційної системи стає все більш складним у зв'язку зі зростаючим числом користувачів інформаційних технологій. Технологія управління ідентифікацією та доступом користувачів (Identity and Access Management, IAM) є комплексним підходом для управління доступом в організації з єдиної консолі. Реалізація технології управління доступом та ідентифікацією користувачів створює умови забезпечення багатьох сучасних функцій безпеки. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:
1. На основі проведеного аналізу, в роботі встановлено зміст проблеми в ідентифікації та управлінні обліковими записами, визначено мета та завдання управління ідентифікацією та доступом до корпоративної інформаційної системи.
2. Досліджено методи та засоби управління ідентифікацією та доступом до корпоративної інформаційної системи на базі рішення Oracle Identity and Access Management.
3. Запропоновано варіант технології застосування системи управління ідентифікацією та доступом до корпоративної інформаційної системи на базі рішення Oracle Identity and Access Management та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно та послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:
1. У магістерській роботі бажано було б провести саме порівняльний аналіз рішень IAM системи різних виробників, виявити позитивні та негативні сторони рішень.
2. Запропонований варіант топології системи управління ідентифікацією та доступом до корпоративної інформаційної системи на базі рішення Oracle Identity and Access Management не є достатньо показовим на практиці.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку «**відмінно»**, а студент **Єрмак Максим Володимирович** - присвоєння кваліфікації магістр 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 (_____)

_____

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

AD – Active Directory

AAD – Azure Active Directory

ACL - Access Control List

AWS – Amazon Web Services

BYOD – Bring Your Own device

LDAP - Lightweight Directory Access Protocol

IAM – Identity and Access Management

SAML - Security Assertion Markup Language

MFA – Multi-Factor Authentication

OID - Oracle Internet Directory

OUD – Oracle Unified Directory

ODSEE – Oracle Directory Server Enterprise Edition

DIP - Oracle Directory Integration Platform

ВСТУП

Актуальність дослідження. Шляхом до підвищення ефективності бізнес-процесів сучасного підприємства є впровадження та застосування інформаційних технологій. Підвищення технологічності бізнес-процесів підприємства обумовлює зростаюча кількість облікових записів, котрими мають користуватися працівники компанії та збільшена різноманітність електронних пристроїв для роботи.

Застосування мобільних пристроїв в мережах та інформаційних системах підприємства, а також впровадження системи управління ідентифікацією та обліковими записами веде до більш продуктивної та зручної роботи як працівників так і адміністраторів системи. Що виводить організацію на новий рівень безпеки та працездатності.

……

Вищенаведені аргументи актуалізують тему даної магістерської роботи, зміст якої становлять дослідження щодо технології управління ідентифікацією та доступом користувачів інформаційної системи підприємства на базі Oracle Identity and Access Management.

Об'єкт дослідження – процес забезпечення управління ідентифікацією та доступом користувачів.

Предмет дослідження – технологія ідентифікації та доступу користувачів.

Мета роботи – розробити варіант топології системи управління корпоративними обліковими записами та рекомендації щодо застосування технології управління ідентифікацією та доступом користувачів.

Наукові завдання:

дослідити сутність проблеми управління ідентифікацією та доступом користувачів;

встановити сутність завдань управління ідентифікацією та доступом

користувачів;

проаналізувати існуючі технології управління ідентифікацією та доступом користувачів;

проаналізувати методи та засоби управління ідентифікацією та доступом користувачів;

проаналізувати основні функції та принципи реалізації управління ідентифікацією та доступом користувачів.

розробити варіант рішення Oracle Identity Management.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи захисту корпоративних мобільних пристроїв.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо топології системи методів та засобів управління ідентифікацією та доступом на прикладі рішення Oracle Identity and Access Management.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ У СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

1.1. Сучасні технології захисту підприємства

Наразі існує безліч загроз, котрі можуть спровокувати збитки для підприємства. І не так важливо, чи то збитки будуть від прямих уражень, чи непрямі збитки, чи репутаційні. В будь-якому разі, компанія має враховувати усі існуючі загрози для неї. Відповідно до цих загроз має створюватися модель захисту підприємства.

Інформаційна загроза – це дії, які можуть порушити заданий стан захисту інформації, її доступність, цілісність або конфіденційність. Будь яке з цих порушень, або всі разом можуть нанести збитки. При цьому захист інформації – це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Законодавством України вноситься необхідність захисту персональних даних у вигляді інформації при їх обробці та побудови системи інформаційної безпеки відповідно до Статті 27 Закону України «Про інформацію».

За змістом всю інформацію можна поділити на декілька видів, по змісту [1]:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- інформація про стан довкілля (екологічна інформація);
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;

- правова інформація;
- статистична інформація;
- соціологічна інформація;
- критична технологічна інформація;

За міжнародним стандартом ISO/IEC 27000:2018 , у котрому зібрані найкращі практики та зазначені еталонні моделі забезпечення безпеки, зазначається, що організації всіх типів та розмірів, незалежно від виконуваних задач [3]:

1) збирають, обробляють, зберігають та передають інформацію;

2) усвідомлюють, що інформація та пов'язані з нею процеси, системи, мережі та персонал є важливими активами для досягнення цілей організації;

3) стикаються з низкою ризиків, які можуть впливати на функціонування активів;

4) вживають заходів щодо ймовірного впливу ризиків, впроваджуючи засоби управління інформаційною безпекою.

Вся інформація, що обробляється в організації піддається загрозам атак, помилок, негативних природних явищ (наприклад, повеней або пожеж) тощо, а також є об'єктом впливу вразливостей, пов'язаних з її використанням. Концепція інформаційної безпеки у своїй основі розглядає інформацію як актив, який представляє цінність, яка потребує відповідного захисту, наприклад, від втрати можливості застосування, конфіденційності та цілісності. Забезпечення можливості використання в потрібний момент точної та повної інформації тому, хто має відповідні потреби та права, сприяє ефективності бізнесу. Захист таких інформаційних активів за рахунок результативного визнання, досягнення, забезпечення та покращення інформаційної безпеки є суттєвим для здатності організації досягати своїх цілей, а також підтримки та покращення відповідності законодавчим вимогам та іміджу компанії. Ці скоординовані дії, що спрямовують виконання відповідних моделей управління та опрацьовують визнані неприпустимими інформаційні ризики, широко відомі як елементи менеджменту інформаційної безпеки.0

Також, в цьому стандарті зазначаються такі основоположні поняття для організації, як:

- управління доступом (access control) засоби, котрі мають гарантувати, що доступ до активів дозволено та обмежено відповідно до вимог бізнесу та безпеки;
- атака (attack) спроба знищити, розкрити, змінити, зробити недоступним, вкрасти чи отримати несанкціонований доступ або несанкціонованою використовувати актив;
- атрибут (attribute) властивість або характеристика об'єкта, відмінність якого кількісно чи якісно – від іншого може бути встановлена безпосередньо людиною або автоматизованими засобами
- аудит (audit) систематичний, незалежний та документований процес отримання свідоцтва аудиту та об'єктивної його оцінки з метою визначення ступеня, з яким виконуються критерії аудиту
- аутентифікація (authentication) забезпечення гарантії того, що заявлені характеристики об'єкта є справжніми
- справжність (authenticity) властивість, що вказує, що об'єкт є те, що він заявляє про себе.

Найпоширенішими загрозами інформаційній безпеці вважаються:

- Атака постійних серйозних загроз - це складна кібератака, яка полягає в тому, що порушник (або група) отримує доступ до робочої мережі та даних і залишається непоміченим протягом тривалого часу.
- Бот-мережа. Термін бот-мережа утворений від слів "robot network" (роботизована мережа) і означає мережу пристроїв, які порушник уражає інфікованим кодом, а потім віддалено керує ними.
- Розподілені атаки на відмову в обслуговуванні. DDoS-атаки утворюються за допомогою бот-мереж і використовуються для заспамлення корпоративних веб-

сайтів та програм, через що доступ для справжніх користувачів цих служб стає недоступним через надмірне навантаження на ці сервери.

- Атаки прихованого завантаження. Це фрагмент коду зловмисника, який автоматично завантажується на пристрій жертви після того, як той відвідує фішинговий веб-сайт. Таким чином користувач стає жертвою та відкритим для подальших дій зловмисника.

- Набір експлойтів - комплексний набір інструментів, що використовують програми для виявлення вразливостей і враження пристроїв шкідливим програмним забезпеченням з наступим його використання проти користувача.

- Внутрішня загроза. Завжди існує загроза того, що внутрішній авторизований користувач буде використовувати свій доступ для неправомірних дій щодо організації, які можуть зашкодити інформаційній безпеці.

- Атака зловмисного посередника. Порушник підключається до лінії передачі інформації під виглядом авторизованого користувача та отримаю всю конфіденційну інформацію, котра мала бути передана.

- Фішингові атаки. Під час фішингових атак зловмисники маскуються під справжні інформаційні ресурси або користувачів, щоб отримувати інформацію через електронну пошту, текстові повідомлення або через форму вводу даних на сайтах.

- Зловмисні програми з вимогою викупу. Дія таких програм зводиться до того, що програма шифрує інформацію з окремої станції або цілого серверу, вимагаючи після цього сплатити викуп під загрозою знищення цієї інформації.

- Соціотехніки. Цей тип кібератак використовує людський фактор. Він заснований на тому, що зловмисник завойовує довіру жертви, заражені антивірусні програми або фішинг, а потім збирає персональні дані та використовує їх для подальших атак.

- Атаки в соцмережах. Одна з частин соціотехніки під час яких кіберзлочинці вражають платформи соціальних мереж, застосовуючи їх як механізми

поширення шкідливого програмного забезпечення, або крадуть інформацію чи дані про користувачів.

- Віруси та хробаки. Це приховане шкідливе програмне забезпечення, яке запрограмоване би самостійно поширюватися в мережі або системі користувачів використовуючи всю вільну пам'ять системи. [2]

Порушення стану інформаційної безпеки може бути викликано як спланованими діями зловмисників, так і недосвідченістю співробітників. Всі користувачі інформаційної системи повинні мати хоч якесь поняття про безпеку, по шкідливому програмному забезпеченню, щоб своїми діями не завдавати шкоди компанії. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали. Основними джерелами загроз є окремі зловмисники («хакери»), кіберзлочинні групи і державні спецслужби (кіберпідрозділи), які застосовують весь арсенал доступних кіберзасобів. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки в роботі програмного забезпечення і веб-додатків, вади в конфігураціях мережевих екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів.

Технологія управління доступом користувачів досить рідко має змогу працювати сама по собі, та задовольняти при цьому потребу у безпеці. Кращим варіантом запровадження є комплексної системи, у котрій буде кілька ланок захисту. Проте правильне та чітке написання всіх вимог у такій системі є важливою запорукою стабільного захисту системи.

1.2 Методи та технології забезпечення інформаційної безпеки

Організувати інформаційну безпеку можуть допомогти спеціалізовані програми, розроблені на основі сучасних технологій, переважна більшість з яких

вигідніше розташовувати на хмарних серверах компаній-посередників, через більшу незалежність та гнучкість. Серед цих ПЗ можна виділити, такі як:

- захист від небажаного контенту (антивірус, антиспам система, веб-фільтри, анти-шпигуни);
- мережеві екрани і системи виявлення вторгнень (IPS);
- управління обліковими записами (IDM);
- контроль привілейованих користувачів (PUM);
- захист від DDoS;
- захист веб-додатків (WAF);
- аналіз вихідного коду;
- антифрод;
- захист від націлених атак на організацію;
- управління подіями безпеки (системи SIEM);
- системи виявлення аномального поведінки користувачів (UEBA);
- захист автоматизованої системи управління технічними пристроями;
- захист від витоків даних (DLP);
- шифрування даних;
- захист мобільних пристроїв користувачів;
- резервне копіювання даних;
- системи відмовостійкості.

Та одні лише програмні засоби встановлені на сучасному устаткуванні не може гарантувати повну безпеку даних та інформації в межах організації, також неможливо виключати такі засоби:

- Організаційні. Комплекс дій та засобів організаційно-правового та організаційно-технічного характеру. До них відносять законодавчі та нормативні акти, локальні нормативні документи організації, а також заходи по обслуговуванню інформаційної інфраструктури об'єкта.

- Апаратні (технічні). Спеціальне обладнання та пристрій, що запобігає витоку, що захищає від проникнення в IT-інфраструктуру об’єкта .
- Програмні. Спеціальне ПО, необхідне для захисту, контролю, зберігання інформації.
- Програмно-апаратні. Спеціально розроблене обладнання з встановленим ПО для захисту даних.

LDAP – це різновид протоколу, що використовується задля доступу до служби каталогів. Котрий використовує технологію TCP/IP для передачі даних про авторизацію користувача, пошук та редагування. Цей протокол має відкритий код, що дозволяє його модифікацію та використання. Широко використовується у службах каталогів.

SAML – це відкритий стандарт обміну даними, котрий використовується для надання доступу до кількох сервісів, використовуючи при цьому лише один вхід користувацьких облікових записів для авторизації. До цього стандарту використовувались файли cookies, котрі є більш вразливими до кібератак та неможливими для використання у різних доменах. Стандарт SAML використовується для обміну даними про аутентифікацію користувача та постачальниками послуг, але для цього сайти та додатки мають підтримувати цей стандарт. Використовуючи SAML разом з двох факторною аутентифікацією можливо поліпшити захист від найпоширеніших атак на інформацію.

OAuth 2.0 – це досить розповсюджений та зручний протокол, котрий дає можливість користувачу не передаючи сайту свої логін та пароль передати закриті дані з іншого сайту або авторизуватись за допомогою іншого сайту. Він працює таким чином, що при спробі аутентифікації на сторонньому сайті є можливість аутентифікації за допомогою вже відомого сайту, на котрому вже зареєстрований користувач. При цьому остання точка входу не буде знати про користувача нічого, крім логіна та ідентифікатора.

Здійснення контролю за інформаційною безпекою підприємства

Для забезпечення повноцінної та надійної інформаційної безпеки підприємства можна тільки за умови застосування комплексного та послідовного підходу. Система інформаційної безпеки повинна бути побудована з урахуванням всіх можливих та актуальних загроз і вразливостей, також з урахуванням тих загроз, які будуть виникати у майбутньому. Через такий підхід необхідно забезпечити підтримку постійного контролю, який повинен діяти щодня і цілодобово, та постійно документуватись. важливою умовою є дотримання контролю на кожному з етапів життєвого циклу інформації, починаючи з моменту її входження в інфраструктуру компанії і закінчуючи втратою її актуальності або знищення.

Існує багато видів контролю інформаційної безпеки, впровадження яких дозволяє компанії знижувати ризики в забезпеченні безпеки та мінімізувати ризики. У тому числі розрізняють:

- Адміністративний контроль. Це система, що складається з комплексу написаних стандартів, принципів роботи, політик і процедур. Цей різновид контролю визначає поведінку бізнес-процесів та дії з управління персоналом. Він включає законодавчі та нормативні акти, затверджену на підприємстві політику корпоративної безпеки, систему найму співробітників, дисциплінарні та інші заходи.
- Управління доступом. Зазвичай цей метод використовують в електронному вигляді, надають певний доступ для певного аккаунту, певної людини до певного середовища. На початкових етапах компанії цей процес може бути ручним, але зі збільшенням організації він потребує автоматизації. Автоматична реєстрація відбувається заздалегідь вказаними параметрами.
- Фізичний контроль. Заснований на тому, аби не дати посторонній особі доступ до захищеного середовища. Загалом зосереджений на середовищі робочих

місць і засобах обчислення. Він передбачає забезпечення ефективного функціонування інженерних систем будівель підприємства, робота яких може вплинути на збереження і передачу інформації. До таких систем відносяться опалення та кондиціювання, протипожежні системи. Іншою складовою фізичного контролю є системи контролю та управління доступом співробітників на охоронні об'єкти. До фізичного контролю можна віднести контрольні пункти пропуску, на якому зазвичай доступ надають охоронці та(або) автоматичні пропускні пункти.

•Механізми шифрування. Досить довгий час шифрування було пов’язано лише з державною таємницею. Були ГОСТи, в котрих відповідним чином відображалася її робота. Та на зараз, останній ДСТУ ГОСТ 28147:2009 котрий базувався на блочному шифрі був відмінений та запроваджений новий. Цей алгоритм створений для шифрування невеликих (до 616 біт) повідомлень для будь-яких алгоритмів шифрування, в тому числі визначеними національними стандартами України. Як і стандарт цифрового підпису ДСТУ 4145:2002, новий алгоритм заснований на криптографічних перетвореннях у групі точок еліптичних кривих, котрі використовують замість кривих у формі Вейєрштрасса найновітніші розробки у галузі еліптичної криптографії – криві у формі Едвардса та є більш швидким та ефективним за попередній [4]. Шифрування також застосовують на кінцевих точках користувачів, за допомогою шифрування дисків. Найкраще з цим справляється Bitlocker шифруючи диск використовуючи чіпи TPM. А також, технології VPN, котрі можуть створювати захищені потоки даних між важливими точками. При цьому шифруючи весь трафік, що проходить повз.

•Протидія шкідливим програмам та вірусам. В цю категорій зазвичай включають найпоширеніші трояни, програми-вимагачі, віруси, черв’яки та банківські шкідливі програми. При роботі з актуальною Windows ОС можна використовувати програмне забезпечення Microsoft Defender. Котрий поставляється комплектом до ОС [5]. Це є компонентом захисту кінцевої точки, використовуючи машинне вивчення, аналіз великих даних та вивчення

сприйняття ризиків. Котрий може працювати в кількох режимах: активному (перевірки, ідентифікації та зупинки ризиків), пасивному (перевірки та ідентифікації, без активних дій) та відключеному.

- Апаратні системи захисту. Це проміжні системи між фізичним та програмним захистом. До них відносять апаратні мережеві екрани, котрі встановлюють між різними сегментами мережі, генератори шумів у бездротових мережах, фізичні пристрої, для зберігання паролів, апаратні модулі дозволенного завантаження ОС, котрі не дозволяють завантаження інородної системи при включенні. Досить часто апаратні методи захисту виконують подібні до програмних засобів функції, але через те, що апаратні мають менше вразливостей та важче зламуються – їх поєднують. Важливою деталлю буде використання саме сертифікованих засобів, адже їх робота підтверджена в такому разі сертифікатами якості.

- Програмні засоби захисту. Тут використовуються методи протидії шкідливим програмам та вірусам, схожі функції з апаратним захистом та засоби розмежування доступу, інструменти віртуалізації (для побудови системи з тестування недовірених програм), програмні фаєрволи та брандмауери, DLP-системи які попереджують витік інформації, SIEM-системи які фіксують активність.

- Організаційні засоби захисту. Це перелік внутрішніх правил, щодо користування інформаційною мережею працівниками, та зменшення ризиків від внутрішніх загроз шляхом обмежень та навчань. Принцип персональної відповідальності є найефективнішим з точки зору організації безпеки.

- Морально-етичні засоби, це складені моральні нормі в колективі, виконання яких допомагає у збереженні інформації в організації, а порушення таких норм прирівнюється до правил поведінки й тягне за собою втрату авторитетності у колективі.

У всіх економічно-розвинених країнах питання кібербезпеки та кіберзахисту вирішується введенням сучасних стандартів, наприклад NIST

Cybersecurity Framework, або План дій по національній безпеці для кібербезпеки «Cybersecurity National Security Action Plan» в США, Nationales Cyber-Abwehrzentrum, NCAZ засноване у Німеччині.

Головна концепція Cyber Security Strategy for Germany 2021, як і більшості країн ЄС полягає у

- Обговоренні рамок дії федерального уряду в галузі кібербезпеки;
- Створює прозорість та зрозумілість для всіх, хто має відношення в уряді, промисловості, населенні;
- Сприяє активному залученню всіх зацікавлених сторін;
- Враховує специфікації та стандарти ЄС;
- Залишає звітність та контроль на стратегічному рівні;
- Постійно готується до можливих майбутніх перевірок та вдосконалення.

Розроблені ці стандарти з безпеки та плани дій дозволяють виявляти, реагувати та навіть запобігати багатьом кіберінцидентам, вони вже застосовуються багатьма організаціями по всьому світу. ЄС також вже має вдалий досвід протидії кіберзлочинності. У них цим документом є «Директива з мережевої та інформаційної безпеки» («NIS Directive»). Україна, використовуючи світовий досвід, створила власне правове підґрунтя [6,7]. В рамках виконання Стратегії національної безпеки було прийнято Закон України № 2163-VIII від 05.10.17 р. «Про основні засади забезпечення кібербезпеки України», який став підґрунтям забезпечення кібербезпеки України.

Сучасні засоби захисту можуть виявити майже всі можливі загрози, засобами штучного інтелекту можливо як прослідкувати створені вже загрози та на їх прикладі проаналізувати можливі майбутні зміни та порівнювати їх зі збереженими зразками шкідливого коду. Такі об’єкти можна відкривати в «пісочниці», лікувати або видаляти. Або ж обмежувати та сповіщати користувача для вибору подальших дій з об’єктом.

За допомогою інших засобів можна шифрувати дані або приховувати трафіки даних у інформаційних мережах серед нешифрованого трафіку. Розробляти алгоритми сповіщення про інциденти та робити резервні копії для відновлення або аналізу логів у разі непередбачених або позаштатних ситуацій в організації.

Ефективними також є методи контролю доступу користувачів до інформації, даних та внутрішнього середовища. Саме цим методом найбільше користувались до появи всесвітніх мереж зі зберігання та передачі інформації (інтернету). Адже так можливо забезпечити контроль та документування доступу до об'єкта як фізичного так і інформаційного. Важливим моментом застосування такого методу є ідентифікація та авторизація особи у конкретному місці та проміжку часу, адже право доступу може надаватись на деякий термін. При цьому необхідним також є ідентифікація активів та визначення ідентифікаторів, котрі надають право доступу саме до конкретного активу.

1.3 Порівняння систем управління ідентифікацією та доступом (IAM)

Система управління ідентифікацією та доступом є однією зі складових загальної системи керування доступом, взагалі їх розрізняють чотири типи:

- Система керування життєвим циклом облікових записів (Identity Management, IDM);
- Система ідентифікацією та контролю доступу (Identity Management, IAM);
- Системи керування політиками та контролю доступу (Identity and Access Governance, IAG);
- Компонент служби каталогів (Direcroty Services,DS).

Для зручного керування обліковими записами їх необхідно відокремлювати, в тому числі, можливо по групам які створюються для різних ролей. На вкладці Access Management - User groups представлена можливість створення нових та

керування існуючими групами. У ці групи можливо додати необмежену кількість політик, відповідних цій групі або ж створити нову (але цим займаються досить рідко), вибір вже налаштованих політик досить великий.

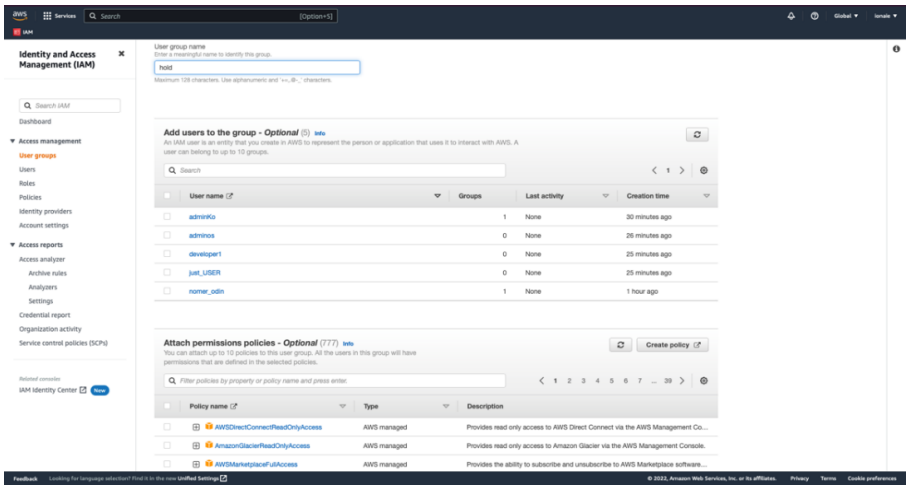

Рис. 1.1 – Створення користувацьких груп

При створенні нових облікових записів використовується схожа схема, спочатку задається ім’я, та спосіб авторизації користувачів. Це може бути як програмний код (обліковий номер та секретний пароль) для входу використовуючи засоби AWS API, CLI, SDK та інші, так і звичайний пароль користувача та логін. Вибір тимчасового паролю та заданого адміністратором. Та опція примусової заміни першого виданого паролю, задля безпечного використання аккаунта.

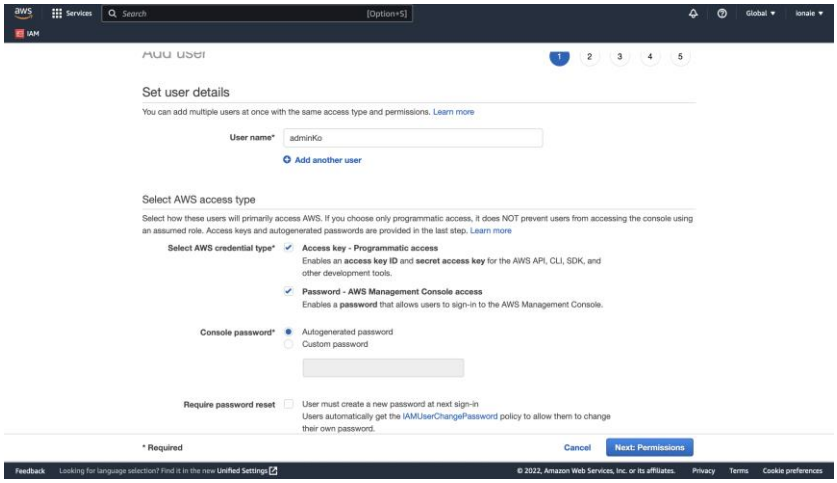

Рис. 1.2 – Створення облікових записів

Також, при створенні нових записів є можливість додати запис до вже створеної групи, створити групу а ще, скопіювати всі групи, котрі закріплені на іншим обліковим записом. Це дуже зручна функція, дивлячись на, що кількість груп не обмежена а списки доданих груп досить часто можуть бути однакові. Групи дають доступ користувачам до певних інформаційних активів. Це можуть бути як файли так і програми.

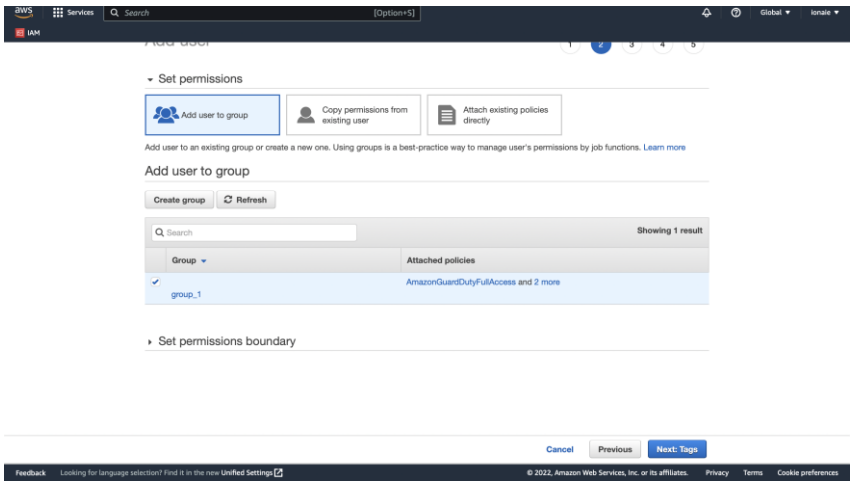

Рис. 1.3 – Створення облікових записів

Після надання всіх необхідних дозволів, додавання до груп та політик надаються унікальні сгенеровані системою облікові номери та паролі. Та можливість надсилання даних для входу в новий обліковий запис на пошту.

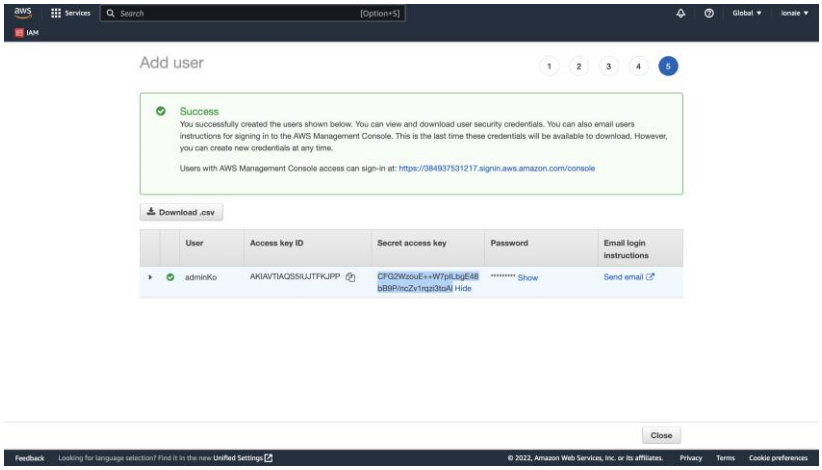

Рис. 1.4 – Створення облікових записів

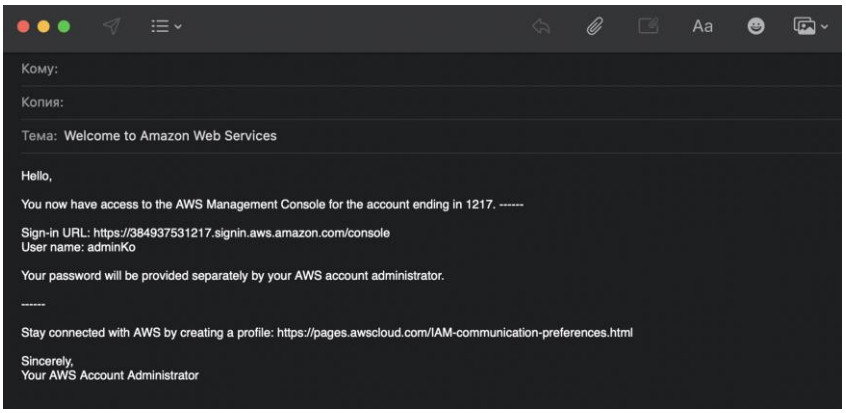

Рис. 1.5 – Оповіщення нового користувача

Далі можливо створювати ролі, цим механізмом надаються права для користувачів на використання наданих ресурсів. Кожна роль має набір дозволів на виконання запитів до сервісів, при цьому вона не пов’язана з будь-яким користувачем в системі.

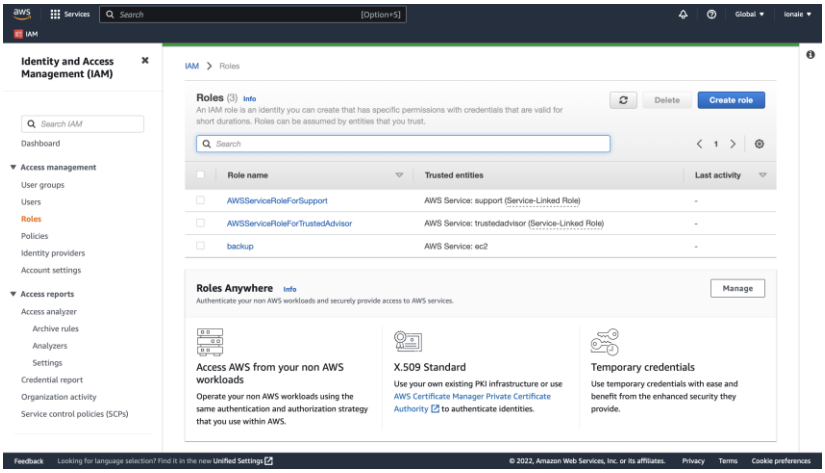

Рис. 1.6 – Створення ролей для користувачів

Через багатофункціональність серверів системи, доступ до них може бути за допомогою різних інструментів:

- AWS service. Доступність виконання дій сервісами EC2, Lambda та іншим у мережі AWS.

- AWS account. Можливість виконання дій іншими акаунтами, власником котрих є третя сторона.

-Web identity. Дозволяє користувачам брати на себе одну роль для виконання дій під цим обліковим записом, якщо вони об’єднані одним надавачем постачальником сертифікатів.

- SAML 2.0. Дозволяє користувачам із корпоративного списку виконувати дії в цьому обліковому записі.

- Custom trust policy. Можливість створення своєї політики для облікових записів.

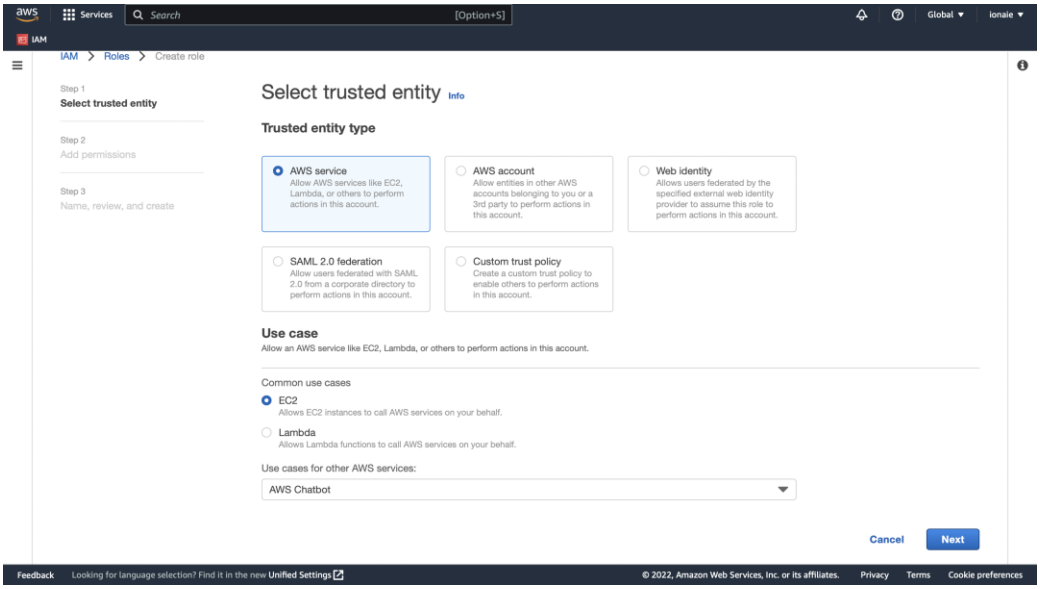

Рис. 1.7 Варіанти входу в робочий аккаунт

Для зручності керування політиками їх винесли в окреме вікно, де відбувається їхнє керування, та створення нових.

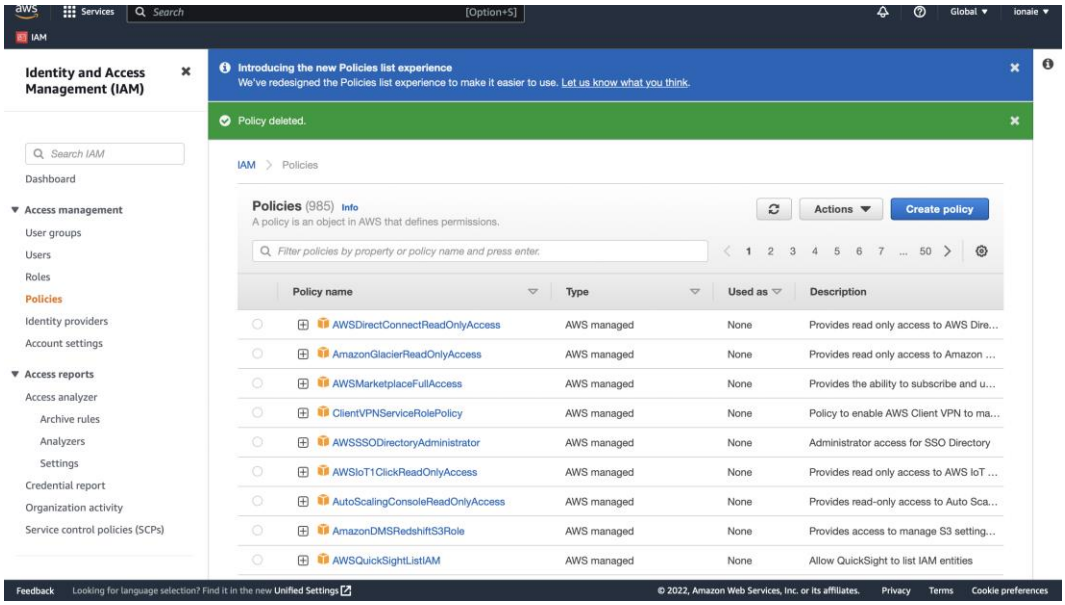

Рис. 1.8 Варіанти вибору політик керування

Для безпечного доступу до сервісу AWS існує кілька варіантів входу:

Пароль, використовується при вході разом з логіном до захищеного облікового запису в системі AWS в форматі консолі, AWS форумів, AWS

підтримки. За політикою безпеки пароль має бути складним та періодично змінюватись.

Мульти-факторна аутентифікація (MFA). При цьому методі входу дозволяється вхід до облікового запису лише після підтвердження користувача на додатковому пристрої, це може бути код-пароль, відбиток пальця, або токен.

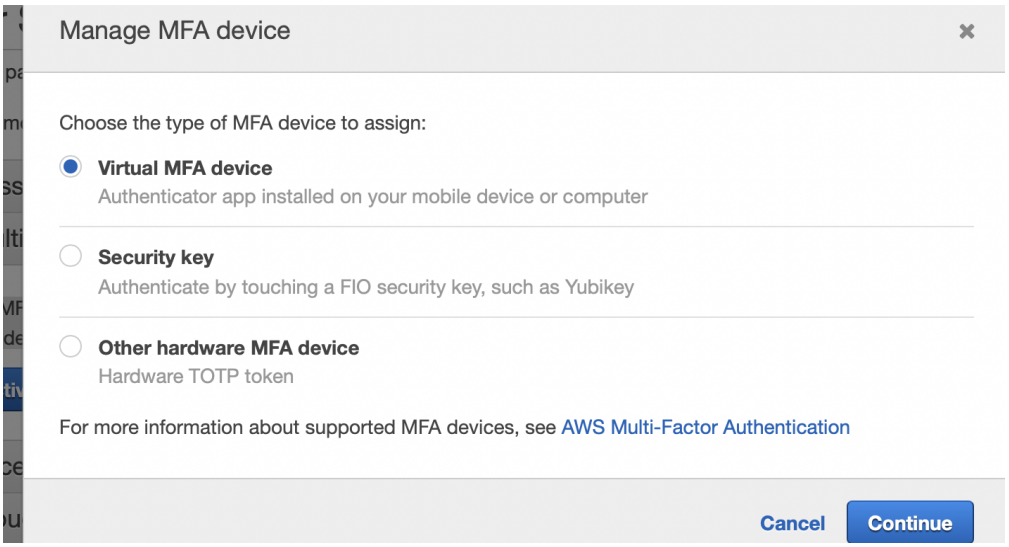

Рис. 1.9 Варіанти вибору MFA

Сертифікати X.509. Це цифрові документи, корті видаються користувачу центром сертифікацій компанії та перевіряються перед входом до мережі AWS. Такі сертифікати шифровані та містять відкритий код користувача і звіряються на відповідність. Вони використовуються безпечних запитів протоколів SOAP у сервісах AWS. Через це, система AWS рекомендує періодично змінювати ці сертифікати на нові, при цьому у користувача не повинно бути більше двох таких сертифікатів одночасно.

- Інформація, котра знаходиться у таких сертифікатах має такий вигляд:
- Дані про суб’єкта сертифіката
- Відкритий ключ
- Дані про центр сертифікації
- Підтримувані алгоритми шифрування та цифрового підпису
- Дані для визначення статусу да доступності сертифіката

Ключі доступу. Це зазвичай два секретні ключа, які зберігаються у користувача та слугують ідентифікаторами для прямих викликів інструментів PowerShell, AWS SDK (JavaScript) та AWS API. При втраті одного з двох ключів користувач має видалити попередній та встановити новий.

Доступний також підпис запитів AWS API, котрий, за допомогою командного рядка AWS CLI (або інших інструментів) можуть підписувати запити за допомогою налаштованих ключів. Проте, такі підписи дійсні лише у тому випадку, якщо їх підписує автор запитів. При відправці запитів API до AWS відбувається ідентифікація користувача за підписом, у якому знаходиться ідентифікатор ключа та секретний код доступу. Використовуючи підписи можна забезпечити надійність передачі даних, шляхом перевірки особи відправника, захисту від потенційного перехоплення та відтворення цих запитів.

Під час відпису відбувається обчислення хешу повідомлення, додавання до нього деякої іншої інформації та секретного коду відправника. З цих даних далі формується підпис і додається у заголовок HTTP або є частиною URL -адреси при запиті. [9]

Azure Active Directory (AD, ADD)

Компанія Microsoft пропонує для своїх підписників сервіс Azure Active Directory, який включає в себе керування всією системою доступів до сервісу та облікових записів з одного місця. Адже користуючись такими популярними

додатками як O365, Teams, Power BI, Word, Excel користувачі заразом потрапляють під дію сервісів Azure Active Directory.

При роботі з цим сервісом клієнт спочатку звертається до Active Directory, авторизується в ньому з логіном та паролем та видає клієнту персональний токен. Вже тільки після цього, клієнт звертається із запитом до цільового сервісу і надає йому свій токен для перевірки. А цільовий сервіс, в свою чергу окремо перевіряє запитом дійсність цього окремого токену запитом до Active Directory та вирішує, чи погоджувати вхід чи ні.

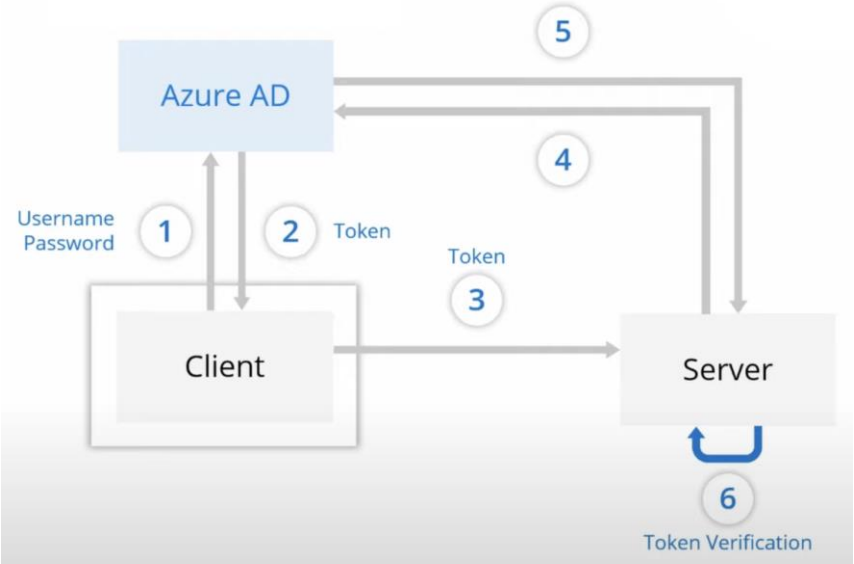

Рис. 1.10 Перевірка токенів у AD

Служба AAD надає можливість адміністратору управління доступом до хмарних рішень, таких як хмарним додаткам, локальним додаткам, а також ресурсам компанії. Ресурси можуть бути як у середині компанії, так і за її межами, такі як Azure AD, SaaS, Power BI, SharePoint.

Доступ до ресурсів може надаватися як одному конкретному користувачу, так і виділеній групі в котру входять користувачі. Також, можна передавати право на визначення доступів іншому користувачу.

Використання Azure Active Directory також ґрунтується на методі мінімальної довіри до користувача, надаючи таким чином лише доступ до тієї

інформації, котра необхідна в даний час для роботи. Використовуючи всі можливі змінні атрибути для користувачів та груп користувачів. За допомогою яких можна фільтрувати та знаходити окремі об’єкти та надавати їм певні права.

Власник ресурсу може створювати групи та визначати власника цієї групи, який вже в свою чергу визначає користувачів для цієї групи. Доступ до цієї групи відбувається після авторизації користувачів, зіставлення їх прав до перегляд та редагування інформації.

У адміністраторів є можливість використання PowerShell для автоматичного редагування та внесення змін до об’єктів, чи запуску автоматизованих скриптів для управління через командну строку.

Права доступу можуть бути назначені таким способом:

- Пряме назначена власником ресурсу користувача.
- Вибір групи, користувачі якої автоматично набувають права користування ресурсом.
- Відбір на основі правил, котрі ґрунтуються на атрибутах окремих користувачів. Котрі пов’язанні між собою конкретними ознаками.
- Надання права зовнішньому каталогу, котрий матиме та надаватиме сам право на доступ своїм користувачам.

За необхідності, налаштовується можливість для користувачів надсилати запити до власника ресурсів для надання доступу, або автоматичне надання доступу при запиті. Але при наявності кількох власників ресурсу на відхилення запиту хоча б одним з них цей користувач не отримує доступ до ресурсу, лише повідомлення про відхилення.

Так у версії Windows Server 2012 з’явилась можливість налаштування динамічного контролю доступом до ресурсів. Вона надає адміністраторам можливість написання вимог для користувача, котрі мають бути виконані для доступу до певного ресурсу. Це правила, які вміщують конфіденційність, роль

користувача, використовуваний девайс для входу, мережа через яку відбувається вхід, певні вимоги до ПК. Якщо використовується такий вид доступу можливості користувача будуть змінюватися динамічно системою та доповнюватись опис та атрибути даного користувача для входу.

Служба Active Directory виконує завдання з ідентифікації та доступу користувачів до ресурсів компанії, та її можна поділити на кілька ролей, а залежності від направлення:

- Служба сертифікації Active Directory, це Active Directory Certification Services. Більш розширені організації також додають собі центри сертифікацій, для генерації власних сертифікатів доступу котрі відмічають певних користувачів з їхніми атрибутами певним ключем. Та в результаті керування даними ключами.
- Служба керування правами доступу Active Directory Rights Management Services. Забезпечує захист інформації використовуючи правила та шаблони збережених політик доступу для користувачів у мережі.
- Служби Active Directory Federation Services, можуть забезпечувати для організації розширення та використання інших платформ для ідентифікації користувачів.
- Служба Active Directory Lightweight Directory Services зберігає дані додатків для їх швидкого використання.

Azure Active Directory має підтримку такого мережевого протоколу, як RADIUS – служба віддаленої аутентифікації, для забезпечення централізованої аутентифікації та авторизації користувачів для безпеки мережі. AAD підтримує багатофакторну аутентифікацію на основі цього протоколу за допомогою серверу NPS. Цей сервер перевіряє облікові записи у AD та відправляє запит на багатофакторну аутентифікацію до AAD. Після цього користувач виконує вхід на довіреному пристрої та підключається до сервісу.

Хоча AAD використовує для аутентифікації користувачів службу RADIUS, та пропонує для реалізації саме цих цілей більш безпечний протокол SAML SSO. Він припускає можливість обміну інформацією про облікові записи між хмарним сервісом та постачальником посвідчень. Таким постачальником є Google Apps, Office 365 або ін. хмарний сервіс з підтримкою SAML SSO. До запиту на аутентифікацію додається підпис PKI, у якому містяться дані користувача та є гарантом оригінальності.

Головним аспектом використання SAML SSO виступає прив'язка користувача до постачальника посвідчень, аби сервіси мали змогу чітко вибирати куди саме потрібно перенаправляти запити по аутентифікації.

Через такий підхід, адміністрування записів користувачів у організації значно полегшується. При внесенні змін до запису вони автоматично будуть відображені у всіх сервісах, у котрих користувач був авторизований. Це відноситься до додавання, видалення та редагування прав користувача.

Мінусами використання такого сервісу можливо розглядати не завжди кваліфіковану технічну підтримку своїх сервісів, про що йдеться у багатьох групах обговорення Microsoft. Коли користувачі або не могли отримати відповіді та допомогу або ж отримували їх зі значною затримкою у часі.

Відсутність повної документації щодо використання та роботи більшості функцій Microsoft 365 та їх можливих проблем. Усе, що надається користувачу виглядає як опис можливостей та використовуваних технологій. Як саме вони між собою будуть реалізовані – немає у публічному доступі.

У рішення AD також є обмеження щодо використання у системі Windows. Та при цьому є додаткова підтримка через спрощену версію Active Directory Lightweight Directory Services (AD LDS), через нього можливо покривати потреби організації при використанні лише незначної долі сервісів на інших архітекторах, адже зі збільшенням таких сервісів буде фінансово невигідно їх підтримання та

адміністрування цією спрощеною версією AD LDS. Крім того, каталоги AD можуть бути змінені в будь-якому місці доступу, але найдобірнішою базою даних для каталогів є каталоги відділу кадрів. Через це дані скоріш синхронізуються із цих джерел. Та не мають рішень по керуванню синхронізацією у LDAP.

Досить великий час внесення деяких змін до сервісів, що зумовлюється реплікацією робочих серверів компанії. Дані просто не встигають оновлюватися, що є іншою стороною безпеки та гарантованої доступності. Бо хмарні сервіси Microsoft мають як основний сервер, на якому проводиться робота так і резервний (другий), на який відразу все копіюється. Також, задля гарантій цілісності Microsoft копіює робочі дані серверів на бекап сервери, але це вже не так заважає роботі та не викликає затримки у відгуках серверів на дії адміністраторів.

Одним з головних мінусів рішення Azure Active Directory можна вважати залежність усіх хмарних рішень компанії від одного сервісу. Так, вже в історії AAD був серйозний збій 28 вересня 2020 року, коли користувачі з багатьох країн не мали можливості користуватися сервісами через збої аутентифікації та перевірці додатків на авторизацію. Тож проходження усіх користувачів через одну систему може бути вкрай небезпечним рішенням для організації. Адже сервери налаштовані таким чином, що для роботи з будь-яким сервісом буде необхідно виконати вхід до AAD, а це в свою чергу може стати вузьким місцем.

2 АРХІТЕКТУРА ТА КОМПОНЕНТИ ДЛЯ РІШЕННЯ ORACLE IDENTITY MANAGEMENT

2.1. Oracle Internet Directory

Сервіси каталогів є найкритичнішою частиною будови усієї системи, адже з ними співпрацюють усі сервіси і в них зберігається уся інформація про системи. У них зберігаються усі дані з додатків та за наявності хорошої організаційної структури можна гарантувати ефективне управління багатьма функціями у системі. Проблемою організацій часто буває надходження інформації до такої бази із різних джерел, та представлення її потім у єдиному зручному для обробки вигляді для користувача. Така інформація може надходити про співробітників від HR відділу, від партнерів та співробітників у CRM системах, від суміжних LDAP каталогів. Тож система каталогів є основою для безпечних бізнес-процесів, котрі ґрунтуються на ідентифікації та управління ідентифікацією (IDM). Через те, що більшість зовнішніх додатків використовують стандартний механізм доступу до атрибутів ідентифікації, а саме використовуючи LDAP, для ідентифікацію користувача, прав доступу та інформації о профілі.

Сервіс Oracle Directory Services Plus (ODSPlus) пропонує рішення по комплексному керуванню службою каталогів , включаючи синхронізацію, зберігання та віртуалізацію.

- Oracle Internet Directory (OID) забезпечує можливість для зберігання декількох версій в одному місці, що дозволяє керувати та редагувати один каталог одразу у кількох додатках.
- Цей сервіс можна масштабувати до до великих розмірів на тій же кількості заліза, що сприяє здешевленню роботи цього сервісу.
- Забезпечує безпековий рівень, необхідний для функціонування бази даних на кожному рівні передачі, обробки та зберіганні інформації. Крім функцій безпеки LDAP він використовує функції Oracle для більшої безпеки зберігання та резервного копіювання - технологію прозорого шифрування інформації.
- Забезпечує кілька рівнів доступності для забезпечення високого рівня доступу до інформації.
- Надає широкий спектр інструментів для обробки різних видів каталогів, використовуючи каталоги Active Directories, AD LDS, Sun, eDirectory, OpenLDAP у одному сховищі каталогів.

Адміністратори OID можуть налаштовувати служби каталогів таким чином, аби надавати різні рівні допуску до інформації каталогах залежно від того, як саме користувач аутентифікувався у додатку.

Access Control List (ACL) – список правил, котрий надає користувачам певні привілеї та доступи до певних можливостей мережі, таких як інтернет, телефонія, відео-зв’язок. Використовуючи такий інструмент адміністратори мають можливість тонкого налаштування доступу до даних.

Сервіси Oracle підтримують зовнішню аутентифікацію користувачів, коли паролі зберігаються у зовнішніх каталогах, не синхронізуючись каталогами OID.

Така взаємодія забезпечує швидше розгортання сервісів та прибирає проблему з копіюванням паролів.

Також, адміністратори можуть налаштувати шифрування на рівні атрибутів, аби забезпечити захист даних, котрі зберігаються у каталогах.

Oracle Database Vault. Цей сервіс може забезпечувати:

- Захист даних програми від доступу та зміни даних користувачем з високим рівнем доступу.
- Забезпечення розподілення обов'язків між користувачами.
- Ведення контролю над тим, хто, коли і які додатки та бази даних можуть бути доступні на даний момент.

OID має функцію інтегрування каталогів для синхронізації даних між різними зовнішніми каталогами. Така синхронізація гарантує, що зміни, які були внесені у каталозі будуть коректними. Цей набір сервісів та інтерфейсів для синхронізації може гарантувати коректне використання із зовнішніми каталогами. За допомогою такої платформи клієнти створюють єдиний корпоративний каталог, що містить інформацію для автентифікації та авторизації користувачів, а також дані програми.

Для компактності розташування каталогів у репозиторії програм OID виконує міграцію та консолідацію даних. Oralce має інструменти, котрі допомагають виконувати міграцію розосереджених даних в єдиний інтернет-каталог. Міграція замінює існуючі каталоги одним централізованим. За неможливості заміни існуючого каталогу платформа виконує двонаправлену синхронізацію.

При міграції зовнішніх каталогів спочатку відбувається створення метаданих схеми каталогу, як атрибутів і класів об'єктів та їх порівняння та узгодження з існуючими. Виконання цього процесу займає багато часу та можуть виникати

помилки при цьому процесі. За допомогою інструменту «schemasync» цей процес проходить в автоматичному режимі з підтримкою адміністратора. Наступним етапом міграції відбувається експорт даних зі сховища та їх перетворення у LDAP формат. Інструмент «Idifmigator» створює файл LDIF на основі шаблонів, котрі можна настроювати та експортованих даних.

2.2. Oracle Identity Manager Architecture

Платформа Oracle Identity Manager автоматизує управління правами доступу, безпекою та надання інформаційних ресурсів користувачам. За її допомогою відбувається підключення, обмеження та відміна несанкціонованого доступу задля захисту корпоративної інформації.

Ця платформа може забезпечувати такі функції:

- Масштабованість архітектури. Вона досягається за допомогою використання серверу прикладних програм J2EE Oracle Identity Manager, а також аварійне перемикання та балансування навантаження між програмами. Він може надавати програми з підтримкою LDAP, а також і без неї.

- Глобальне керування користувачами. Oracle Identity Manager дозволяє будь-які організаційні ієрархії та групи користувачів. Можливе як наслідування, налаштування політик ідентифікаторів користувачів, управління політиками паролів та політиками доступу користувачів задля забезпечення вимог бізнесу. Адміністратори мають змогу керувати політиками програм та додатків, дивитись історію розподілення ресурсів та надає повне керування налаштуваннями для управління користувачами.

- Самообслуговування користувачів. Також, мається можливість налаштовувати портал для надання змоги користувачам вносити зміни до власних облікових записів, змінювати інформацію, міняти та синхронізувати паролі,

створювати запити на дозволи для використання програм, переглядати та редагувати доступні права облікового запису, а також, співпрацювати з робочим процесом.

•Гнучкий механізм процесів. За допомогою Oracle Identity Manager можлива підтримка відстежування робочих процесів, перевіряючи поточний статус на даний момент, його поточний статус, та у разі неуспішності – код помилки. Він підтримує розгалуження процесів в організації та процеси з обміном залежності та обміном даними. Цей процес можливо повністю настроювати.

•Звітність для аудиту. Надання повного звіту у реальному часі із відміткою стану для всіх процесів у даний час та повній інформації про стан. Manager підтримує складні звіти о роботі, аналізи та динамічні запити.

•Керування змінами. Вбудовані можливості Oracle Identity Manager дозволяють у кілька натисків мишкою керувати імпортом та експортом процесів, переміщувати пакети із системи в систему.

Java 2 Platform, Enterprise Edition (J2EE) це стандарт, створений для розробки багаторівневих додатків та програм.

Сучасні реалії бізнесу провокують створення та розвитку таких технологій, котрі б могли відповідати вимогам ефективності, продуктивності та можливостям масштабованості систем управління інформацією. Після проходження достатньої кількості тестів специфікація J2EE показала себе з найкращої сторони. Ця архітектура підтримує розробку додатків на основі компонентів, та зазвичай ділиться на такі рівні:

•Клієнтський рівень. Це Web-компоненти або Java програми які надають для користувача графічний інтерфейс з проміжного рівня.

•Проміжний рівень. Це рівень серверу, на якому об’єкти EJB та Web-служби виконують завдання передані з бізнес логіки програми та зберігаються дані.

•Рівень даних підприємства. На цьому рівні зберігаються дані підприємства, зазвичай у вигляді реляційних баз даних. [10]

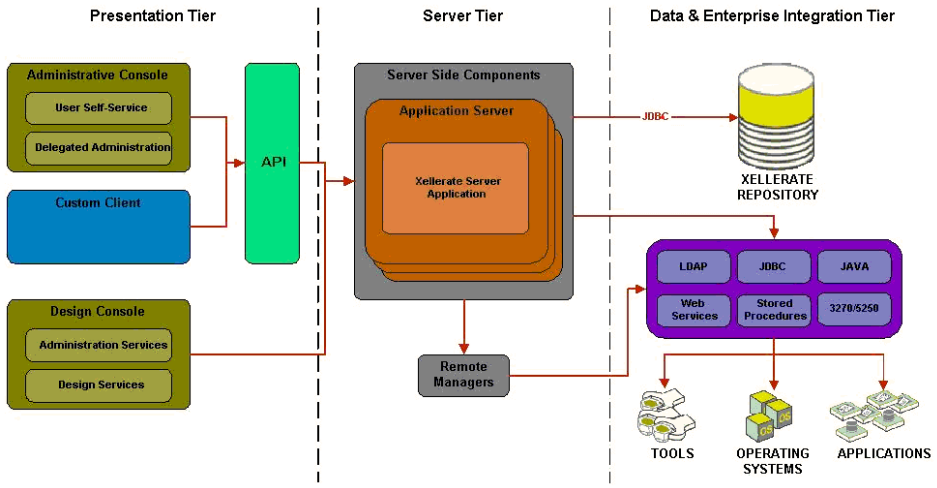

Рис. 2.1 Складові Oracle Identity Manager

Oracle Identity Manager базується на трьох рівнях інтеграції:

1. Клієнтський. У цього рівня існую два інтерфейси Designe Console та Administrative and User Consol. Зазвичай користувачі використовують для входу Administrative and User Consol, яка передає серверу облікові дані користувача. За допомогою цієї консолі користувачі можуть шукати, редагувати та видаляти інформацію у базі даних.

2. Сервер додатків. Цей рівень має реалізувати бізнес-логіку у форматі Java Data Objects. Лише компонент J2EE-сервер додатків що має взаємодіяти з базою даних. Він відповідає за таку функціональність, як:

•Вхід до Oracle Identity Manager, сервер додатків підключає клієнт до бази даних.

•Обробка запитів від клієнтів, сервер передає інформацію між клієнтом та базою даних та навпаки.

•Масштабованість. Сервер додатків може підтримувати піл з’єднань або ж спільну взаємодію з додатками. Та покращує продуктивність підключень до бази даних та може динамічно змінювати розмір пулу з’єднань через оптимізацію ресурсів для у задачах для масштабованості використання клієнтів.

•Захист даних на системному рівні. Oracle Identity Manager може запобігати несанкціонованому доступу своїх користувачів до метаданих системи, аби не давати можливості випадково або навмисно змінювати та видаляти системні файли. При спробі редагування та видалення системних файлів неавторизований користувач отримує сповіщення від системи.

3. База даних. Цей рівень відповідає за керування та збереженням даних у Oracle Identity Manager.

2.3 DataBase of Enterprise User Security

Дане рішеннядля адміністраторів дає можливість керувати доступом до кількох баз даних у великої кількості корпоративних клієнтів, та при цьому не витрачаюси на це велику кількість часу. Використання цього рішення в парі з OID можуть вормувати стратегію безпеки для користувачів у організації. Дані користувачів DB of Enterprise зберігаються у каталозі з автентицікацією та авторизацією (ролі та привілеї). У разі отримання доступу до бази даних Oracle, база даних підключається до OID як клієнт LDAP для отримання даних про користувача та проходить процес автентифікації та авторизації, який використовується для встановлення підтексту безпеки користувача на цьому сервері баз даних.

Централізоване управління баз даних значно зменшує адміністративні витрати, при додаванні, видаленні чи при зупинці прав на користування ресурсом. У такому випадку відбувається лише одна зміна у каталозі підприємства. Також, при використанні таких каталогів користувач може змінювати інформацію один раз, а зміни будуть відображені скрізь, де використовується дана інформація.

2.4 Oracle Authentication Services for Operation Systems

Не рідкою проблемою в управлінні даними аккаунтів постає необхідність використання деякими користувачами Unix та Linux подібних систем (Solaris, HP-UX, AIX, Linux, NetBSD, OpenBSD, FreeBSD та ін.) для своєї роботи. Адже у них забезпечується можливість керування рідним обліковим записом у системі, а такий варіант є дось кропітким для адміністрування. Хоча стандарт NIS (Network Information Services) може забезпечувати централізоване управління користувачами та їх даними автентифікації, але він має свої проблеми, судячи зі статей, безпека протоколу NIS досить ненадійна, адже будь-який користувач , знаючи назву домена може виконати запит RPC до ypserv та отримати наповнення карт NIS на даному сервері. Тож, налаштування безпеки на цих системах займе доволі багато часу, або ж зупиняти свій вибір на більш безпечних протоколаів, таких як LDAP.

Для вирішення таких проблем можна використовувати рішення Oracle Authentication Services for Operating Systems (OAS4OS) забезпечує централізоване керування автентифікацією користувачів Unix та Linux, їх політиками паролів та політиками авторизації за допомогою Oracle Internet Directory. OID використовуючи у Unix і Linux відкриті стандарти, такі як PAM_LDAP, NSS_LDAP, SUDO LDAP включно з засобами автоматизації та міграції користувачів може надавати весь комплекс управління обліковими записами для організації.

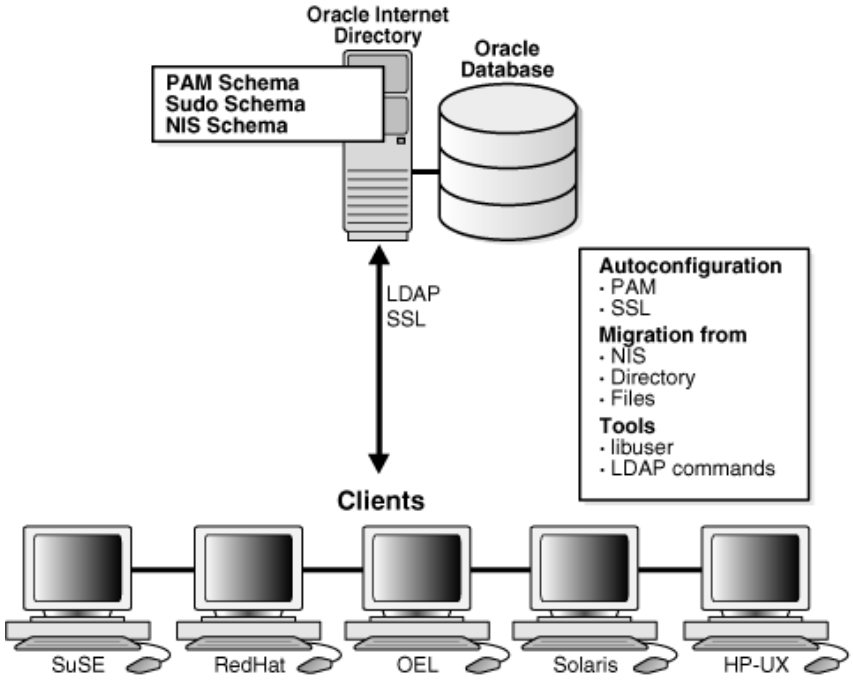

Рис. 2.2 Схема Oracle Authentication Services

Автентифікація користувачів у Oracle Internet Directory проходить наступним чином. Після надання користувачем своїх даних (це може бути ім'я та пароль, xdm, ssh, su або інших програмних даних) відбувається:

1. Програмний модуль автентифікації при вході перевіряє локальні файли конфігурацій, щоб визначити, яким чином можна автентифікувати користувача. Ці файли вміщують у собі інформацію про метод використання (LDAP), місцезнаходження серверу, налаштування SSL та сертифікати.
2. Модуль автентифікації спочатку спробує автентифікувати даного користувача на сервері OID за допомогою облікових записів, потім, якщо налаштовано, через модуль SSL з використанням сертифікату.
3. На наступному етапі проходить звірка, чи правильні дані та чи активний обліковий запис, та надається доступ. Якщо щось йде не так, сервер повідомляє про помилку користувачеві.
4. Далі модуль питає дані у OID про дозволені групи користувача.

5. OID надає інформацію про членство у групах.

2.5 Oracle Directory Integration Platform (DIP)

Також у компанії Oracle є готове рішення для інтеграції зовнішніх додатків та каталогів, включаючи LDAP для скорочення переносу даних під час переходу на цю систему та економії коштів. DIP підтримує використання Oracle Unified Directory, Oracle Internet Directory або Oracle Directory Server Enterprise Edition в якості основного робочого каталогу. Цю платформу можливо використовувати для таких цілей:

- Зберігати дані про співробітників у Oracle HR.
- Присилати сповіщення до додатків з підтримкою LDAP, коли вносяться будь-які зміни до внутрішнього каталогу.
- Синхронізацію паролів користувачів у Microsoft Active Directory з паролями в Oracle Unified Directory або Oracle Directory Server Enterprise Edition.
- Oracle DIP може гарантувати, що під час перенесення зовнішніх каталогів робочі додатки та інші каталоги будуть отримувати всю необхідну інформацію захищеною передачею даних.

Oracle DIP може підтримувати такі каталоги:

- Microsoft Active Directory 2003, 2008 і 2012
- Active Directory Application Mode або ADAM, версія 1 з SP1 на Windows 2003 (Microsoft Active Directory Lightweight Directory Service (AD LDS))
- Oracle Directory Server Enterprise Edition (ODSEE) 11gR1 (11.1.1.3+), який раніше був Sun Java System Directory Server
- Novell eDirectory 8.8
- OpenLDAP 2.2
- IBM Tivoli Directory Server 6.2
- Oracle Unified Directory 11gR1 (11.1.1.5+)

- Oracle Internet Directory

Синхронізація дає можливість координувати усі зміни поміж основним внутрішнім каталогом та усіма іншими підключеними каталогами. Для гарантії актуальності даних всі каталоги мають бути сповіщені про будь-які зміни, внесені у інших каталогах. Синхронізація може забезпечувати узгодженість усіх змін. Для таких дій створюються профілі синхронізації та налаштовується формат та зміст даних, що синхронізуються між зовнішнім та внутрішнім каталогом.

Як внутрішній каталог для синхронізації з Oracle Directory Integration Platform можна налаштувати наступні каталоги:

- Oracle Unified Directory
- Oracle Internet Directory
- Oracle Directory Server Enterprise Edition

Ще однією схожою до синхронізації фунцією є резервування. Через резервування можливо гарантувати, що програма буде повідомлена про зміни в каталозі. Такі зміни необхідно перевіряти при допуску до процесів та визначення, які ресурси можуть бути використані користувачем.

Зазвичай резервування використовують при роботі з додатками, котрі мають такі вимоги:

- Не підтримує каталог
- Підтримує LDAP
- Доступ до додатків дозволяється лише авторизованим користувачам

Синхронізація та резервування відмінні одне від одного поняття. Резервування застосовується для обробки даних між каталогами одного постачальника послуг. Синхронізація, забезпечує контроль даних, які повинні бути синхронізовані між внутрішнім каталогом та підключеними каталогами

інших постачальників каталогів на основі правил перетворення та відображення, які надає DIP.

Як сховище, в якому компоненти Oracle та інші додатки зберігають і отримують доступ до ідентифікаційних і облікових даних користувачів, можуть використовуватися або OUD, або OID, або ODSSE. Внутрішній каталог Oracle використовує спочатку підключений сервер каталогів для автентифікації користувачів шляхом порівняння облікових даних, що вводяться користувачами, з обліковими даними, що зберігаються у внутрішньому каталозі Oracle.

Потім, коли облікові дані зберігаються в підключеному каталозі, а не у внутрішньому каталозі Oracle, користувачі все одно можуть бути автентифіковані. Тоді каталог Oracle, що виступає як внутрішній каталог, використовує зовнішній плагін автентифікації, який автентифікує користувачів на сервері підключеного каталогу.

Внутрішні каталоги OUD та ODSEE використовують наскрізну автентифікацію для передачі автентифікації до підключеного каталогу, такого як Microsoft AD, для користувачів, що надходять з OUD та ODSEE.

Сервер Oracle Directory Integration Platform виконує такі функції:

Служба синхронізації Oracle DIP:

- Планування - обробка профілю синхронізації запланованого адміністратором розкладу
- Відображення - виконання правил перетворення даних між зовнішньо підключеними каталогами та внутрішнім каталогом Oracle
- Поширення даних - обмін даних з підключеними каталогами за допомогою коннектора
- Обробка помилок

Служба резервування каталогів Oracle DIP:

- Планування - обробка профілю синхронізації запланованого адміністратором розкладу
- Сповіщення про події - повідомлення додатку про відповідну зміну даних користувача або групи, що зберігаються у внутрішньому каталозі Oracle
- Обробка помилок

Майже всі сучасні системи спеціалізовані на керуванні доступом вже мають досить простий інтерфейс для адміністраторів. Часто робота адміністратора закладається в тому, щоб вносити редагування та використовувати фільтри при пошуку необхідної інформації. Через такі фільтри досить легко знаходити необхідного користувача, навіть при наявності кількатисячної бібліотеки. При додаванні користувачів у бібліотеку є багатий вибір атрибутів та описів, котрі можливо додати до кожного користувача окремо, інколи, для зручності вводиться спеціальний опис, для надання користувачу всіх повноважень і функцій. Хоча такий метод є досить небезпечним і не має використовуватися задля виконання правила найменших привілеїв. Зазвичай, для вибору функцій користувача досить лише відмітити прапорець навпроти необхідної функції.

Oracle має найбільш комплексне вирішення проблеми для служб каталогів, включаючи рішення по віртуалізації, синхронізації та зберіганню даних компанії. Такий відрив від конкурентів досягається реалізацією власної архітектури Oracle Data Base, зручністю використання технології Web 2.0 і корпоративної служби Oracle Enterprise Manager, інтеграцією майже всіх служб та протоколів для аутентифікації користувачів та технологією LDAP. Усі ці служби та технології в купі з інструментами міграції OVD та OID дозволяють організації вийти на новий рівень керування своєю інфраструктурою, стандартизувати її форму для використання та зберігання аби підвищити її безпеку та фінансову рентабельність.

3 РОЗРОБКА ВАРІАНТУ РІШЕННЯ ORACLE IDENTITY MANAGEMENT

4

3.1. Налаштування рішення Oracle Identity Management

Існує кілька версій продукту від Oracle IAM. Однією з яких є пробна версія на 30 днів, що дозволяє ознайомитись із продуктом, та за необхідності почати впровадження цієї системи у організації. Адже впровадження – це досить трудомісткий та надважливий процес існування системи.

Після вибору та реєстрації назви компанії (домену) потрібно створити користувачів цієї мережі. Доступними для адміністратора пунктами є ім’я, фамілія, електронна скринька та приналежність до необхідних груп компанії.

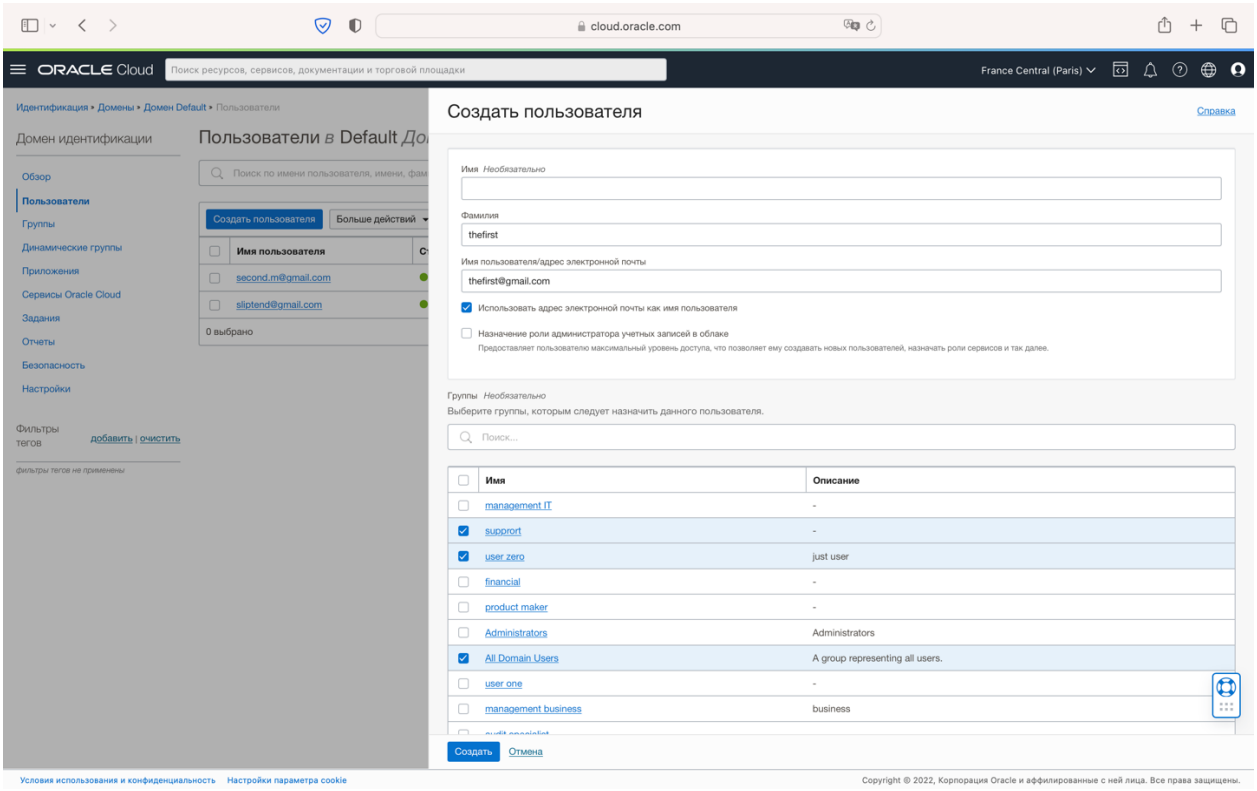

Рис. 3.1 Створення користувача Oracle IAM

Для зручності, краще використовувати латинський формат підпису при створенні. При наявності поштового сервісу використовувати як ім’я для поштової скриньки – ініціали користувача (напр. yermak.m@dut.com). Важливо, доступ до груп додавати лише необхідний для правильної роботи користувача. Та мати одну загальну групу, аби при необхідності вносити необхідні редагування одразу до всіх облікових записів.

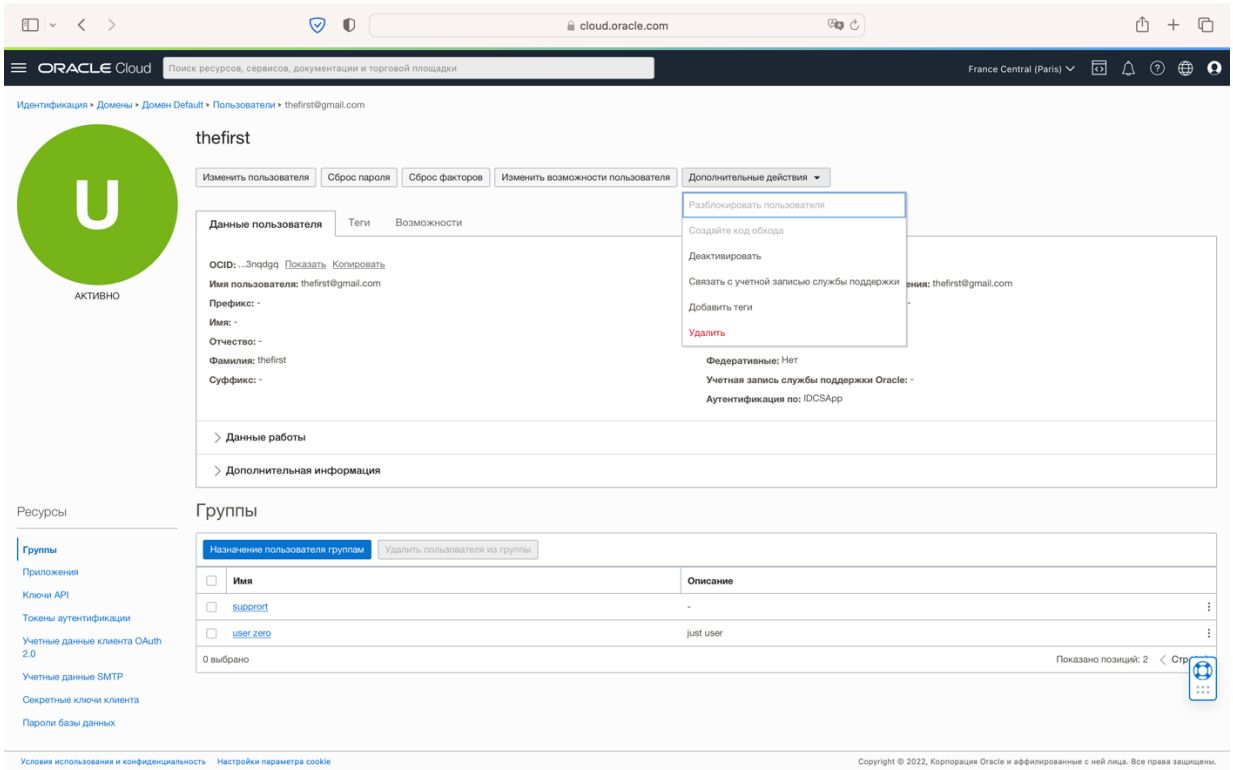

Рис. 3.2 Редагування користувача Oracle IAM

Після створення облікового запису адміністратору надається можливість його редагування. На сторінці редагувань є можливість зміни ролей, доступу до

груп, блокування, видалення, усього, що зазвичай доступно для роботи з системою IAM.

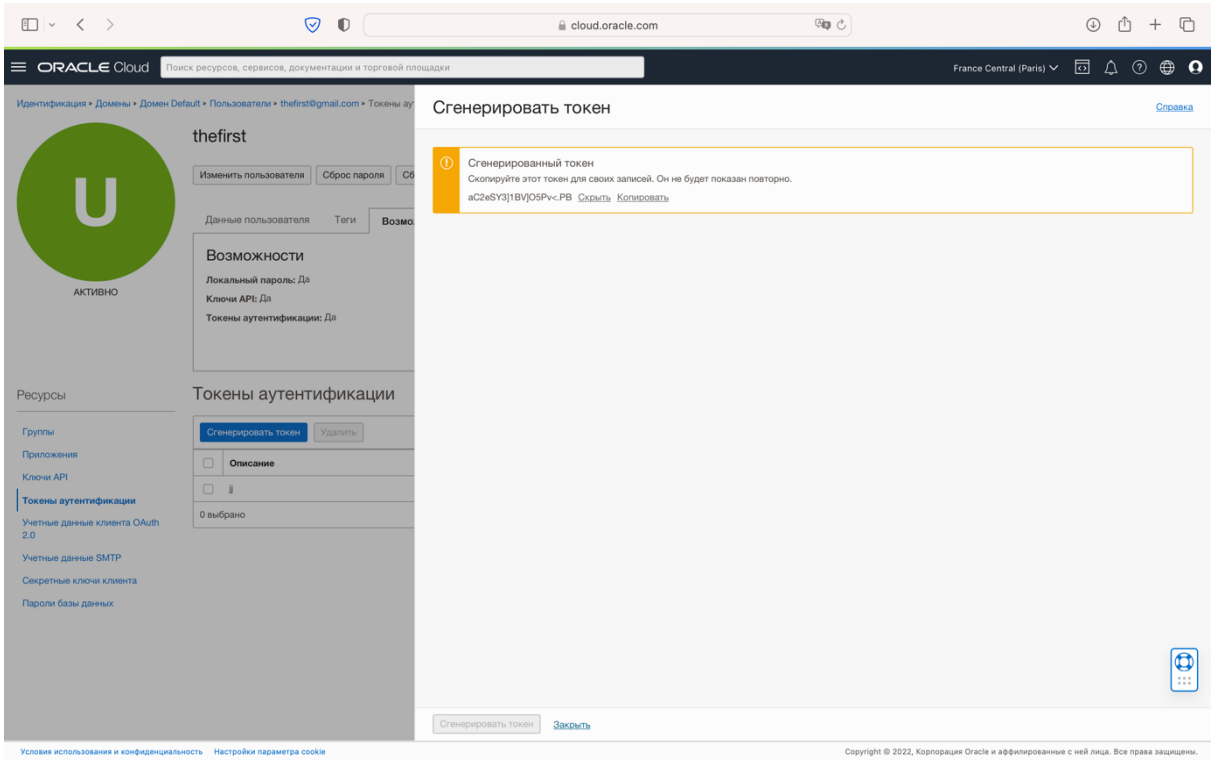

Рис. 3.3 Редагування користувача Oracle IAM

Також, для входу користувачів та надання їм відповідного доступу у зовнішніх додатках API можливо згенерувати токен аутентифікації, котрий в цілях безпеки показується тільки один раз. Знаючи цей токен будь-який користувач може аутентифікуватися як легітимний у зовнішніх додатках API. І це є небезпечним моментом, через це, зберігання та передача такої інформації має бути під контролем. Адже такий токен виступає як заміна звичайного паролю, при тому, що пароль не перестає діяти на обліковому записі.

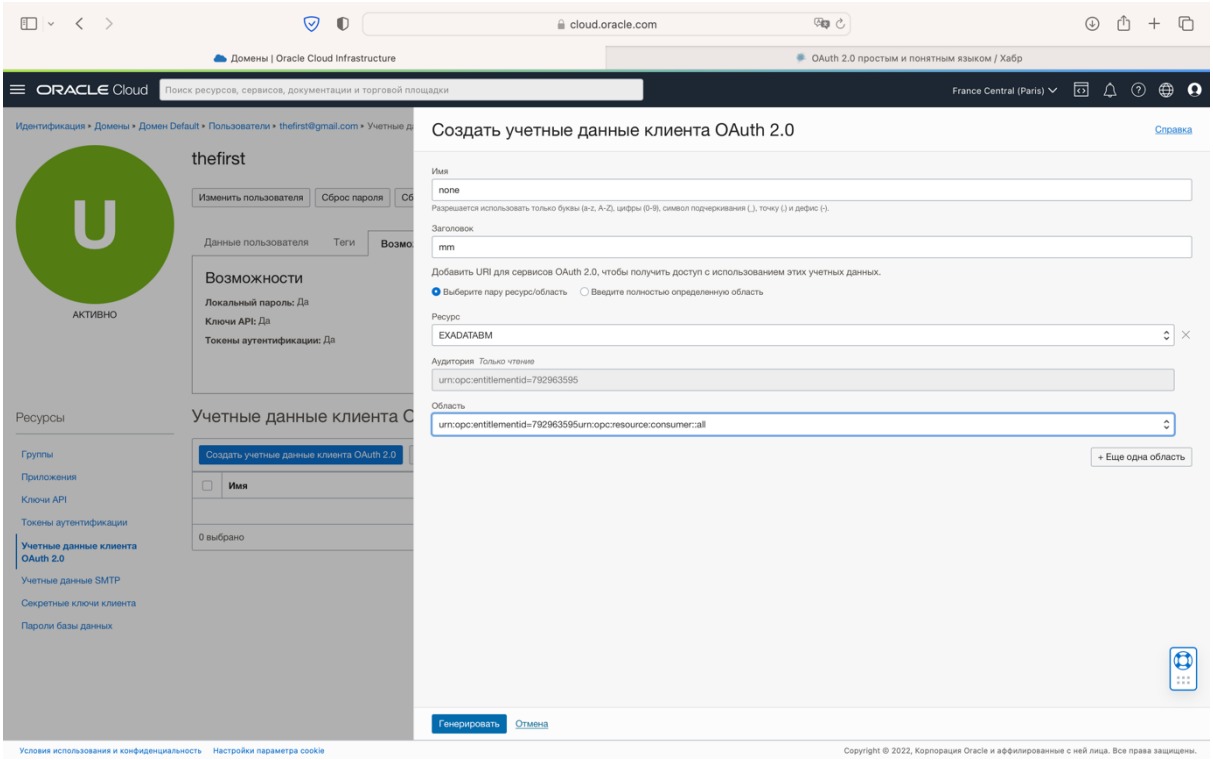

Рис. 3.4 Редагування користувача Oracle IAM

Адміністратор може налаштувати для користувача вхід аутентифікацію по протоколу OAuth 2.0. Тут необхідно адміністратору налаштувати точку на сайті сервісу для авторизації користувача. Після чого користувач зможе авторизуватись за допомогою своїх даних.

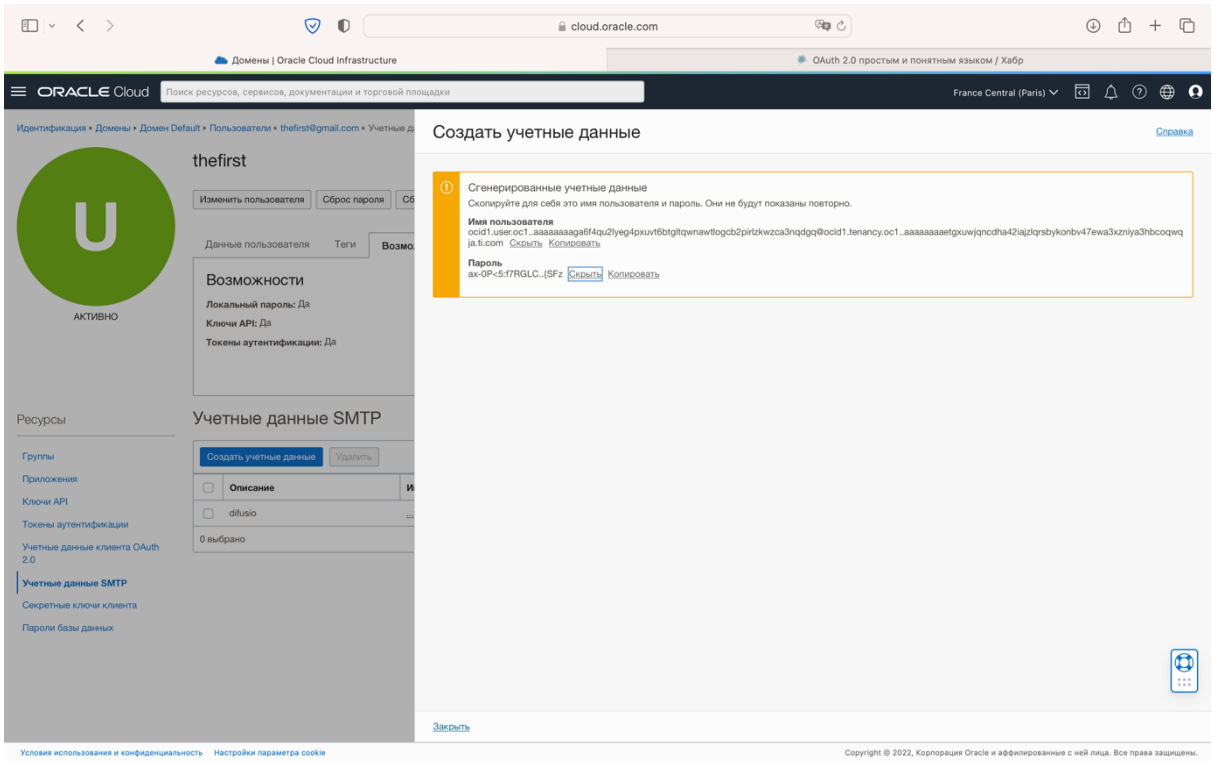

Рис. 3.6 Редагування користувача Oracle IAM

Кожен користувач, що створений у Oracle може редагувати свої дані електронної адреси, але система не дозволяє тримати на одному користувачеві більше двох електронних скриньок. Для цього необхідно створювати новий обліковий запис.

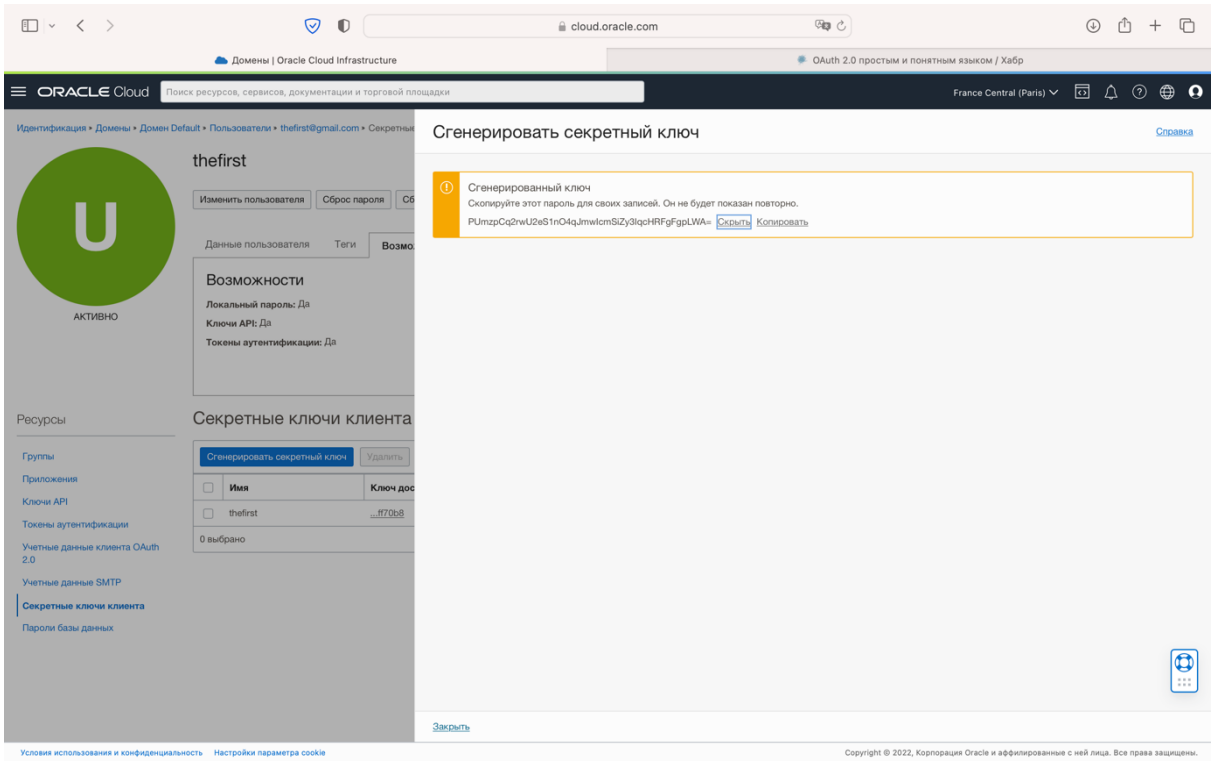

Рис. 3.7 Редагування користувача Oracle IAM

Секретні ключі генеруються не більше двох штук задля роботи з API сервісами сумісними з Amazon S3. Вони використовуються у парі з ключем доступу, які пов’язані з логіном користувача. Користувачі мають можливість управління своїми ключами від самого початку, це дозволяється з урахування базової політики безпеки. Та для роботи з API сервісами сумісними з Amazon S3 необхідний додатковий доступ.

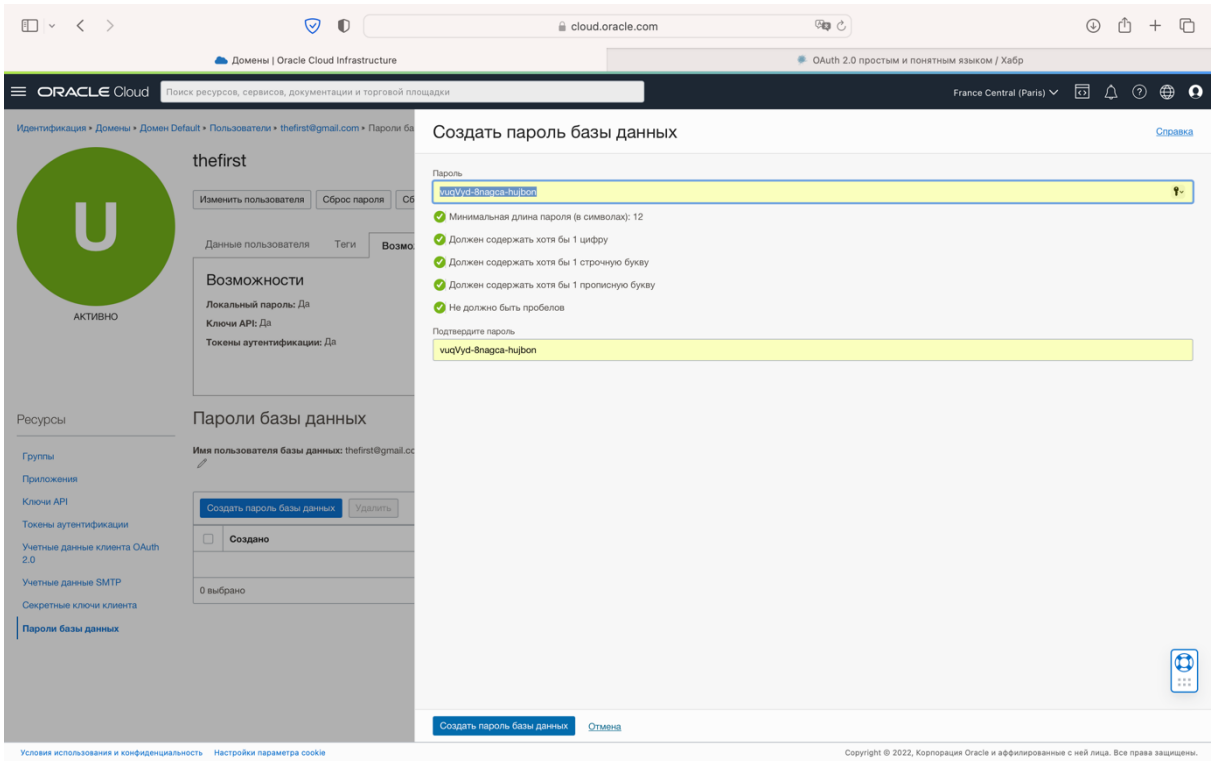

Рис. 3.8 Редагування користувача Oracle IAM

Для забезпечення необхідного рівня безпеки користувачам пропонується застосування паролів для своїх баз даних. При цьому є жорсткі вимогу до паролю. Використання імен облікових записів баз даних IAM та паролів баз даних IAM для доступу підвищує безпеку, і таким чином дозволяє адміністраторам IAM централізовано керувати користувачами. А також, доступом користувачів до паролів баз даних в рамках IAM, а не локально в кожній базі. Коли користувач залишає організацію, його обліковий запис IAM призупиняється, таким чином, доступ до всіх баз даних автоматично призупиняється. Цей метод виключає можливість використання старих облікових записів на серверах баз даних після звільнення користувача.

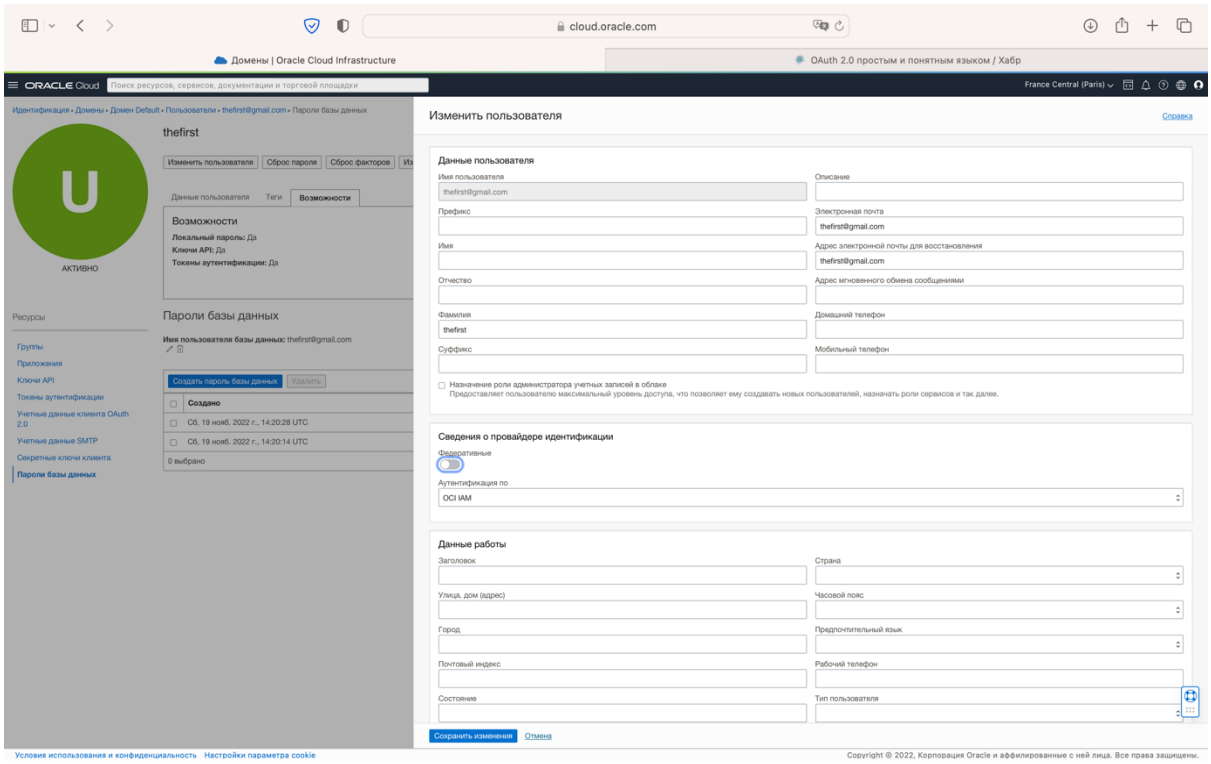

Рис. 3.9 Редагування користувача Oracle IAM

Після того, як адміністратор додав користувача можна також вносити зміни до запису, та надавати більше необхідної інформації. Це може бути як атрибут, чи телефон, чи місце роботи співробітника. Зазвичай відділ кадрів або сам заповнює цю інформацію, чи надсилає заповнену форму адміністратору, котрий вже сам переносити цю інформацію до бази.

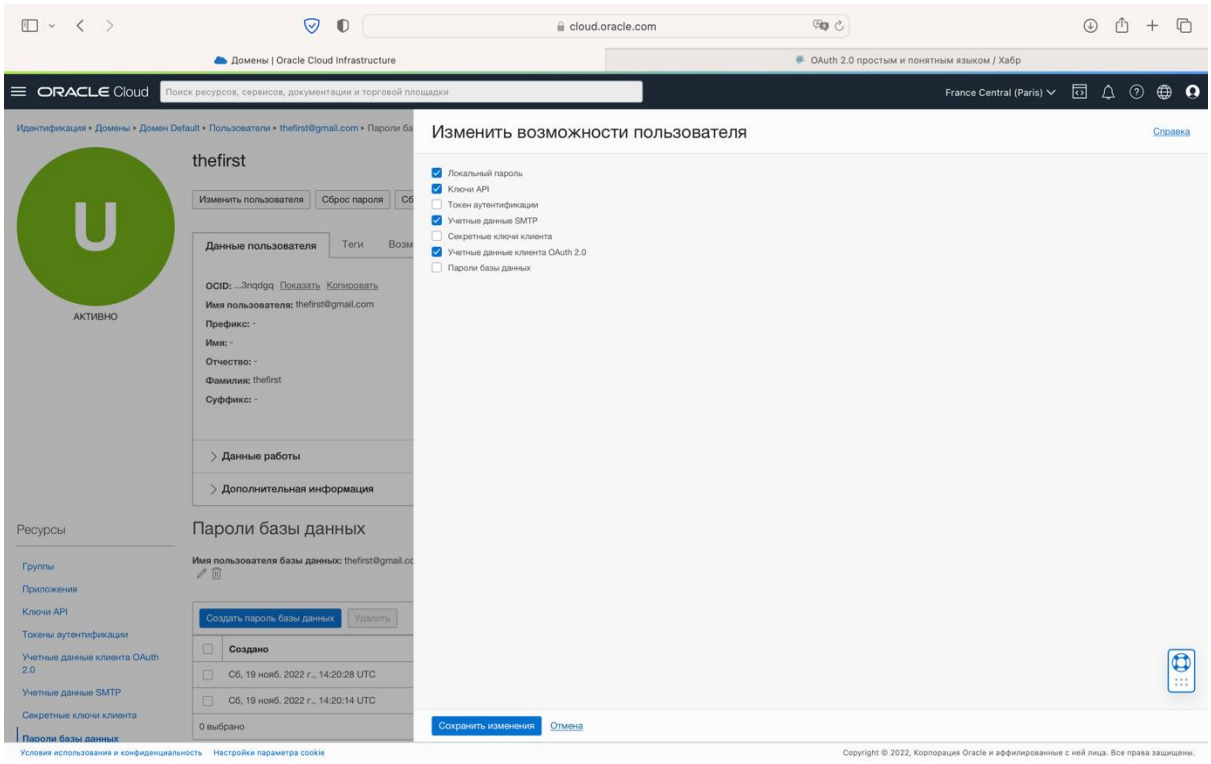

Рис. 3.10 Редагування користувача Oracle IAM

У адміністратора є можливість внесення змін щодо можливостей користувача використовувати різноманітні способи входу до мережі. Зазвичай, рекомендується мати необхідний мінімум таких методів, котрі збігаються з політикою організації. Не рекомендується вмикати їх всі, адже це може надавати більше можливостей зловмисникам для несанкціонованого входу.

На цьому етапі налаштування для конкретних користувачів закінчуються, залишається створити та додати групи і налаштувати двох факторну аутентифікацію користувачів.

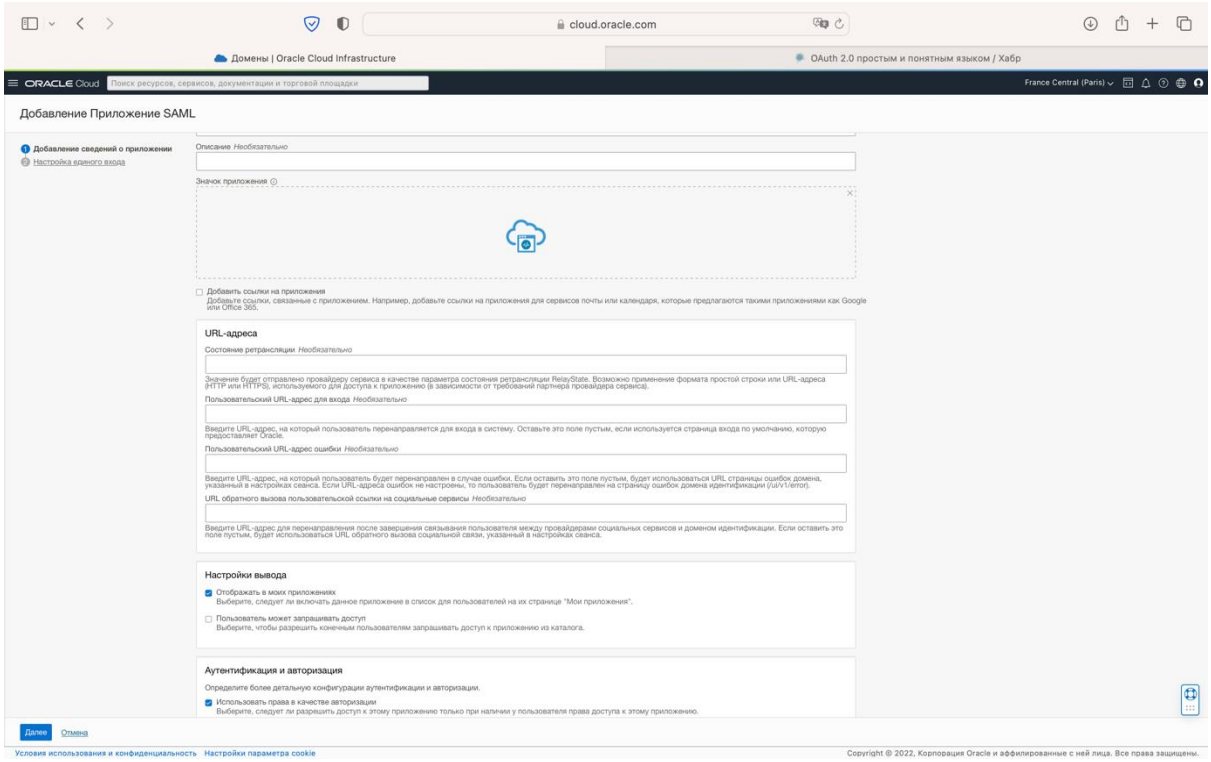

Рис. 3.11 Налаштування безпеки Oracle IAM

Налаштування технології входу SAML є складовою частиною налаштування технології єдиного входу до системи користувачем. Тут заздалегідь визначаються необхідні програми та додатки з цією технологією та можливість користувача генерувати запити на додання йому такого входу. І додається сторінка організації для аутентифікації користувача в мережі.

Далі, можливо вибирати необхідний рівень шифрування повідомлень, в котрих будуть передаватися ці дані. Зазвичай вибирають не надто складний алгоритм шифрування, для пришвидшення його обробки сервером і мережеві більш захищені протоколи https Та адреси перенаправлення у разі успішного і неуспішного входу в систему. Присутня можливість додання сертифікатів для перевірки.

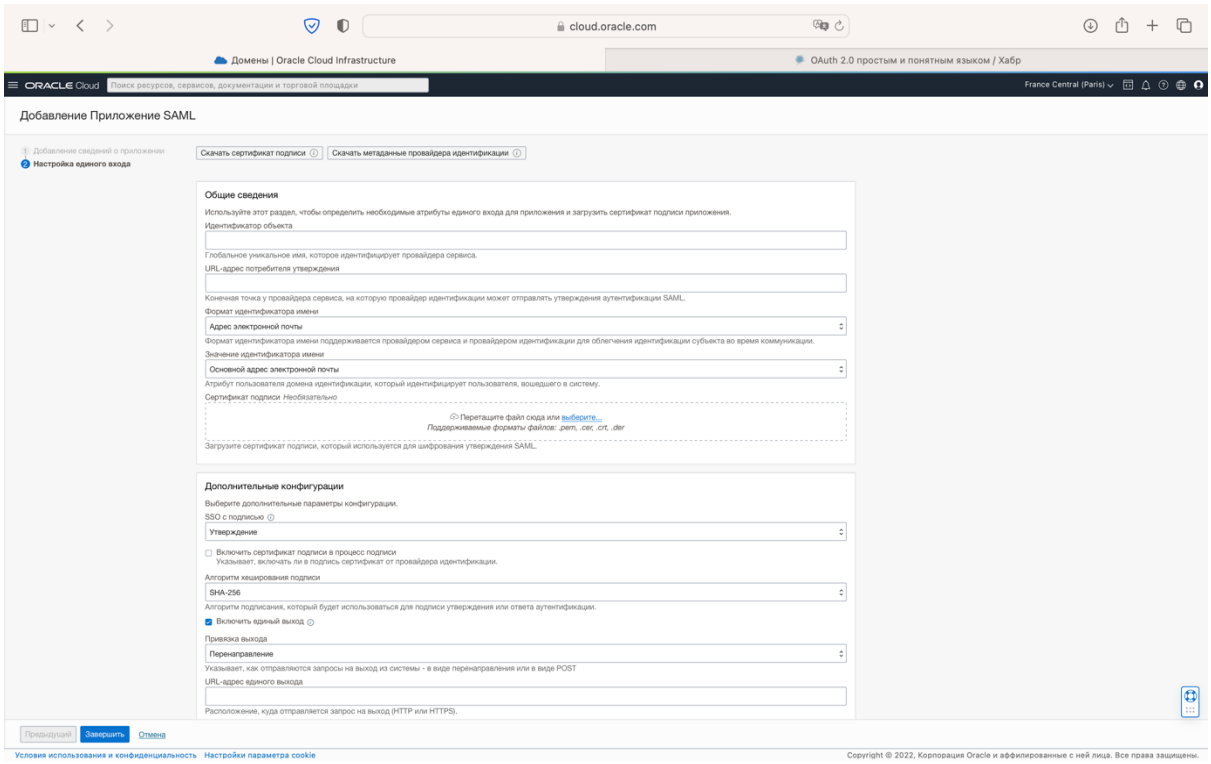

Рис. 3.12 Налаштування безпеки Oracle IAM

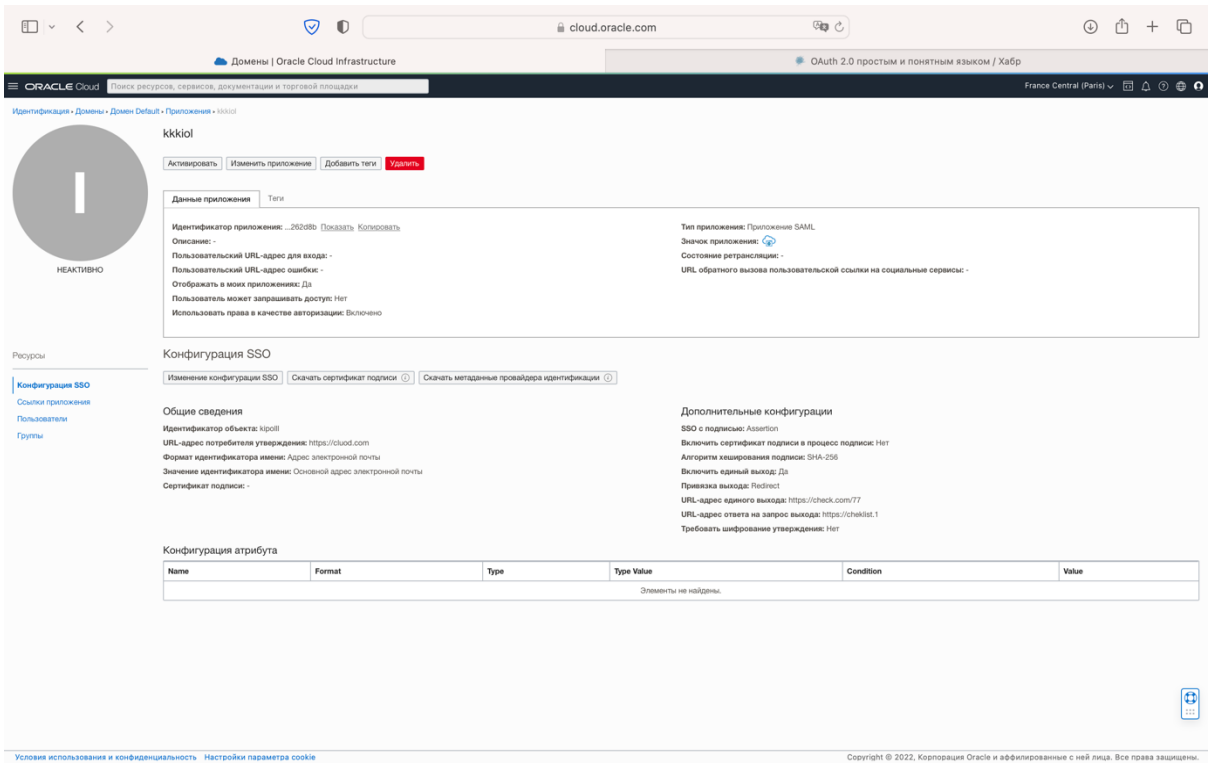

Рис. 3.13 Налаштування безпеки Oracle IAM

Сторінка додатку, вхід до якого дозволений через протокол SSO має приблизно такий вигляд. Де відображаються його назва, малюнок та всі налаштовані адреси та методи шифрування при передачі інформації. При необхідності є можливість всієї конфігурації конкретного додатку.

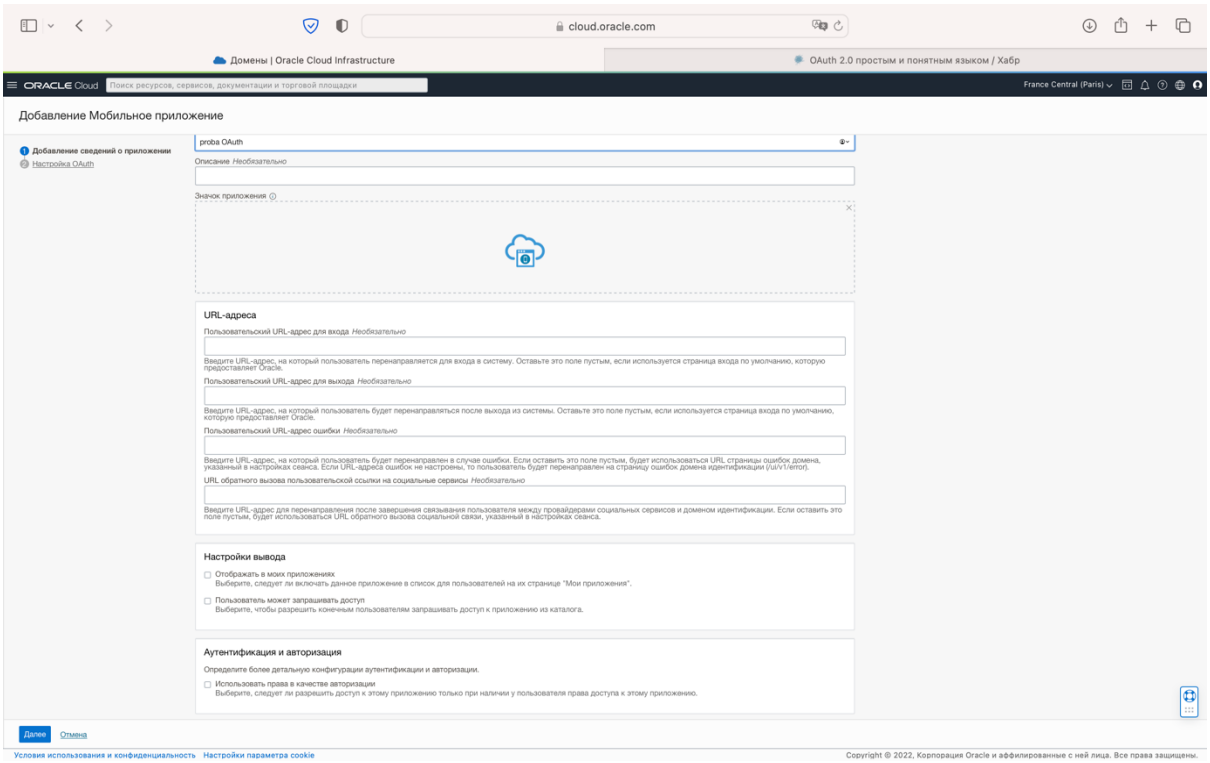

Рис. 3.14 Налаштування безпеки Oracle IAM

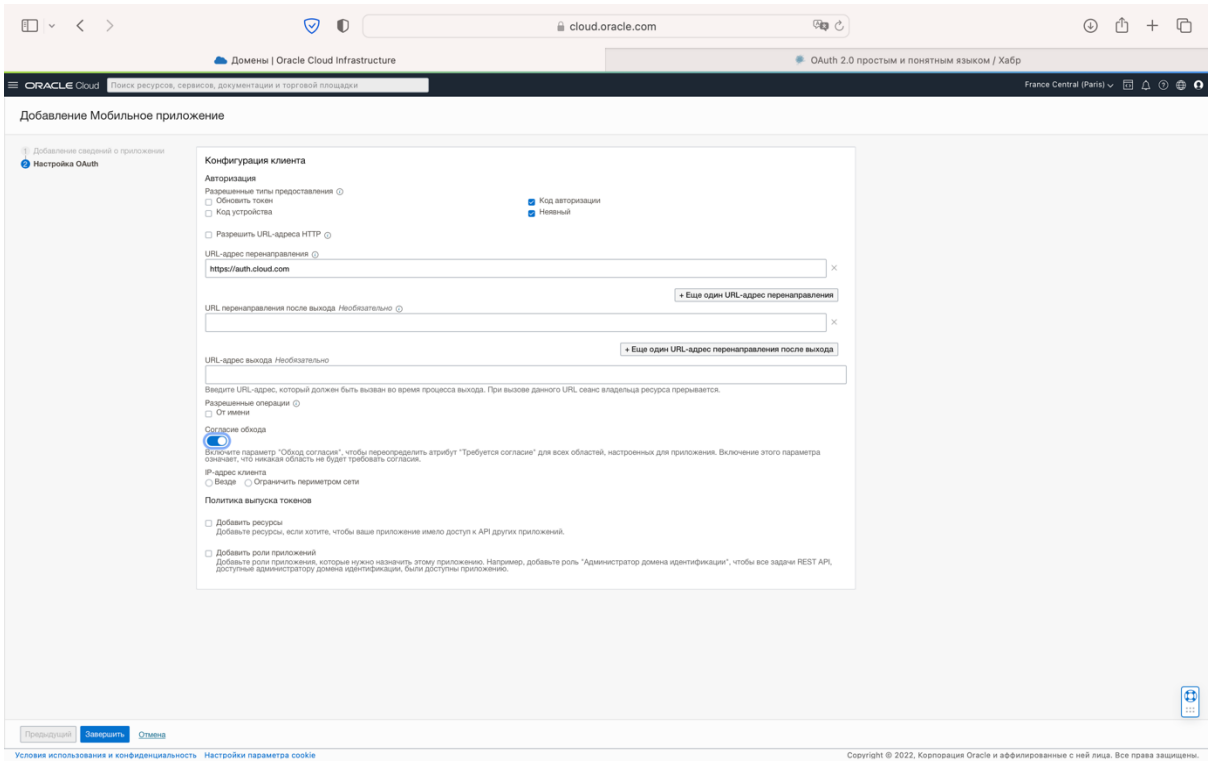

Рис. 3.15 Налаштування безпеки Oracle IAM

Система пропонує також можливість налаштування протоколу OAuth 2.0. Для його налаштувань досить вводу необхідних посилань на джерела та сайти перенаправлення запитів від користувачів. Досить дивно, що не пропонується шифрувати або перевіряти на шифрування такі запити.

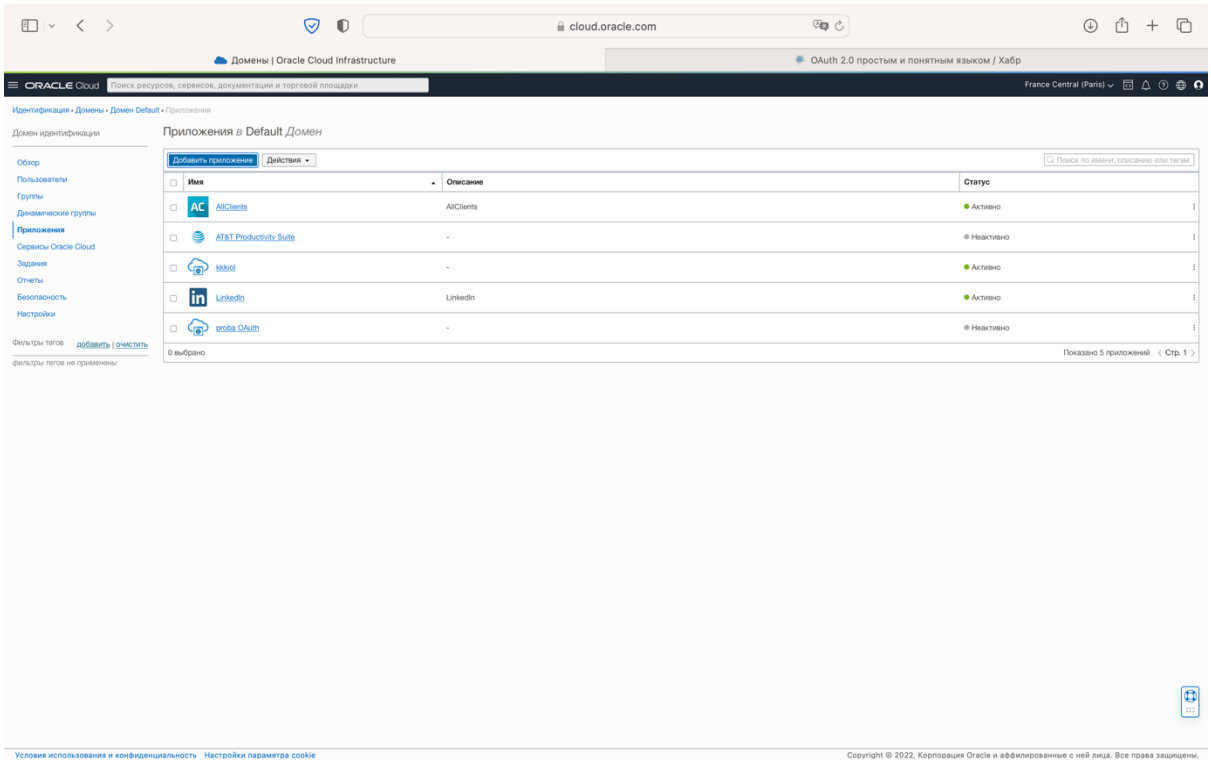

Рис. 3.16 Налаштування безпеки Oracle IAM

Існує можливість додавання застосунків до можливих в організації. На ознайомчій версії таких застосунків максимально можливо лише шість. При цьому зберігається досить великий вибір, серед яких фони поділені на категорії організація сама вибирає які застосунки мають використовувати працівники та орендує ліцензії на їх використання. Ціна ліцензії залежить від кількості працівників.

Такі додатки можливо як активувати, так і тримати на паузі, якщо необхідно обмежити до них доступ (напр. ввести глобальні зміни).

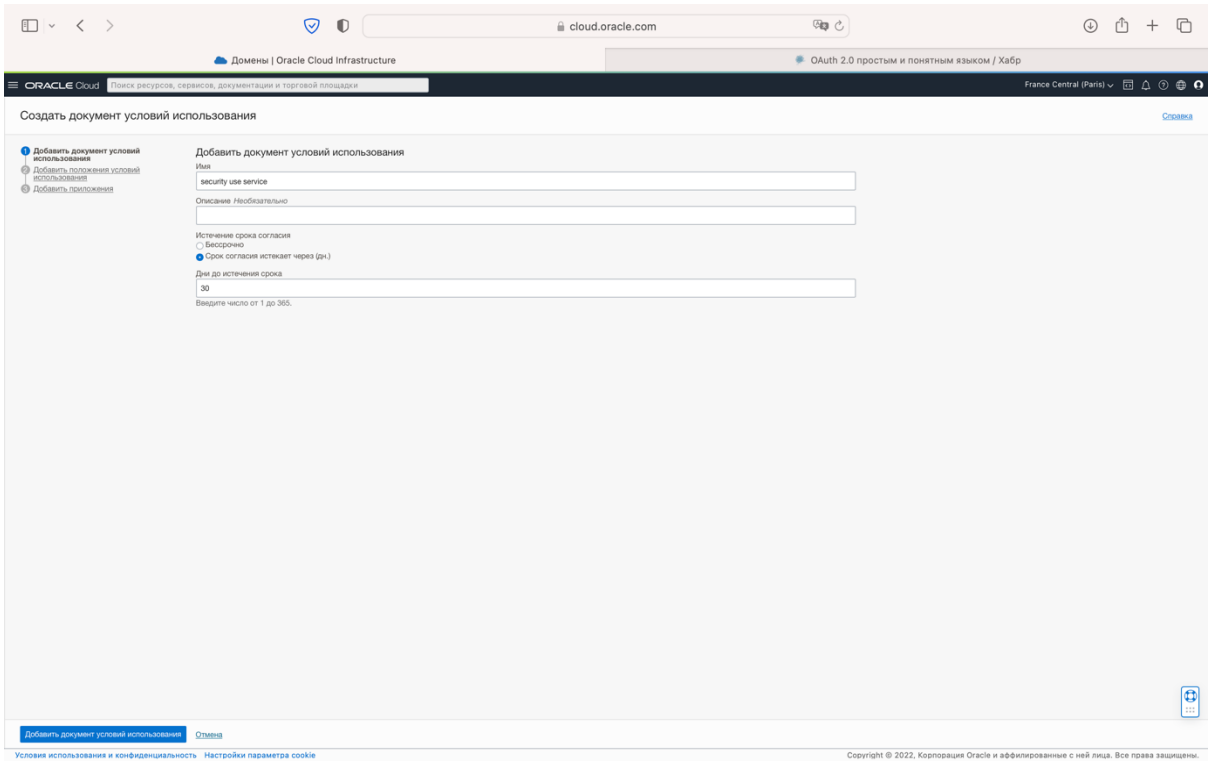

Рис. 3.17 Налаштування безпеки Oracle IAM

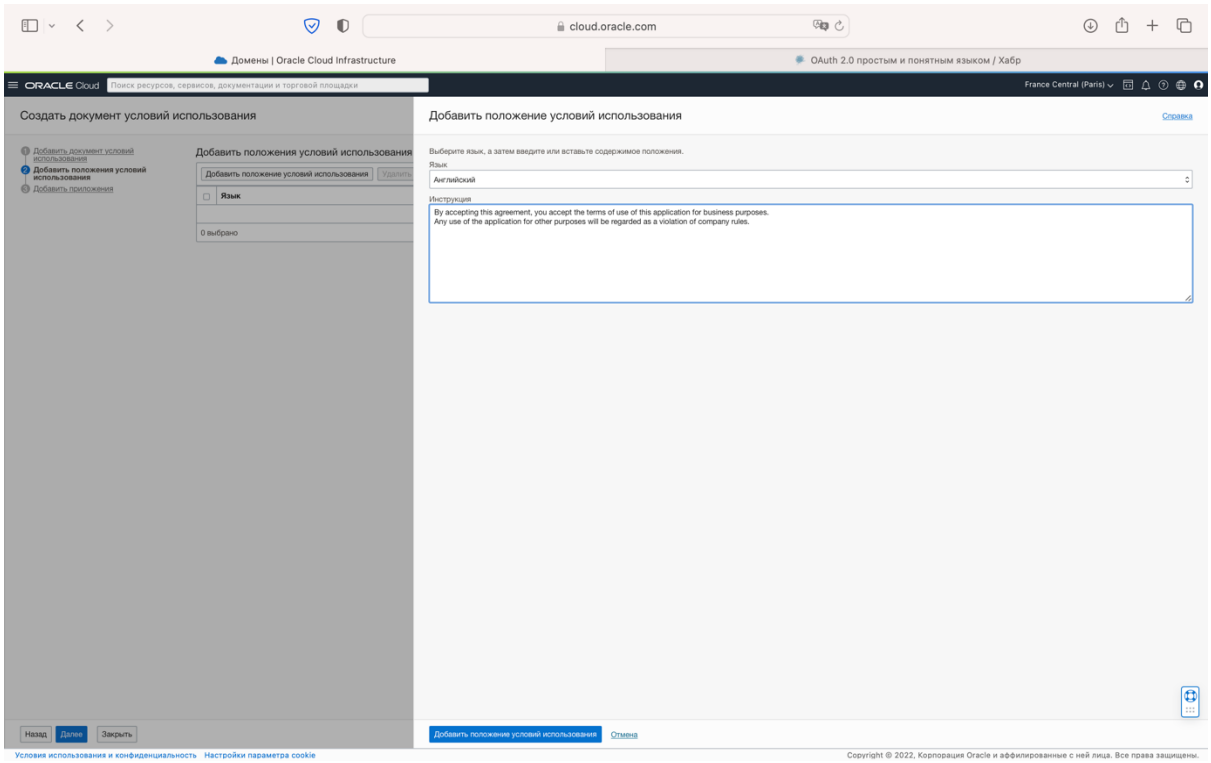

Рис. 3.18 Налаштування безпеки Oracle IAM

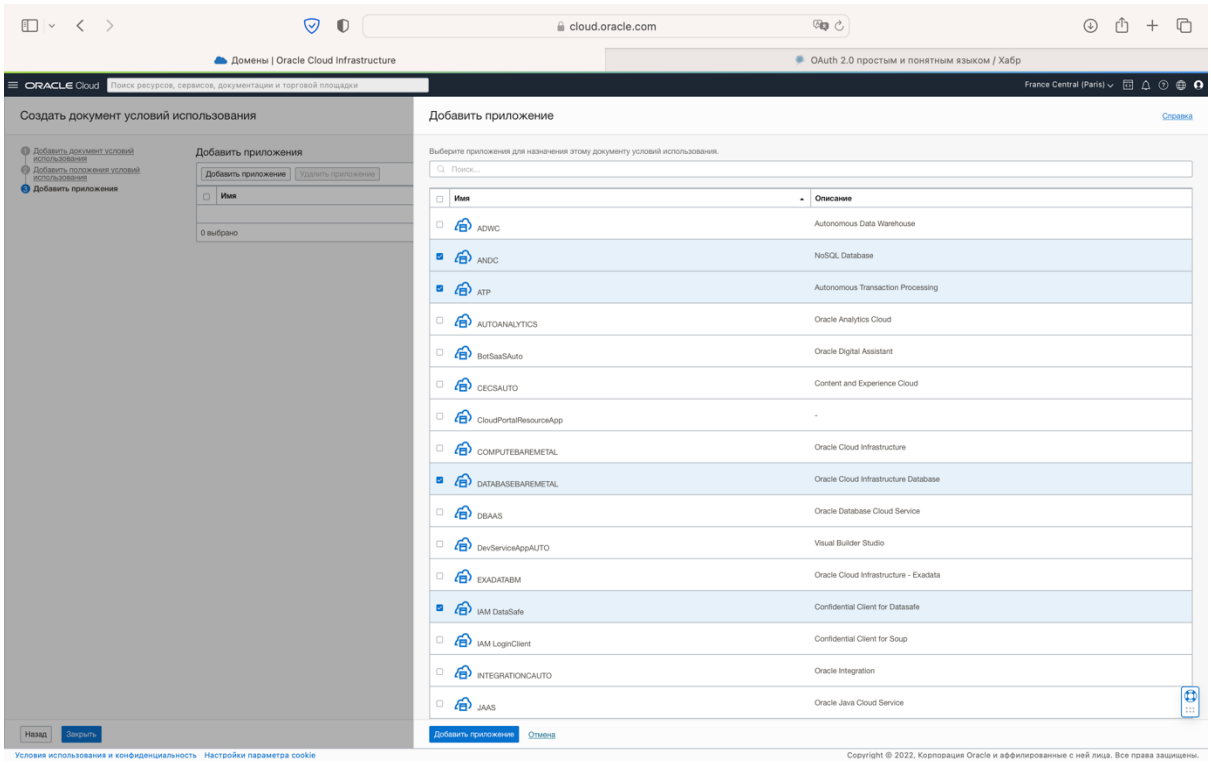

Рис. 3.19 Налаштування безпеки Oracle IAM

При використанні ліцензійного програмних рішень досить часто користувачів просять ознайомитись із правилами користування та інструкціями. У адміністраторів є можливість написати повідомлення, котре побачать та наддадуть підтвердження користувачі. Після чого доступ буде дозволений. Можливо написати таке повідомлення як на всі додатки, так і на деякі вибрані.

Зазвичай такі повідомлення стосуються безпеки використання та нагадування про відповідальність кінцевого користувача за свої дії в системі. Окрім тих, які користувач має підписувати під час прийому на роботу. Такі політики безпеки мають бути створені та погоджені з керівництвом на початкових етапах розвитку організації, та періодично має відбуватися їх перегляд та доповнення.

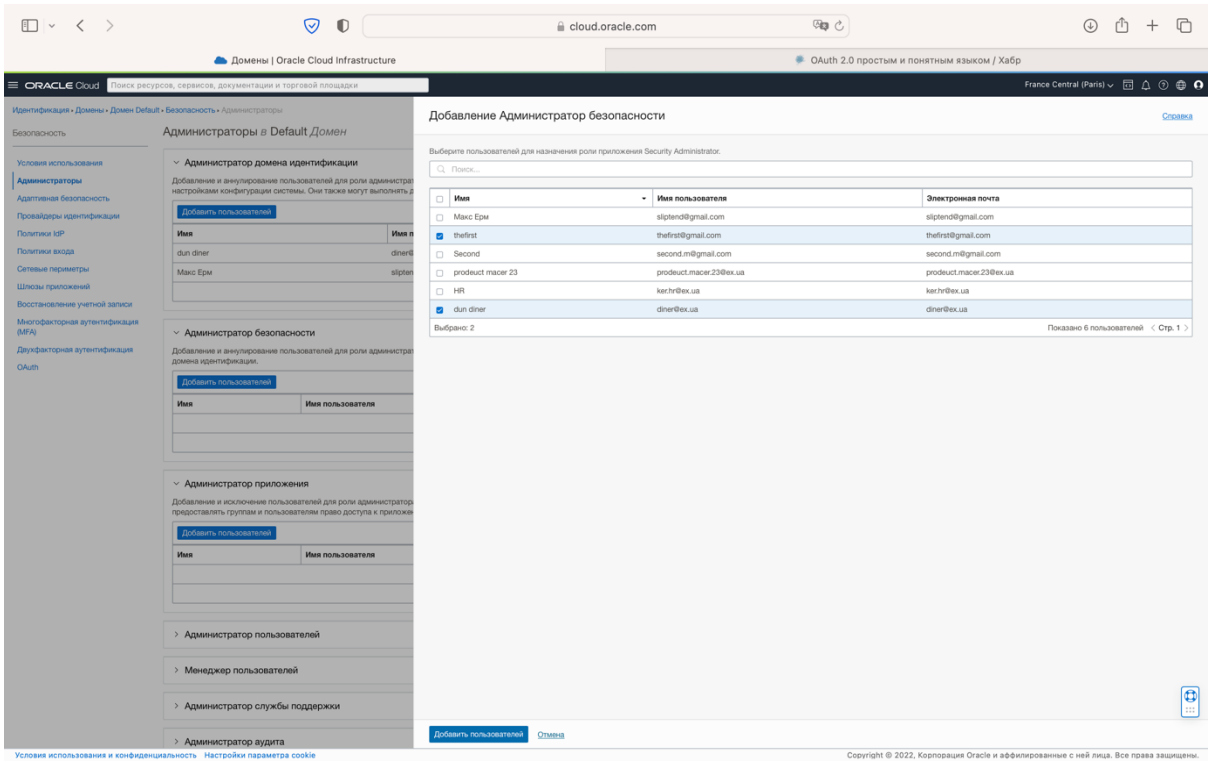

Рис. 3.20 Налаштування безпеки Oracle IAM

Через присутність великої кількості співробітників (адже система на таку кількість і розрахована) обов’язки по адмініструванню користувачів мають бути розосередженні між кількома співробітниками. Вкрай небажано, аби однин аккаунт мав права доступу на всіх напрямках адміністрування. Керування аккаунтами передбачає також своєчасне блокування або ж видалення доступів у разі закінчення їх актуальності (зміна ролі, відпустка, звільнення). Цим займається окрема адміністративна роль.

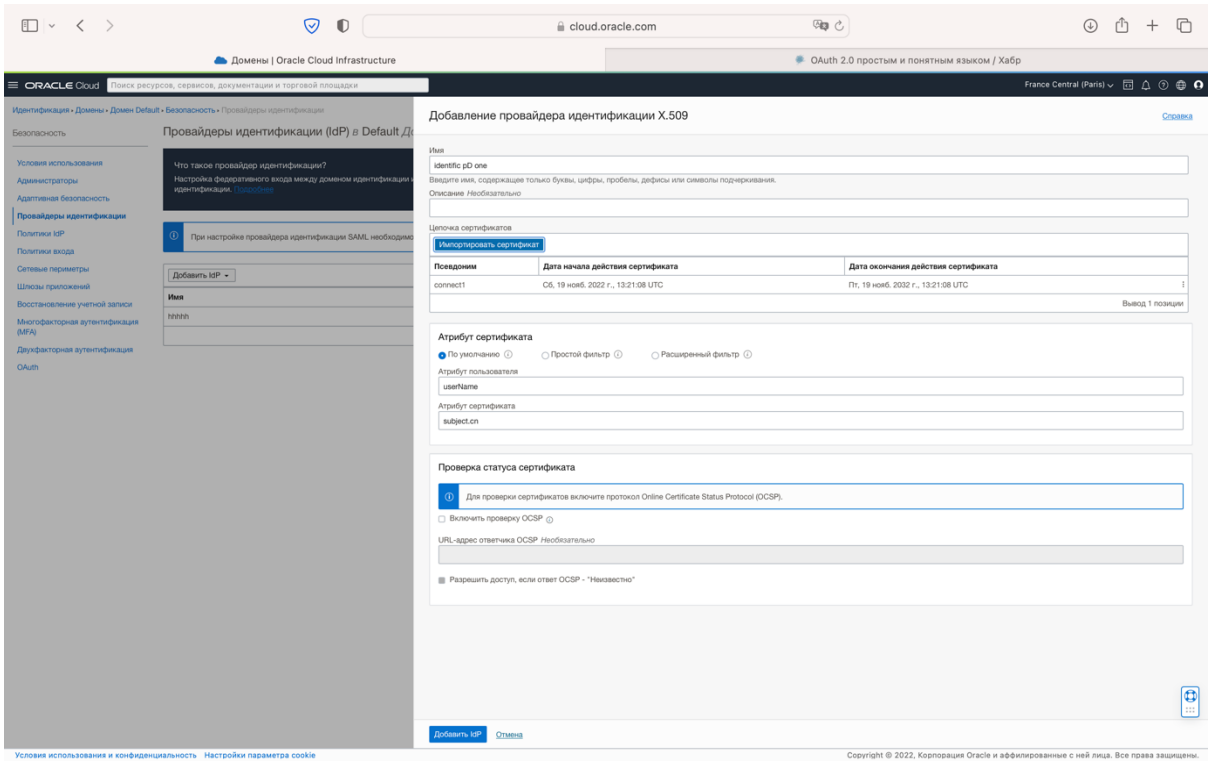

Рис. 3.21 Налаштування безпеки Oracle IAM

При налаштуванні безпеки є варіант з забезпеченням підключення провайдеру ідентифікації X.509. Цим варіантом варто скористатись як додатковим, разом з сертифікатами відповідності та звичними логіном паролем для безпечної аутентифікації користувачів в мережі. Добавляється ім’я та сам список вже налаштованих сертифікатів з ключами доступу для відповідних користувачів.

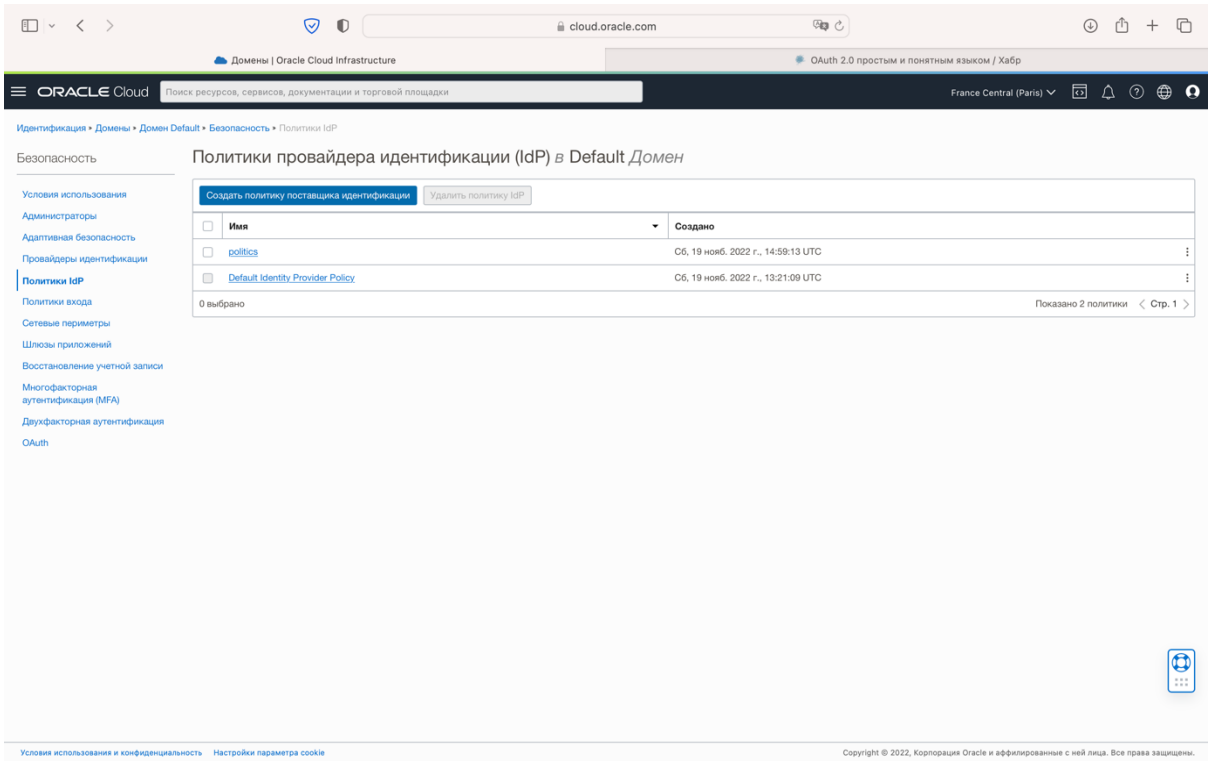

Рис. 3.22 Налаштування безпеки Oracle IAM

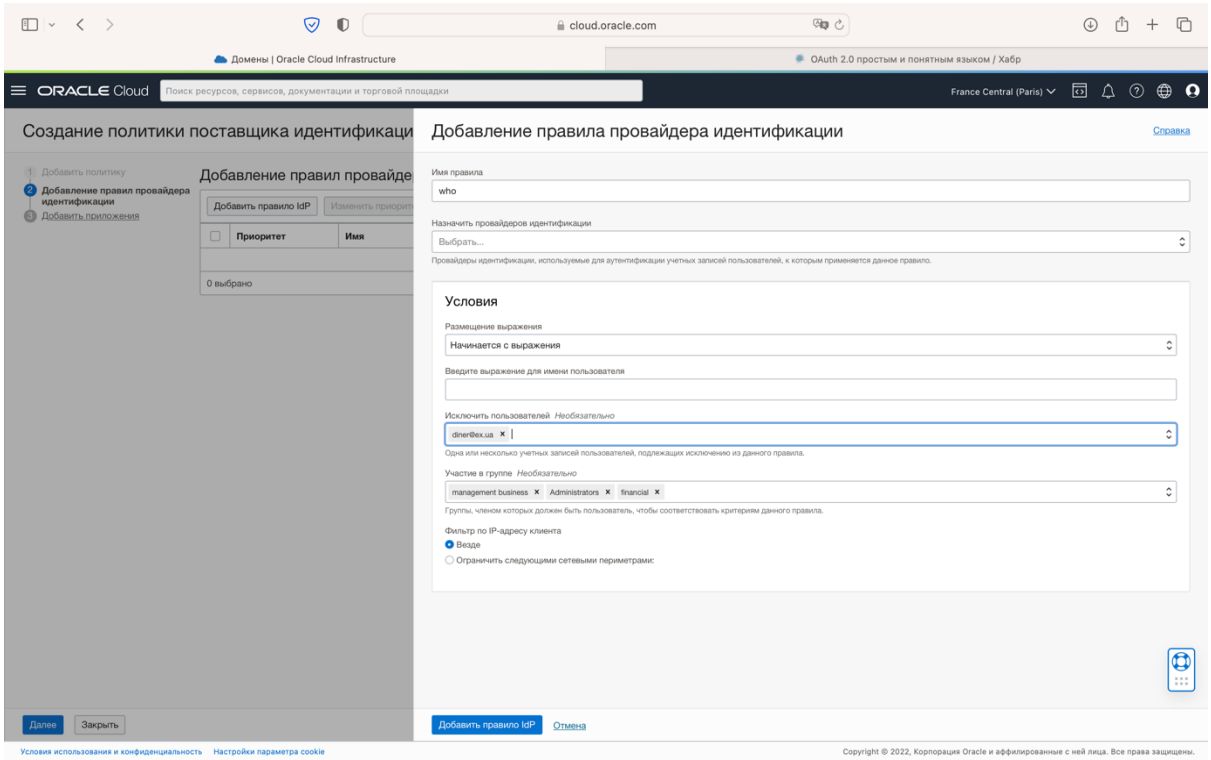

Рис. 3.23 Налаштування безпеки Oracle IAM

Крім базової політики ідентифікації (IdP) необхідно додати нові до бази для забезпечення необхідного рівня безпеки. Зв'язавши обліковий запис користувача домену ідентифікації з соціальними обліковими записами користувача, користувач може отримати доступ до домену ідентифікації, використовуючи свої соціальні облікові дані, як-от Facebook, Google, LinkedIn, Microsoft і Twitter. Таким чином пов’язуються дві бази для аутентифікації користувачів. Також можна додати чи виключити таку можливість для групи чи окремих користувачів.

Такий метод підходить лише до обмеженої категорії користувачів, та є не бажаним через свою небезпечність з витоку інформації компанії. Сервіс дозволяє налаштувати кілька таких правил.

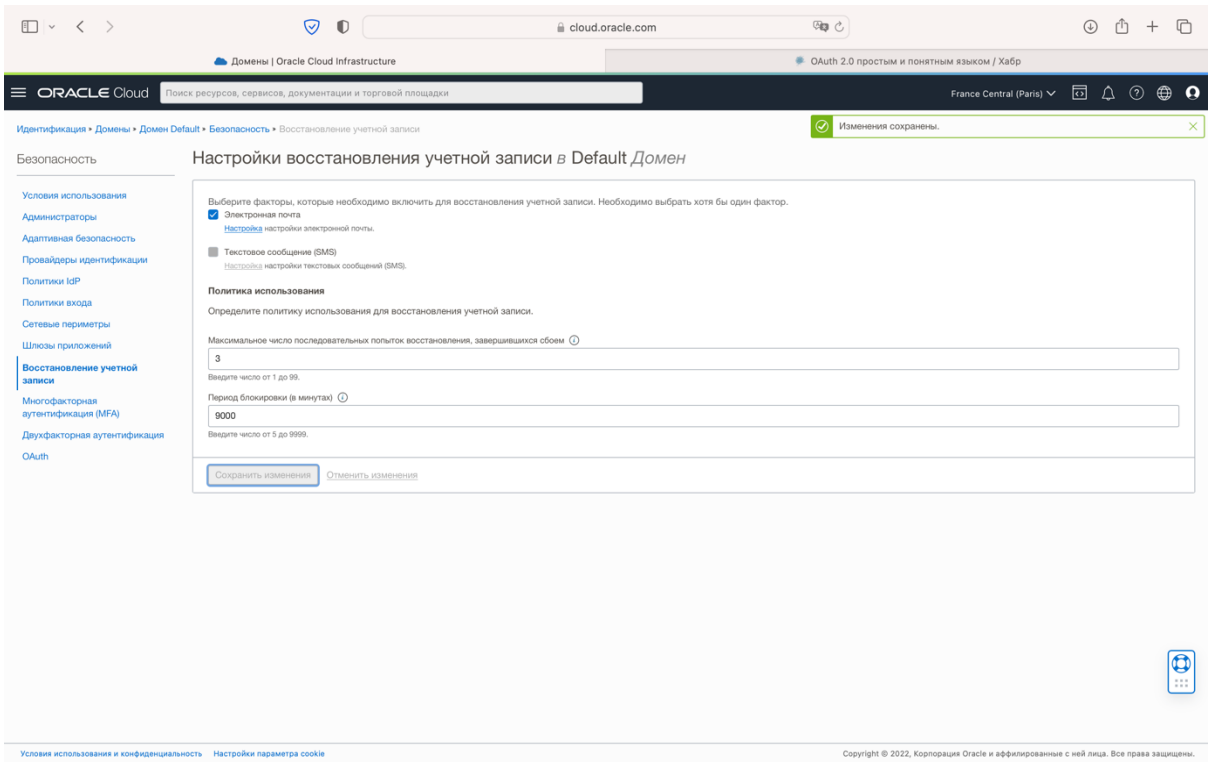

Рис. 3.24 Налаштування Oracle IAM

Існує політика з відновленням облікових записів, найкраще їх настроювати з жорсткими рамками для користувача. Аби уникнути несанкціонованого доступу обмежити кількома спробами, після котрих необхідно буде звертатися до адміністратора. Та часу блокування, для захисту від атак зловмисника необхідно виділяти кілька годин.

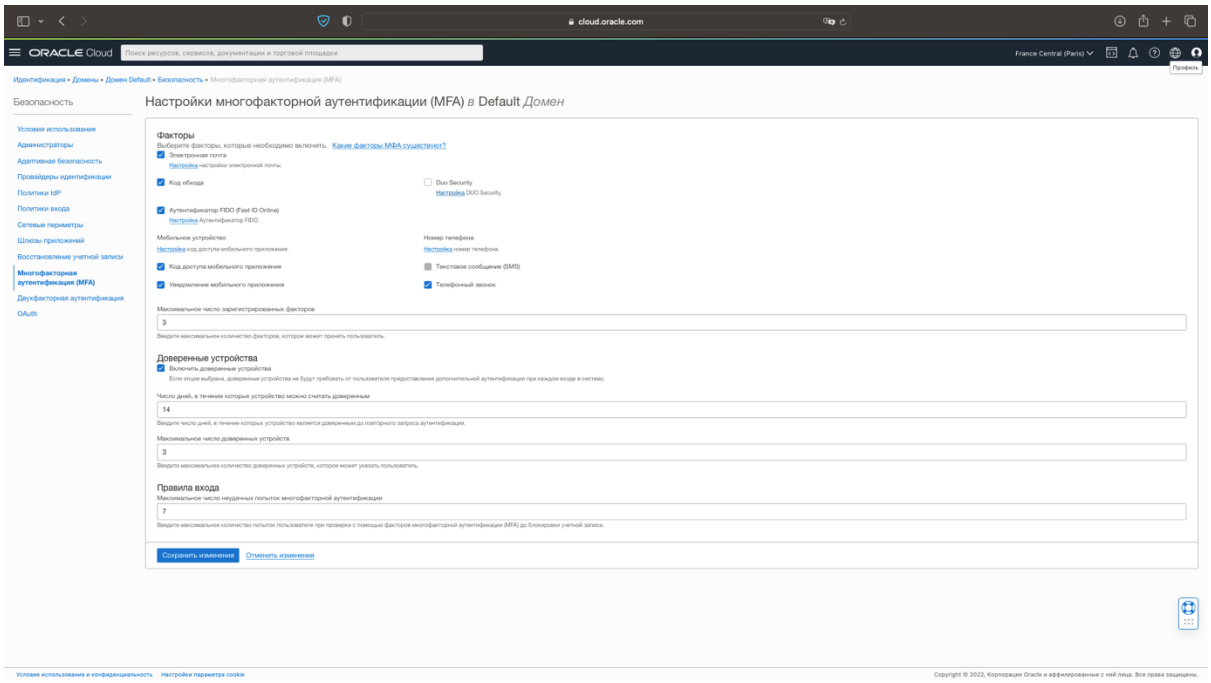

Рис. 3.25 Налаштування безпеки Oracle IAM

Налаштуваннями MFA також можливо досить сильно ускладнити життя зловмисників, котрі намагаються отримати несанкціонований доступ до мережі.

При виборі варіантів факторів входу до облікових записів маже бути використана максимальна різноманітність. Але задля безпеки увімкнених таких факторів має бути обмежена кількість, аби не доводилося контролювати вичерпну кількість приладів. Та правила для самих пристроїв мають бути жорсткими, аби самі пристрої не були скомпрометовані. Для цього зазвичай обмежують пристрій

актуальною версією прошивки та наявністю увімкненого паролю на самому пристрої. Та необхідну кількість невдалих запитів обмежують.

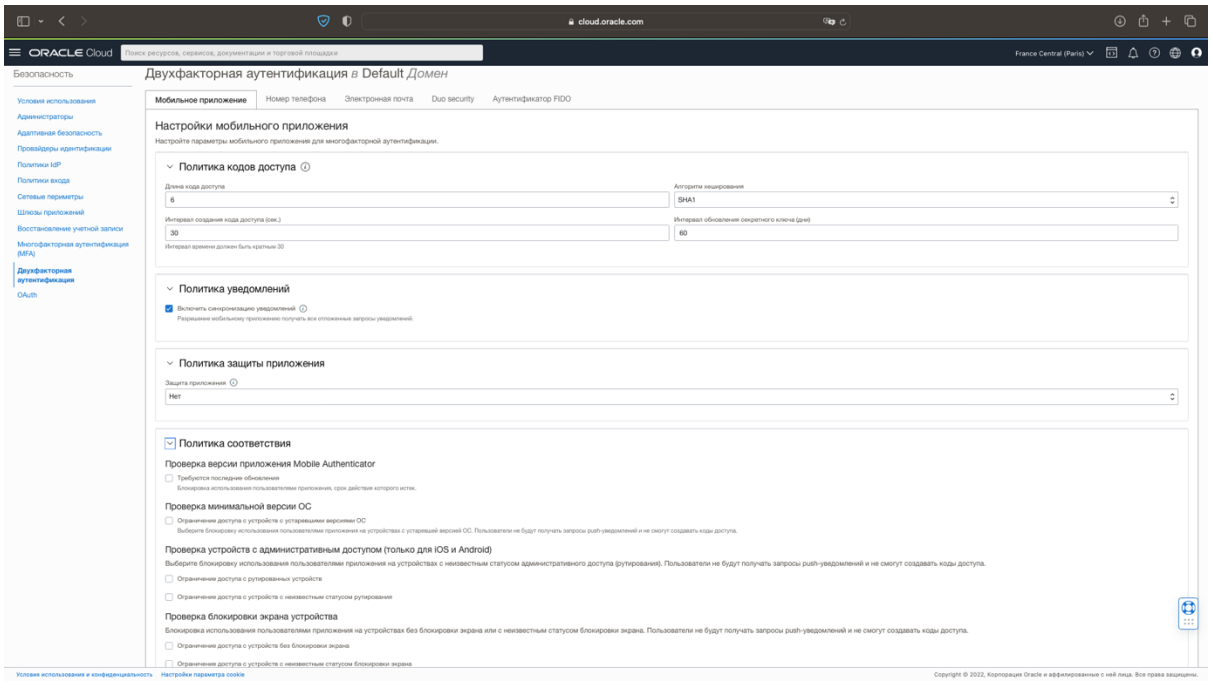

Рис. 3.26 Налаштування безпеки Oracle IAM

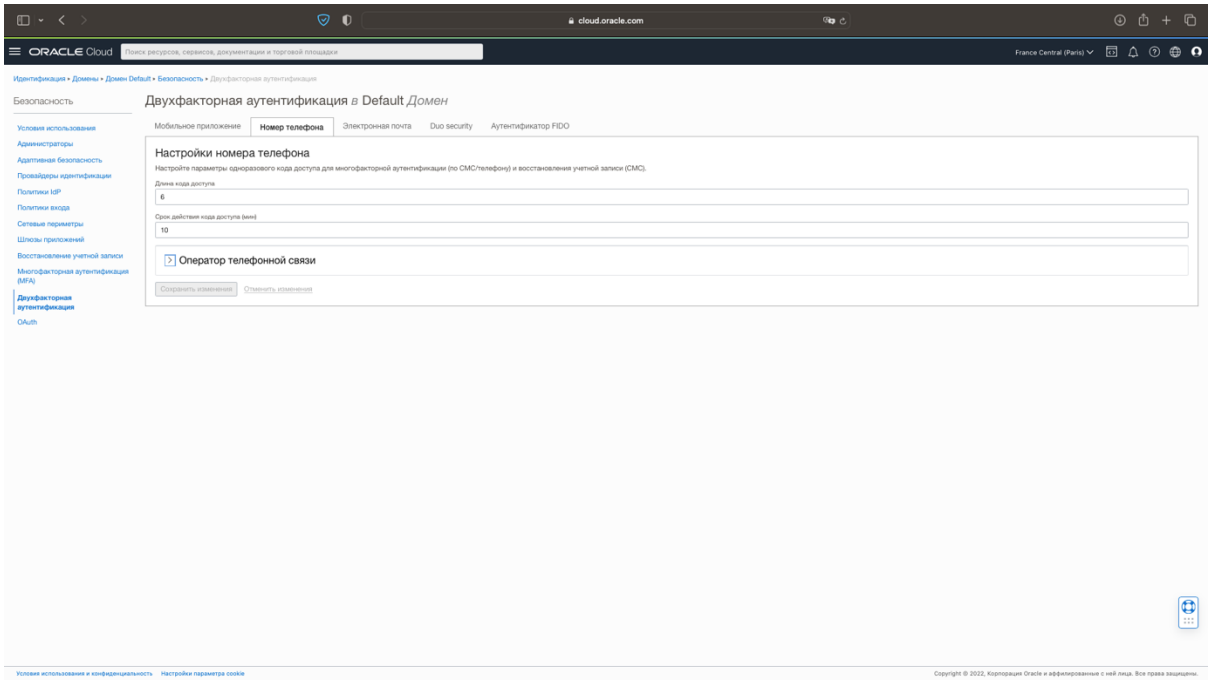

Рис. 3.27 Налаштування безпеки Oracle IAM

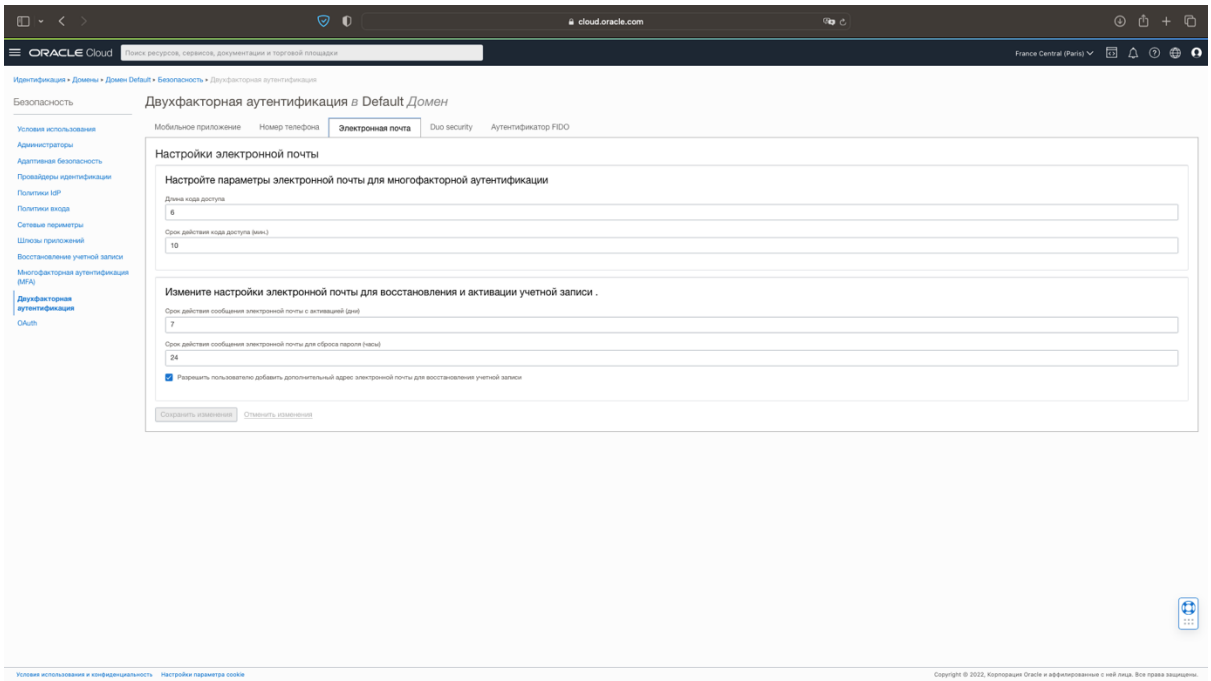

Рис. 3.28 Налаштування безпеки Oracle IAM

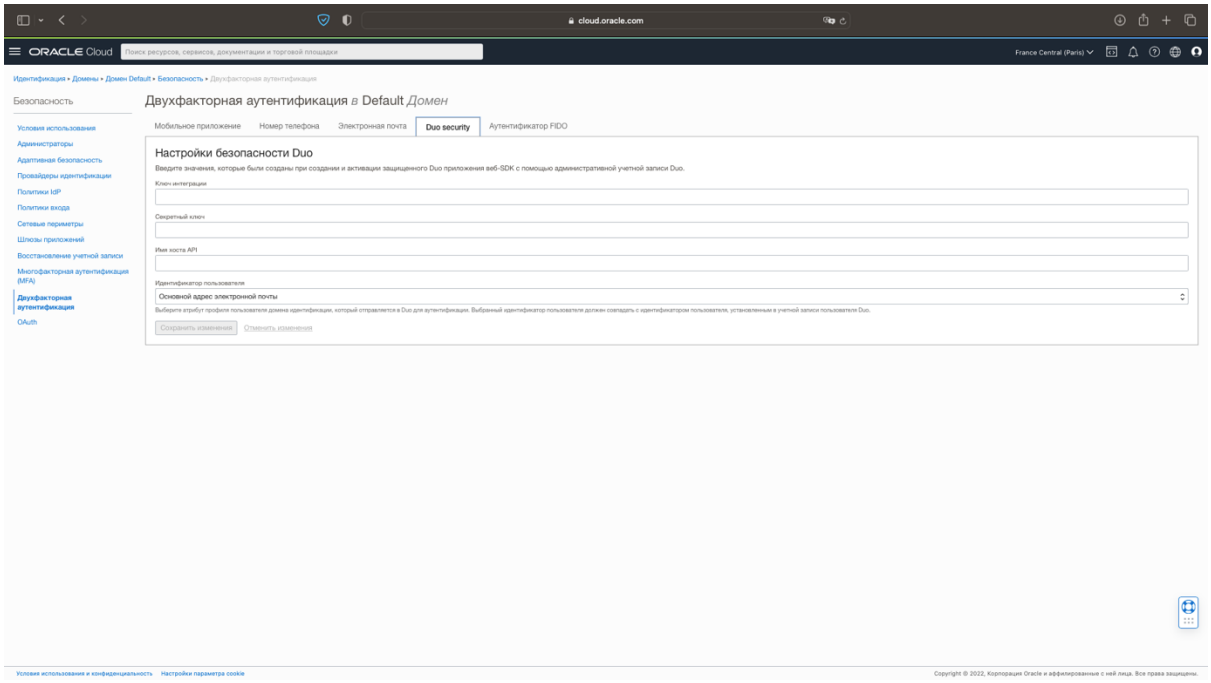

Рис. 3.29 Налаштування безпеки Oracle IAM

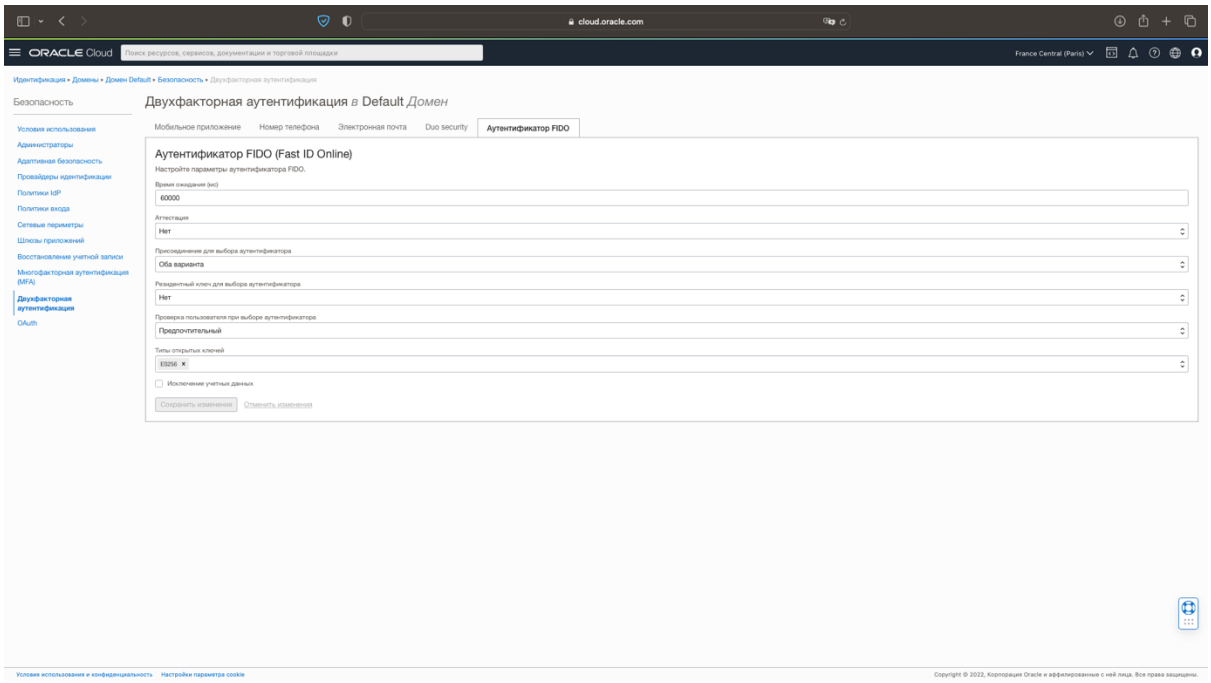

Рис. 3.30 Налаштування безпеки Oracle IAM

До політики багатофакторної аутентифікації також відносить двох факторна аутентифікація, котра має налаштовуватися окремо. Її наявність є обов'язковою через заходи безпеки. Хоча налаштування тут дечим співвідносяться з

багатофакторною аутентифікацією через свою суть. Адже наявність політик відповідності пристроїв вимогам має важливий статус (напр. телефони з будь-якими видами розблокованого ядра не мають допускатися до дозволеної категорії пристроїв).

Адміністратору пропонується налаштування усіх видів двох факторної аутентифікації окремо. Можливість підключення сторонніх додатків та видів їх шифрування. Налаштування коду допуску, котрий буде надходити до користувача у смс- повідомленні. Вдалим варіантом буде 4-6 значний код зі строком дії 5-15 хвилин. З такими ж параметрами можливо робити і повідомлення на електронну пошту. Використовуючи хмарне платформу Duo Security для управління ідентифікацією та безпекою даних можливо захищати дані організацій у великих масштабах. Oracle дозволяє налаштовувати такий сервіс за допомогою багатьох рішень (Cisco, Duo). Для цього достатньо вписати ключі організації та адрес для входу. Та вибрати метод за яким буде проведена ідентифікація користувача.

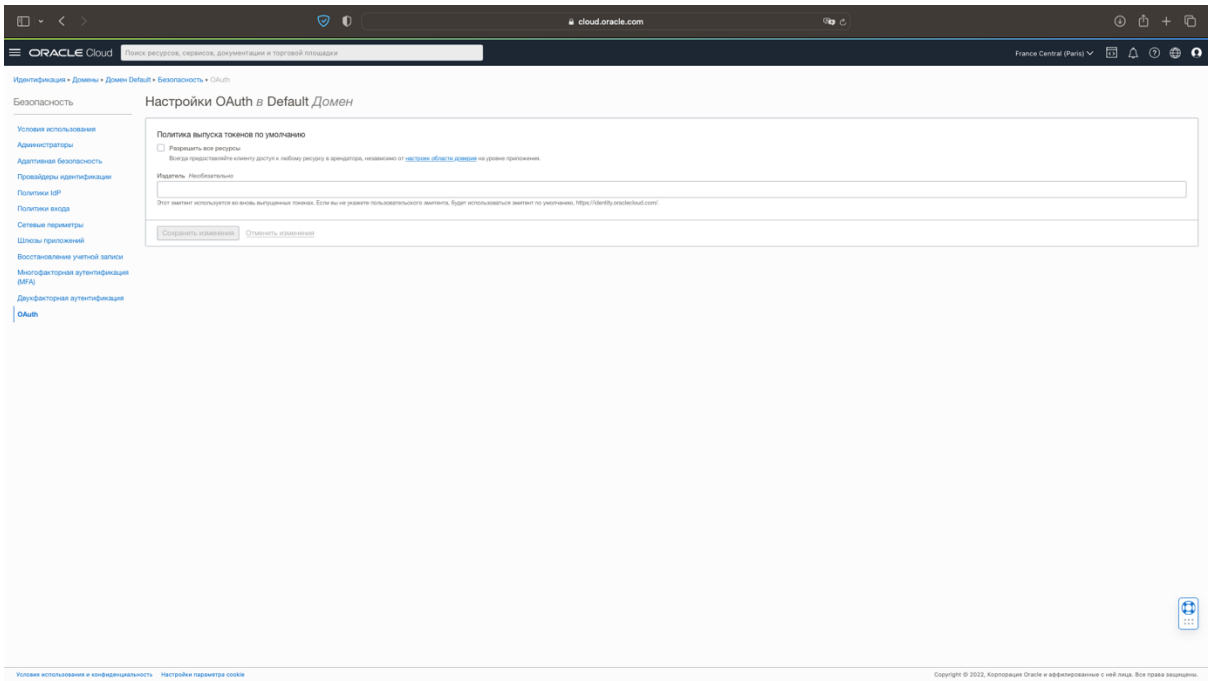

Рис. 3.31 Налаштування безпеки Oracle IAM

Останнім у списку налаштувань аутентифікації буде виступати метод OAuth, в котрій необхідно вибрати варіанти токенів для роботи. Їх достатньо одного, якщо адміністратор використовує лише один ресурс або ж додати ще.

3.2. Рекомендації фахівціям з кібербезпеки щодо управління ідентифікаціїєю та до ступом користувачів до інформаційної системи

При використанні будь-яких технологій важливо дотримуватися інструкцій котрі надає виробник (якщо такі є). Але також треба орієнтуватися на кращі світові практики використання цієї або подібних рішень для організації. Адже стандартне налаштування усіх безпекових рівнів не може гарантувати повну безпеку, тому як таке рішення для зловмисників може бути вже знайомим. Через це рекомендується переглядати політику організації стосовно безпеки як мінімум кожні 2 роки, та за необхідності вносити необхідні корективи частіше.

У такій політиці безпеки має бути чітко виділено, які функції виконують користувачі і які їм необхідні для цього права. Використовуючи правило мінімальних привілеїв можливо забезпечити певний захист даних. Ніякий користувач не повинен мати доступи до всіх файлів, це буде дуже ризиковано. При цьому кожному ресурсу має бути присвоєний ідентифікатор або належний атрибут користувача, котрий має до нього доступ. Та виділено правило, хто саме і який доступ надає користувачам. У всіх ресурсів організації має бути визначені можливі користувачі. Досить зручно створювати групи та керувати групами а не різними користувачами, наділяючи групу якимось привілеєм та додаючи до такої крупи користувачів.

Користувачі у організації мають бути ідентифікованими для можливості доступу до ресурсів. Ця ідентифікація має бути багатофакторною, включаючи

різні методи входу. Багатофакторна ідентифікацією має бути з максимально жорстким правилами підтвердження. Разом з тим, зараз досить популярним є рішення єдиного входу, яке дуже спрощує життя для користувачів надаючи їм можливість зменшення кількості разів вводу логіна та паролю.

При проектуванні системи організації необхідно з самого початку піклуватися про стандартизований вигляд служб каталогів, для забезпечення швидкої міграції у разі розширення або зміни використовуваного рішення. Адже стандартний вигляд таких каталогів може навести порядок на пришвидшення синхронізації з іншими сервісами. В цих каталогах можливо зазначення будь-якої необхідної інформації та зберігання її у вигляді бази даних. Важливим моментом зберігання таких каталогів є їх резервне копіювання, не рідше аніж один раз на добу. Зазвичай таке резервне копіювання налаштовується на найменш завантажений час доби та зберігається близько місяця, в залежності від необхідності.

Впровадження однієї технології не може гарантувати повну безпеку ресурсів організації, це має бути повне рішення з багатьма складовими для забезпечення високого рівня захисту. Не зайвими будуть сканери, антивіруси, детектори та інші програмно-апаратні засоби захисту.

При впровадженні технології управління доступом досить розумним вибором може стати рішення Oracle IAM, через багатофункціональність, сумісність з великою кількістю різноманітних каталогів та операційних систем, багату базу знань та рішень на найпопулярніші проблеми та якісну роботу служби підтримки. Підтримка багатьох сучасних сервісів, варіантів аутентифікації та великої кількості додатків виводить це рішення у топи для впровадження в сучасній організації.

ВИСНОВКИ

Система ідентифікації та управління аккаунтами впроваджується для надійного та відповідального керування та забезпечення відповідного права доступу користувачів до корпоративних документів та додатків.

Технологія IAM дозволяє вирішити такі завдання для організації:

- налагодити ефективну роботу над обліковими записами.
- Виконувати синхронізацію записів у різних додатках.
- Надавати користувачу доступи до сервісів в автоматичному режимі.
- Збільшення ефективності перевірок прав користувачів при аудиті.
- Майже автоматичне блокування невикористовуваних облікових записів.
- Запобігання неправомірному доступу до корпоративної інформації.

Основними принципами роботи з системою IAM можливо виділити:

- Розмежування доступу має працювати на рівні каталогів, без обмеження до окремих файлів.
- Права доступу мають призначатися до груп користувачів, призначення їх окремим користувачам не є ефективним рішенням.
- Права розмежовуються на рівні файлової системи.
- Не рекомендується створювати та зберігати інформаційні ресурси на окремих девайсах користувачів. Має використовуватися хмарне рішення.
- Заборона роботи з системними каталогами для звичайних користувачів.
- Єдине розміщення інформаційних ресурсів, не враховуючи резервні копії.
- Жорсткий контроль на інформаційними ресурсами, котрі містять конфіденційну інформацію.
- Використання принципу «найменших привілеїв» у роботі з файлами.

•Планові перегляди привілейованих користувачів.

В основному, для користувачів системи досить вибору прав доступу до файлів лише з «лише читання» або «читання та редагування», у рідкіших випадках власник ресурсу або адміністратор може змінювати ці права.

Під час створення ресурсів, адміністратор має виконати такі дії:

•Створити ресурс. Визначити власника та користувачів.

•Створити групи, які матимуть доступ до ресурсу. Встановити права та правила доступу.

•Додати облікові записи, ролі, або інші атрибути користувачів з доступом до цієї групи.

•Для надання користувачу до ресурсу його запис додають до необхідної групи. Для закриття доступу – видаляють з групи.

За необхідності скидання пароля або внесення змін до облікових записів користувачу необхідно:

- сформувати звернення, в який вноситься особисті дані та причина скидання пароля.
- після цього адміністратор системи або співробітник СБ скидає пароль і надсилає тимчасовий пароль на електронну пошту користувача.
- далі користувач змінює тимчасовий пароль на робочий.

Для зміни облікових даних користувач формує звернення та описує причини для зміни облікових записів. Далі у разі підтвердження таких дій керівником, вносяться зміни.

У разі наявності, такі дії можливо виконувати на порталі самообслуговування.

Адміністратори системи можуть вносити зміни в облікові записи без погодження зі співробітниками про це.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» № 2658-XII від 02.10.92, ВВР, 1992, № 48, ст.651.

2. Що таке інформаційна безпека (InfoSec)? | Захисний комплекс Microsoft [Електронний ресурс] – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec.

3. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems.

4. ДСТУ 9041:2020 Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса.

5. Закон України «Про кібернетичну безпеку України». Відомості Верховної Ради України, 2017. № 45. С. 403.

6. Стратегія кібербезпеки України. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n7 (дата звернення : 21.10.2021).

7. Cyber Security Strategy for Germany 2021 [Електронний ресурс] – Режим доступу: https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html.

8. Захист комп’ютера від вірусів. [Електронний ресурс] – Режим доступу: https://support.microsoft.com/uk-ua/windows/захист-комп-ютера-від-вірусів-b2025ed1-02d5-1e87-ba5f-71999008e026.

9. AWS Identity and Access Management Documentation. [Електронний ресурс] – Режим доступу: https://docs.aws.amazon.com/iam/?icmpid=docs_homepage_security.

10. IBM Rational Software Modeler Documentation [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/ru/rsm/7.5.0?topic=applications-java-ee

11. Oracle Cloud Infrastructure Documentation. [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en-us/iaas/Content/home.htm.

12. Понятия и обзор LDAP. [Електронний ресурс] – Режим доступу: https://pro-ldap.ru/tr/zytrax/ch2/.

13. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software. Michael Schwartz, Maciej Machulak. 2018. 383 с.

14. Что такое пользователи AWS IAM и как ими управлять? [Електронний ресурс] – Режим доступу: https://myroad.club/chto-takoe-polzovateli-aws-iam-i-kak-imi-upravlyat-cloudsavvy-it/.

15. Выбор IAM-решения: на правильные ли вещи вы обращаете внимание? [Електронний ресурс] – Режим доступу: https://www.securitylab.ru/analytics/530059.php

16. Identity and Access Management або система управління обліковими даними. Рішення Microsoft Azure AD. [Електронний ресурс] – Режим доступу: https://www.globallogic.com/ua/insights/blogs/identity-and-access-management-azure-ad/

17. Єрмак М.В. Технологія управління ідентифікацією та доступом користувачів інформаційної системи підприємства на базі Oracle Identity and Access Management. Всеукраїнська науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» 27 жовтня 2022 С. 71-72.

18. TECH Talk: Условный доступ в Azure AD. [Електронний ресурс] – Режим доступу: https://thellpa.com/ru/news/tech-talk-conditional-access-in-azure-ad/

19. OAuth 2.0 простым и понятным языком. [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/vk/blog/115163/.