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 ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ IBM SECURITY VERIFY»

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

КИЇВ – 2023

РЕФЕРАТ

Текстова частина магістерської роботи: 59 сторінок, 69 рисунків, 19 джерел.

Об'єкт дослідження – процес управління ідентифікацією та доступом користувачів до інформаційно-телекомунікаційної системи організації.

Предмет дослідження – технологія управління ідентифікацією та доступом користувачів до інформаційно-телекомунікаційної системи організації.

Мета роботи – розглянути функціонал системи управління ідентифікацією та доступом користувачів до інформаційної системи організації та розробити рекомендації щодо управління ідентифікацією та доступом користувачів.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління ідентифікацією та доступом користувачів до інформаційної системи організації.

В роботі проведено аналіз проблем пов'язаних з управлінням ідентифікацією та доступом користувачів до інформаційної системи організації та визначено мету та завдання методів та засобів управління ідентифікацією та доступом користувачів до інформаційної системи організації. Проаналізовано існуючі технології управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Досліджено методи та засоби управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення IBM Security Verify. Визначено призначення, основні функції, склад та принципи роботи програмного комплексу IBM Security Verify.

На основі досліджень проведених в роботі розглянено варіанти реалізації управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Галузь використання – кібербезпека інформаційної системи організації.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ, МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ, СИСТЕМА УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ

ABSTRACT

Master’s thesis: 59 pages, 69 figures, 19 sources.

Object of research – the process of user identity and access management in the corporate information and telecommunication system.

Subject of research – the user identity and access management technology used in the corporate information and telecommunication system.

The aim of research – to overview the functionality of the identity and access management system used in the information system of the organization and develop recommendations on identity and access management.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison, modeling of the process of identity and access mamagement in the corporate information system.

The paper analyzes the problems related to the identity and access management of users in the information and telecommunication system of the organization and defines the purpose and tasks of methods and tools of identity and access management of users to the information system of the organization. Existing identity and access management technologies to the organization's information system are analyzed.

The paper studies methods and tools for identity and access management on the example of IBM Security Verify solution. The purpose, main functions, composition and principles of operation of the IBM Security Verify software solution defined.

Based on the research conducted in the work, variants of implementing of identity and access management of users in the information and telecommunication system of the organization were defined.

Field of use – cybersecurity of corporate information system.

INFORMATION AND TELECOMMUNICATION SYSTEM, CYBER SECURITY, IDENTITY AND ACCESS MANAGEMENT, METHODS AND TOOLS OF IDENTITY AND ACCESS MANAGEMENT, IDENTITY AND ACCESS MANAGEMENT SYSTEM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IT – Інформаційні Технології

ITC – Інформаційно-Телекомунікаційна Система

IAM – Identity And Access Management

MFA – Multi-Factor Authentication

SSO – Single sign-on

ВСТУП

Актуальність дослідження. Основними методами оптимізації бізнес-процесів для підприємств сьогодення є використання інформаційних технологій та впровадження ефективного менеджменту. Враховуючи умови, що ставить перед людством сучасність, росте попит на використання віддалених робочих місць, доступ до яких має бути наданий не лише через стаціонарні персональні комп'ютери, а і різноманітні мобільні пристрої. Використання численних пристроїв, що можуть знаходитись в будь-якій точці планети, для роботи в інформаційних системах підприємств означає, що все більше підприємств будуть переносити свої системи у хмарне середовище.

Велика інформаційна система організації, що оснащена багатьма різними хмарними сервісами, має велику кількість користувачів з різними можливостями та обов'язками стає проблемною в плані управління тим які користувачі мають доступи до яких систем, а використання різними сервісами різних шаблонів доступу можуть створити проґавини у системі захисту.

Останнім часом популярності набувають системи управління ідентифікацією та доступом, що дозволяють спростити процес надання відповідних доступів та обмежень користувачам у системі та налагодити повне дотримання політик доступу до системи.

Вищенаведена інформація актуалізує тему даної магістерської роботи, зміст якої становлять дослідження технології управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення IBM Security Verify.

Об'єкт дослідження – управління ідентифікацією та доступом користувачів до інформаційної системи організації.

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

Мета роботи – розглянути можливі варіанти реалізації системи управління ідентифікацією та доступом користувачів та розробити рекомендації щодо управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Наукові завдання:

встановити сутність практик управління ідентифікацією та доступом користувачів до інформаційної системи організації;

дослідити сутність проблем управління ідентифікацією та доступом користувачів до інформаційної системи організації;

проаналізувати методи та засоби забезпечення управління ідентифікацією та доступом користувачів до інформаційної системи організації;

проаналізувати існуючі технології управління ідентифікацією та доступом користувачів до інформаційної системи організації;

проаналізувати основні функції та принципи реалізації систем управління ідентифікацією та доступом користувачів до інформаційної системи організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання варіантів системи управління ідентифікацією та доступом користувачів.

Практичне значення одержаних результатів полягає в розгляданні варіантів конфігурації технології управління ідентифікацією та доступом користувачів до інформаційної системи організації на базі рішення IBM Security Verify, а також у розробці рекомендацій щодо управління ідентифікацією та доступом користувачів до інформаційної системи.

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 АНАЛІЗ ПРОБЛЕМ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Сутність та призначення методів і технологій управління ідентифікацією та доступом користувачів

Управління ідентифікацією та доступом (IAM) – комплекс заходів, що спрямовані на отримання санкціонованого доступу до ресурсів сутністю, що має право на отримання такого доступу, в чітко визначений час та з суто позитивною метою [1, 2]. Втілення адекватного IAM є критично важливим з точки зору кібербезпеки, бо отримання ідентифікаційних даних для успішної авторизації під профілем користувача системи є одним з найпоширеніших та найефективніших способів реалізації великих кібератак [3]. До того ж, наразі дуже популярною є практика використання віддалених робочих місць, що створює потребу у керуванні віддаленими обліковими записами працівників та грамотному захисті їхніх пристроїв. Також нормально налагоджена IAM-система значно полегшує ведення бізнесу та підвищує ефективність роботи персоналу тим, що в залежності від наданих привілеїв кожний з облікових записів у системі, має доступ лише до потрібних конкретному працівникові ресурсів, що знижує час на пошук потрібних документів, форм, записів тощо. В свій час все це, дозволяє створити спеціальні профілі для потенційних та вже активних клієнтів компанії, які будуть містити неробочу інформацію, призначену для цих категорій користувачів. На додачу, розгортання IAM-систем полегшують взаємодію організації та урядів держав, бо по-перше згідно з законодавством багатьох країн захист даних є обов’язковою вимогою для компанії, а по-друге дозволяють швидко та зручно зберігати та надавати інформацію, на яку урядові установи можуть надати запит [4, 5].

Єдиного підходу до втілення IAM-систем для усіх ІТС не існує, методи та засоби обираються в залежності від особливостей конкретної системи, проте деякі спільні ознаки, складові та функції випливають з мети – отримання користувачами

легітимного доступу до ресурсів ІТС, при цьому ж таким чином, щоб це покращувало бізнесову складову роботи системи та щоб власне система IAM була ресурсоефективною [1]. Виходячи з цього, можна виділити наступні основні задачі IAM-систем [4]:

управління користувацькими профілями;

надання та позбавлення користувачів ролей;

автентифікація користувачів;

авторизація користувачів;

зручна система доступу;

генерація та надання звітів про діяльність користувачів ІТС.

Враховуючи, що IAM це широка концепція, у роботі з якою слід розуміти ряд понять, варто виділити основні та найчастіше згадувані з них:

ідентифікація – процедура розпізнавання користувача в системі, завдяки даним під якими система знає цього користувача;

автентифікація – процедура розпізнавання системою інформації, до якої має доступ даний користувач. Може бути парольною, біометричною, або вимагати особливого предмету або атрибуту;

багатофакторна автентифікація(MFA) – процес автентифікації, що вимагає двох та більше факторів, для допуску користувача;

авторизація – процес керування системою доступами користувача на основі ідентифікатора та автентифікатора;

сутність – в даному контексті, користувач або програма, що має пройти процес авторизації у системі;

рольова модель управління доступом, або Role-Based Access Control (RBAC) – модель доступу, що передбачає отримання доступу до ресурсів ІТС користувачем, згідно з ролями, що прописані у системі;

розподілення доступу засноване на атрибутах, або Attribute-Based Access Control (ABAC) – модель доступу, що передбачає надання доступу сутності засновуючись на наявності та конфігурації її атрибутів;

роль користувача – набір правил та особливостей, що закріплені за користувачем згідно з політик компанії;

Single sign-on (SSO) – технологія, що дозволяє користувачеві, що вже авторизувався в системі, отримати доступ до усіх ресурсів, втілених у ІТС, без потреби повторно проходити процеси автентифікації та авторизації [4].

Втілення адекватного IAM вимагає від власників бізнесу відкритості та прозорості, тобто IAM-система вимагає широкий ряд доступів в ІТС організації [5].

IAM CONTROL	DESCRIPTION
General requirements	Address access to systems and data, access privileges based on role and assignment of access privileges
Unique access IDs	Assign a unique ID to each user
Assignment of accounts	Mechanism to identify users and the resources they have access to
Access approvals	Define the process for authorizing access and the level(s) of access granted
Management of accounts	Addresses creation, modification and deletion of accounts and associated credentials
Access review and recertification	Processes for reviewing and updating user accounts based on role changes and other criteria
Inactive accounts	Criteria for deleting inactive accounts after a specific period of inactivity
Access revocation and disablement	Address changes in access privileges due to change in access needs, employee terminations or identification of compromised accounts
Privileged account management	Defines criteria for assigning privileged accounts and IDs
Remote access by administrators	Defines criteria for remote administrative access to systems and resources
Segregation of duties	Sets rules to ensure segregation of duties when assigning access privileges
Vendor access to resources	Defines criteria for assigning access to authorized vendors accessing system resources
Access authentication	Assigns criteria for granting permission to system resources through a series of authentication factors
User validation	Process to ensure user authentication is established before any transactions are performed
Password management	Addresses criteria for creating passwords
Authentication of mobile devices	Establishes access criteria for mobile devices
Access to voicemail	Defines criteria for access to voicemail accounts
User session management	Establishes criteria for termination of a session after a defined period of inactivity and criteria for multiple concurrent sessions by a user
Notification of system use	Criteria for displaying a visual message delineating access data prior to granting session access
Remote access	Establishes criteria for granting remote access to system resources
Data protection access	Governs access to data and resources that are considered mission-critical to the organization
Identification and validation of devices	Criteria for identifying all devices before connecting to system resources
Policies and procedures	Approved documents that specify how the organization ensures the confidentiality, integrity and availability of information

Рис. 1.1. Список необхідних доступів для IAM-систем [5]

Враховуючи вищесказане, можна сказати, що IAM-система – це, в більшості випадків, автоматизована система, яка надає можливість створювати, модифікувати та видаляти профілі користувачів, груп користувачів та ролі в ІТС, через спеціальні директорії, які можуть взаємодіяти між собою, в свій час всі ці сутності отримують свої привілеї та обмеження через політики втілені через RBAC. Більшість сучасних IAM-систем мають в собі потужні алгоритми авторизації з відповідними парольними політиками та засобами управління паролями, MFA, поведінковою та біометричною автентифікацією. Також дуже важливим є збір даних про події в ІТС пов'язані з діями користувачів(час проведений у системі; до яких ресурсів заходив користувач; тип автентифікації, що пройшов користувач для отримання доступу; кількість спроб увійти в систему тощо). [4]

Існує декілька способів розгорнути IAM-систему в IT-інфраструктурі організації. Це можна зробити силами спеціалістів даної організації, якщо вона їх має, тобто весь процес розробки та розгортання покладено на саму організацію, також можна скористатись численними продуктами, що надаються провайдерами на ринку. З технічної точки зору IAM-система може бути вбудованою в IT-інфраструктуру, представлена у вигляді окремого програмного, технісного чи програмно-технічного комплексу, або ж може бути надана через хмарні сервіси. Також дуже популярним рішенням, що випливає з вищесказаного, є розгортання гібридної моделі IAM-системи.

Підсумовуючи, можна сказати, що втілення нормального IAM для ІТС організації є доволі комплексним процесом, що передбачає паралельне використання різних підходів та технологій. Це в свою чергу, створює ряд проблем для фахівців з кібербезпеки, бо з'являється потреба в налагодженні нормального функціонування кожного окремого елемента та усього комплексу загалом.

1.2. Аналіз проблем пов’язаних з втіленням та роботою систем управління ідентифікацією та доступом користувачів

Враховуючи те, як стрімко розвивається галузь IT однією з основних проблем пов’язаною з IAM є те, що керівництво та спеціалісти багатьох компаній не встигають модернізувати системи згідно з реаліями сьогодення. Власники великих корпорацій часто переоцінюють свої системи захисту та не бажають витрачати велику кількість коштів на постійну актуалізацію кіберзахисту компанії. Керівництво компаній, що не є великими гравцями на ринку доволі часто вважають, що їхня компанія не стане ціллю кіберзлочинців. Обидва підходи є хибними, бо кіберзлочинці вишукують своїх жертв усюди та бажають витягнути з них усю критичну інформацію, до якої зможуть дістатись. Лише приклади нещодавніх атак показали, що більшість IT-інфраструктури потребують значного поліпшення та актуалізації, особливо в сфері IAM [6].

2019 рік вважається одним з найгірших років за кількістю кіберінцидентів, лише за першу половину року зловмисники змогли отримати дані з 4.1 мільярдів облікових записів, особливо цікавим в даній ситуації є факт, що дані з 3.2 мільярдів акаунтів було отримано лише в наслідку восьми зламів, зазначається, що в більшості випадків компанії-жертви мали схожі проблеми з безпекою, що пов’язані з неефективним управлінням доступом [7]. У 2013 році одна з найбільших торгівельних мереж США «Target» піддалась атаці, завдяки якій зловмисники отримали дані понад 110 мільйонів банківських карток клієнтів. Відомо, що хакери надіслали фішингові листи працівникам декількох компаній-вендорів, отримали доступ до облікових записів цих компаній та через них змогли отримати доступ в мережу «Target» [8]. Дуже показовим прикладом стала ситуація з компанією Deloitte в 2017 році. Дана компанія консультувала державні та фінансові установи США та ще ряд мультинаціональних компаній у сфері кібербезпеки, але обліковий запис одного з адміністраторів не мав навіть двофакторної авторизації, через що зловмисники отримали доступ до усієї мережі корпорації, просто зламавши пароль від акаунту [2].

З одного боку, стає очевидним, що сучасний підхід до IAM є критичним для побудови безпечної IT-інфраструктури компанії, але з іншого боку варто зазначити, що по-перше, задля цього доведеться повністю переосмислити підхід до захисту ITC, а по-друге, розгорнуті IAM-системи мають також функціонувати адекватно та виконувати свої функції. З цього випливає перша глобальна проблема людського фактору, яка створює ряд труднощів, від пов'язаних з небажанням витрачати час та ресурси на виконання такого великого обсягу роботи, до нехтування працівниками на всіх рівнях правилами безпеки, парольними політиками тощо.

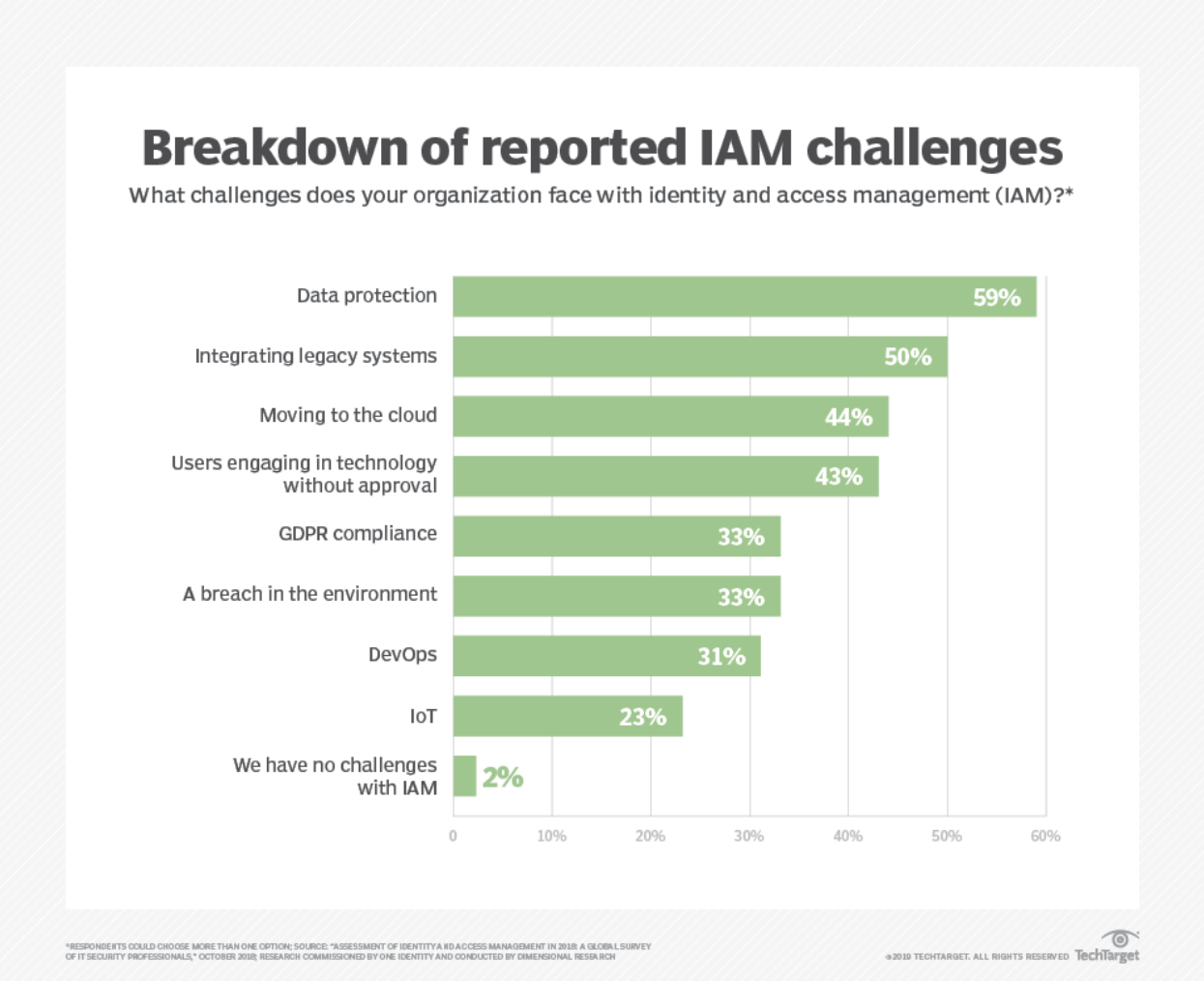

Рис. 1.2. Складності з якими стикаються компанії у сфері IAM [5]

Враховуючи, що обізнаність щодо важливості оновлення систем захисту серед власників бізнесу зростає, стає очевидним що власники бізнесу так чи інакше будуть імплементувати IAM-системи, а ті хто довгий час опирався будуть

вимушені, це зробити після кібератаки пов’язаної з відсутністю сучасних систем управління доступом, ідентифікації та авторизації. Але навіть після розгортання IAM-системи лишається доволі великий ряд проблем, ігнорування яких може призвести до катастрофічних наслідків.

Основою усіх проблем є велика складність оптимізації IAM-політик, що пов’язана зі зростом кількості користувачів онлайн-сервісів загалом, та конкретних ITC зокрема [6]. З цього випливають такі труднощі як, наприклад надмірні доступи та недостатній контроль доступу. Тобто через велику кількість користувачів та розширення штату працівників, може виникнути ситуація, коли з’являється працівник з посадою, якої раніше не було в компанії, але вона за своїм принципом схожа на вже існуючу. Працівникові надають роль згідно зі вже існуючою посадою, таким чином він наслідує привілеї яких за корпоративною логікою в нього не має бути [9]. Наприклад, компанія відкрила невелике відділення з власною локальною мережею, найняла людину на посаду системного адміністратора цієї мережі. В IAM-системі їй надали роль «Системний Адміністратор» і тепер ця особа має можливості до адміністрування усієї мережі компанії.

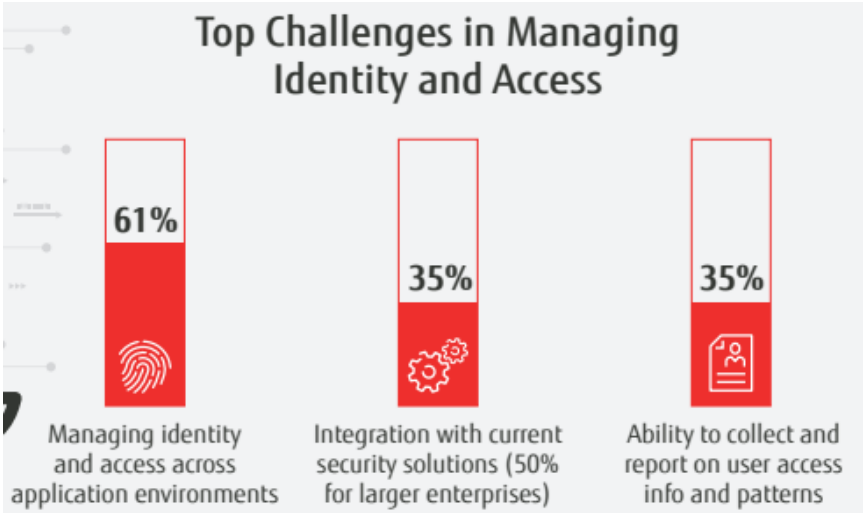

Рис. 1.3. Найбільші виклики в управлінні ідентифікованими профілями та доступами [10]

Враховуючи вищесказане, можна вивести загальний список проблем, що пов’язані з IAM:

проблеми пов’язані з даними ідентифікації та авторизації. Як згадувалось у даному підрозділі, основним джерелом складнощів у сфері парольних політик є людський фактор. На велику кількість сервісів, що потребують авторизації, припадає велика кількість паролів, кожен з яких має відповідати критеріям, встановлених цими сервісами. По-перше, запам’ятовування великої кількості різноманітних паролів доволі клопіткий процес для людини, тому значна кількість осіб надають перевагу створенню одного паролю, що підходить під критерії усіх сервісів, або можливе навіть пом’якшення парольних політик за вказівкою керівництва компанії. По-друге, особливого захисту вимагають сервери, що зберігають ідентифікаційні дані користувачів, бо їхнє викрадення через злам сервера може обернутися катастрофою для компанії, а якщо для авторизації використовувались біометричні дані, то зловмисники можуть отримати колосальні можливості у підробці особистостей. Також, в IAM-системі, що має сервіс SSO, завжди є ризик того, що зловмисник може отримати доступ до усієї системи, завдяки зламу основного робочого акаунту; [4,10]

складності у надані та позбавлені користувачів ролей та доступів. У випадку з додаванням нових користувачів, груп користувачів, ролей, доступів, документів, сервісів тощо, основною проблемою є те що даний процес потребує ручної роботи спеціалістів, що може призвести до помилок. З видаленням все дещо складніше, бо можливий сценарій де видалення певного суб’єкта з системи може викликати проблеми з доступом до ресурсів, що пов’язані з цим суб’єктом; [10]

відсутність прозорості користувацьких доступів до ресурсів та важко відслідковуванні директорії. У великих ІТС з численними сторонніми сервісами доволі важко систематизувати та ясно показати, хто має доступ до чого. Це може виликати низку організаційних, правових та навіть технічних проблем, як наприклад, засмічення системи великою кількістю даних з окремих директорій кожного сервісу; [10]

керування доступом користувачів, що використовують різні браузери та девайси. Великою складністю в IAM, що наразі стає дедалі актуальнішою, є факт існування численної кількості пристроїв та браузерів для кожного з яких IT-

спеціалістам потрібно налагодити свою систему авторизації так щоб не жертвувати захищеністю системи загалом. Це означає, що система має бути налаштована під обробку більшої кількості посилань та ідентифікаційних даних; [10]

складність у підтримці взаємодії сервісів та додатків. Враховуючи, що в сучасних ІТС більшості організацій використовується велика кількість сторонньої продукції, виникає нагальна потреба в постійній підтримці та оновлені системи. Велика кількість різноманітних сервісів, від різних вендорів, вимагає прискіпливо стежити за оновленнями кожного з них та відповідних оновлень і налаштувань в ІТС організації. Також велика кількість сервісів ускладнює підрахування загальних витрат, що може викликати деякі фінансові проблеми. [10]

Рис. 1.4. Найпопулярніші проблеми пов’язані з ідентифікацією [10]

Узагальнюючи можна сказати, що відсутність IAM-системи є такою ж проблемою, як і погано налаштована IAM-система. Саме тому потрібно пильно слідкувати за оновленнями продукції вендорів, що пропонують IAM-рішення, і не забувати ознайомлюватись зі стандартами та рекомендаціями у цій сфері.

1.3. Переваги та сутність роботи систем управління ідентифікацією та доступом користувачів в мережі організації

Виходячи з описаного у минулому підрозділі стає очевидним, що IAM-системи мають бути імплементовані за певними правилами, щоб приносити користь. З концептуальної точки зору, в першу чергу варто звірятись з існуючими міжнародними та державними стандартами, що диктують правила саме у сфері ідентифікації та доступу. Деякими з таких стандартів є: ISO/IEC 24760(1-3):2015-19 – A framework for identity management; ISO/IEC 29146:2016 – A framework for access management. Також, існує спеціальна публікація від NIST 800-63 – Digital Identity Guidelines, на чотири томи, в якій широко та детально дано опис того, як відбувається ідентифікація та автентифікація користувачів в урядових IT-системах через відкриті мережі. З організаційної точки зору можна також розглянути лінійку стандартів ISO 55000 (ISO 55000:2014 Asset management – Overview, principles and terminology; ISO 55001:2014 Asset management – Management Systems – Requirements; ISO 55002:2018 Guidelines for the application of ISO 55001; ISO/TS 55010: Guidance on alignment of asset management, finance and accounting; ISO 55011: Guidance on the development of government asset management policy), що дають змогу зрозуміти, як саме має бути побудоване керування усіма активами організації в цілому. Також існує доволі велика кількість сертифікацій, що дозволяють оцінити наскільки ITC організації відповідає сучасним вимогам у сфері IAM.

The top identity and access management (IAM) certifications

CERTIFICATION	FOCUS	COST
CISSP	General infosec certification; one of 8 domains focuses on IAM	$699
CompTIA Security+	General infosec certification; one of 6 domains focuses on IAM	$370
CISA	IT auditing-related certification	$575 for ISACA members $760 for nonmembers
CIPT	Privacy-related certification	$550
CAMS	Access management certification	$290
CIAM	IAM-specific certification	$390
CIGE	Identity governance certification	$395
CIMP	Identity management certification	$295
CIPA	Identity theft risk management certification	$295
CIST	IAM and security certification	$295
CRFS	Workplace identity theft prevention certification	$295

Рис. 1.5. Найкращі IAM-сертифікації, їхня мета та вартість[5]

В більшості випадків, великі компанії-вендори та IT-спеціалісти вже ознайомлені та працюють за вищезгаданими стандартами. Однією з основних рекомендацій для IAM є дотримання принципів zero-trust [4] (усі джерела даних і засоби обчислення вважаються ресурсами; усі комунікації захищені незалежно від розташування мережі; доступ до особистих робочих сервісів надається на односесійній основі; доступ до ресурсів визначається динамічною політикою, включаючи спостережуваний стан ідентифікації клієнта, сервісу та активу, що запитує, і може включати інші атрибути поведінки та середовища; ведеться моніторинг цілісності і захисту усіх належних і пов’язаних активів; автентифікація та авторизація є динамічною та суворо відслідковується до моменту надання доступу; уся можлива інформація про стан користувачів, активи, мережу та інфраструктуру зберігається та аналізується для подальшого використання [11]).

Також критично важливою складовою у втіленні IAM з технічної точки зору є використання ряду спеціальних стандартизованих мов та протоколів, таких як:

Lightweight Directory Access Protocol (LDAP). Протокол, що працює зі стеками TCP/IP, відфільтровуючи необхідну інформацію (ідентифікаційна інформація, інформація про користувачів та пристрої в мережі, сертифікати шифрування тощо). Завдяки даному протоколу можна проводити операції аутентифікації, пошуку та порівняння, а також операції додавання, зміни або видалення записів. Визначає структуру записів, що складається з набору атрибутів, які в свою чергу складаються з назви або опису, і кількох значень, в залежності від призначення атрибуту. [12, 13];

Security Assertion Markup Language (SAML). Відкритий стандарт, що базується на XML та дозволяє проводити обмін ідентифікаційними даними між користувацькими сутностями та сторонніми сервісами. Фактично, створює єдину базу даних для входу користувача, що дозволяє запровадити SSO [12, 13];

System for Cross-domain Identity Management (SCIM). Відкритий стандарт для хмарних технологій, що налагоджує взаємодію між додатками на принципах REST(створення, читання, редагування та видалення), що дозволяє отримати полегшений доступ до атрибутів користувачів, будови атрибутів, будови груп тощо. Це в свою чергу, дозволяє виділити користувача відповідального за керування сутностями та сервіс, що буде зберігати ідентифікаційні дані [12, 13];

OAuth 2.0. Даний протокол розроблено для паралельної роботи з HTTP, він дозволяє надавати токени доступу до певного сервісу стороннім користувачам через сервери автентифікації, з дозволу відповідної особи [12, 13];

OpenID Connect. Один з найновіших протоколів, в сутності своїй схожий з OAuth 2.0 та SAML, але на відміну від останнього використовує формат JSON для збору та зберігання даних [12].

Варто відзначити, що це далеко не повний список стандартів, що пов’язані з IAM, але це одні з найчастіше використовуваних з них.

Враховуючи усе вищесказане можна зробити висновок, що з нормальним підходом до IAM, організація буде:

Користуватись послугами центрів автентифікації, що не тільки дає змогу централізувати усі ідентифікаційні дані в захищеній системі, а й надає змогу

відслідковувати нетипові ідентифікаційні запити(підозрілі IP-адреси, геолокація тощо), що значно підвищує захист. Це також справедливо для директорій з даними користувачів і систем адміністрування та звітування, що також мають бути централізованими; [10, 14]

Використовувати MFA [14, 15];

Мати змогу втілити динамічну авторизацію, що дає змогу відслідковувати поведінку користувачів, та редагувати доступи в системі в реальному часі[14];

Активно використовувати та мати відповідний захист програмованих інтерфейсів додатків (API) [14];

Використовувати більш суворі вимоги до ідентифікаційних даних користувачів та сервісів, включаючи більш суворі парольні політики, використання тимчасових паролів, ротацію ключів тощо [12];

Мати систему, в якій працює принцип least-privilege permissions, тобто користувач або програма має доступ лише до тих ресурсів, що необхідні для виконання робочих задач[15];

Проводити постійний аудит системи, на предмет застарілих та непотрібних користувачів, ролей, політик тощо, оновлювати та видаляти їх[15];

Мати адекватно втілену систему SSO [4];

В якості моделей доступу використовуватиме RBAC, ABAC та їхні варіації;

Слідкувати за виконанням політик безпеки, постійно їх оновлювати та валідувати їх у системи [15];

Мати впевненість, що зі звільненням працівника, дані з якими він працював будуть доступні й надалі [10];

Мати можливість встановлювати права доступу для різних служб та отримувати звіти про відповідність прав доступу, надані можливості користувачам, а також про дії користувачів у системі [10];

Давати своїм користувачам можливість отримати доступ до системи з максимально можливої кількості девайсів та браузерів [10];

Мати систему, що є посередником усіх робочих сервісів та програм, що дає змогу інтегрувати їх між собою у системі та зручно оновлювати [10];

Мати систему, що підтримує ряд стандартів, протоколів та мов необхідних для обміну ідентифікаційними даними та даними користувачів (LDAP, SAML, XACML, OAuth, SCIM, UMA, NGAC, OIDC тощо) [4, 13];

Варто зазначити, що централізація зазначена в першому пункті стоєть виключно централізованого доступу відповідних адміністраторів до обмеженої взаємодії з ідентифікаційними даними. В плані зберігання ці дані мають бути розгалужені по багатьох сховищах, які відповідно захищені.

Компанії-вендори розуміють, як важливо для ведення бізнесу мати найновітніші розробки у сфері інформаційної безпеки, тому виставляють на ринок власні продукти, що зможуть задовольнити вищеописані критерії.

1.4. Аналіз існуючих систем управління ідентифікацією та доступом користувачів в мережі організації

Наразі на ринку існує достатньо велика кількість IAM-систем, що створює конкуренцію між вендорами, та змушує їх постійно актуалізувати свою продукцію та думати наперед. Основними вендорами є: Cisco, Okta, IBM, Ping, Microsoft і т.д. Для аналізу, порівняння та подальшого вибору продукту було обрано рішення від Okta, Ping та IBM.

Okta Workforce Identity забезпечує захист облікових записів для великих компаній, підтримуючи як хмарні, так і гібридні середовища. Функції Okta Workforce Identity надають безпечний доступ до робочих станцій, включають в себе SSO та MFA, а також покращують доступ до серверів та надають доступ до єдиної масштабованої директорії, що містить дані усіх користувачів, груп та пристроїв. Okta SSO інтегрується з понад 7000 сторонніх сервісів, все це з адаптивними політиками безпеки для аудиту поведінки користувачів. Okta надає адміністраторам інформаційну панель, де вони можуть керувати внутрішніми та зовнішніми користувачами та переглядати змістовні звіти. Okta також забезпечує керування життєвим циклом, яке дозволяє легко керувати користувацькими доступами, яке може бути автоматизованим, і мати розширені інтеграції зі

сторонніми сервісами, не поступаючись у захисті. В залежності від вмінь та навичок адміністраторів, Okta має опції для різного рівня кодингу. Сервіс Identity Engine дозволяє підлаштувати процеси авторизації, автентифікації та регістрації.[16, 17]

Intelligent Identity від Ping надає рішення безпеки, яке не шкодить зручності та простоті у використанні, забезпечуючи відслідковування ідентифікаційних даних. Включає різноманітні можливості для безпарольної автентифікації та авторизації в реальному часі та авторизації з урахуванням ризиків. Має вбудовані системи SSO та MFA. Дане рішення також включає штучний інтелект, який аналізує поведінку для виявлення аномалій і надає декілька методів автентифікації для контролю доступу. Intelligent Identity також маєє інтеграцію з кількома системами виявлення ризиків, загроз та нетипової поведінки, що поєднуються з політиками автентифікації та авторизації, системою моніторингу трафіку. Дане рішення діє як єдине «джерело правди», дозволяючи синхронізувати та збирати важливу інформацію з низки директорій, притому захищаючи її. Платформа пропонує низку варіантів для узгодження ідентифікації та керування доступом із їхніми ресурсами та потребами налаштування.[16, 17]

IBM Security Verify пропонує користувачам низку корисних функцій, включаючи SSO, що надає безпечний доступ до сервісів за допомогою єдиного набору облікових даних. Дане рішення надає високий рівень безпеки та підтримує можливість втілення адекватних політик безпеки, завдяки підтримці MFA, засобів виявлення ризиків та аналізу даних користувачів. Також в рішенні втілено динамічну автентифікацію на основі ризиків для оптимізації прав доступу користувачів. IBM Security Verify також захищає локальні програми, будучи хмарним рішенням та надає спеціальні звіти про події для аналізу системи. В рішенні втілено штучний інтелект, що виявляє небезпечні комбінації доступів у користувачів. Також особливу увагу IBM приділили захисту привілейованих користувачів та централізації управління доступами. [16, 17]

Аналізуючи дану продукцію, оптимальним варіантом для розгляду стало рішення від компанії IBM бо, по-перше, вони є однією з найбільш популярних та

надійних компаній на ринку, по-друге, особливості та функціонал їхнього продукту видається найбільш клієнтоорієнтованим. На магічному квадраті Gartner за 2022 рік, IBM єдині, хто вказані як Visionaries, тобто ті хто аналізують те як будуть змінюватись тенденції в розрізі IAM.

Рис. 1.6. Магічний квадрат Gartner за 2022 рік [18]

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ РІШЕННЯ IBM SECURITY VERIFY

2.1. Призначення та можливості IBM Security Verify

Основною метою IBM Security Verify є створення системи, що може об’єднати репозиторії ідентифікаційних даних та систематизувати політики, задля того щоб клієнти IBM могли підлаштовуватись під вимоги сучасності, які означають більш стрімкий перехід до хмарних технологій та покращення підходу до IT в цілому. Даний продукт надає інтерфейс для підвищення продуктивності працівників та створення відповідного захисту віддалених робочих місць.

IBM Security Verify надається у вигляді SaaS-платформи, що оснащена системою штучного інтелекту, яка відкриває можливості до впровадження адаптивного доступу до системи та може взаємодіяти з іншими IAM-рішеннями. Має широкий функціонал, від стандартних для IAM-систем SSO та MFA, управлінням конфіденційністю до виявлення ризиків, централізації управління та аналізу сутностей системи. Функціонал Security Verify розповсюджується як на хмарні додатки, так і на вшиті в ITC. Продукт постійно оновлюється, до нього додаються нові підсистеми, що стають доступними для клієнтів компанії миттєво. Дуже важливо, що оновлення ніяк не вплинуть та не зіпсують вже налагоджену систему клієнтів компанії, усі нововведені функції відповідні фахівці компанії-клієнта можуть за необхідності підключити самостійно. Взагалі, функціонал IBM Security Verify дуже комплексний та різносторонній, тому вимагає більш детального розгляду. [19]

Рис. 2.1. Особливості IBM Security Verify [19]

IBM Security Verify дозволяє налагодити централізоване управління користувачами, їхніми атрибутами, взаємодією, додатками тощо, завдяки зручному інтерфейсу, яким можна керувати через консоль адміністратора, або через REST API інтерфейси. Security Verify підтримує роботу з SCIM 2.0, що дозволяє брати правила доступу та інші атрибути ролей з HR-систем та розподіляти їх між сервісами та кінцевими точками ITC організації. Тобто продукт надає дуже зручну функцію об'єднання та інтеграції директорій різних сервісів, що можуть бути в ITC, що значно полегшує роботу для адміністраторів та пришвидшує роботу системи. [19]

IBM Security Verify має велику кількість вбудованих модулів для взаємодії додатків, що дозволяє налагодити процедури SSO. Рішення побудовано на відкритих стандартах, таких як OpenID Connect та SAML 2.0, що дозволяє даному рішенню працювати як брокеру автентифікації, що підключає усіх користувачів незалежно від того, де вони перебувають, до усіх сервісів незалежного від того, які методи SSO ці сервіси використовують. [19]

IBM Security Verify оснащено передовими засобами для втілення у ITC найсучасніших та захищених методів автентифікації, як наприклад, FIDO2 WebAuthn, що дозволяє використовувати програми розпізнавання обличчя та відбитків пальців(Windows Hello, TouchID). Також, завдяки використанню

стандарту OAuth є можливість пройти автентифікацію через QR-код. Даний продукт надає можливості до втілення низки способів MFA: питання на знання; одноразові паролі через СМС, телефонний дзвінок та електронні листи(OTP); обмежені в часі одноразові паролі(TOTP); збір біометричних даних; спливаючі вікна, що вимагають певної дії. Рішення від IBM дозволяє налагодити реалізацію дуже детальних політик доступу, що базуються на мережі з якої користувач намагається отримати доступ, його геолокації, атрибутів тощо. Також завдяки напрацюванням іншого продукту IBM Security's Trusteer, з'являється можливість підключити додаткові системи, що дають змогу впровадити адаптивний доступ та автентифіковувати користувачів, залежно від рівня ризику, що вираховується з зібраних даних з девайсу, особливостей підключення та мережі, геолокації та аномалій у поведінці. [19]

Ще однією можливістю Security Verify є налагодження керуванням життєвого циклу користувача, що дозволяє не лише зручно створювати користувачів, редагувати їхні атрибути та доступи та грамотно їх видаляти без порушення доступів до пов'язаних з ними ресурсів, а й налагодити систему, в якій керування доступами напряму зв'язано з керуванням бізнес-процесами та може чітко відслідковуватись та контролюватись. Цього можна досягти як завдяки повній сумісності з відповідними службами Google, Microsoft365(Azure), Box, Salesforce, ZenDesk і т.ін., так і завдяки власним опціям підключення, що базуються на SCIM2.0. [19]

Security Verify дозволяє підключити сторонні продукти для перевірки загального стану IAM-середовища та перевірки наявності ризиків ідентифікаційної інформації користувачів, їхніх життєвих циклів, дозволів і програм. Дана особливість дозволяє розглядати більш детально дані окремих користувачів і додатків, щоб отримати докладнішу інформацію про порушення та оцінки ризику. Зібрані дані програма використовує для виявлення аномалій та надання рекомендацій щодо їхньої ліквідації. [19]

Завдяки Security Verify авторизовані у системі користувачі організації-клієнта IBM можуть бути впевнені, що їхні дані захищено, а завдяки великій

кількості налаштувань, які мають IT-спеціалісти організації, досвід користування ITC буде легким, прозорим та зрозумілим. Відповідний персонал організації може легко створювати форми реєстрації, завдяки інтуїтивно зрозумілому інтерфейсу, системи SSO дозволять користувачеві ввійти в систему використовуючи ідентифікаційні дані соцмереж, можливість налаштовувати IT-оточення організації дозволяє підключати підходящі джерела ідентичності, а аналітика діяльності в мережі дозволить побачити, як саме користувачі та клієнти взаємодіють з сервісами. Дуже важливою з клієнтської точки зору є можливість самостійно модифікувати свої профілі, контролювати дозволи та угоди на використання персональної інформації, підключати та відключати методи автентифікації тощо. [19]

2.2. Архітектура та компоненти IBM Security Verify

Зареєструвавшись на відповідному ресурсі IBM було отримано доступ до пробної версії IBM Security Verify, що дозволяє ознайомитись з інтерфейсом програми. Перше, що можна побачити при вході до програми це інформаційна панель, що має основну інформацію про діяльність у системі: кількість нових користувачів, невдалих спроб входу, з’єднань SSO, підключених додатків, загальних подій автентифікації, основні додатки та користувачі. Події автентифікації можна відображати у вигляді графіку або мапи, обираючи період(останні 24 години, 7 та 30 діб), тип входу(вдалі, невдалі, всі) та масштаб(глобальний, або за країною). Зліва можна побачити меню, де відкривається доступ до іншого функціоналу.

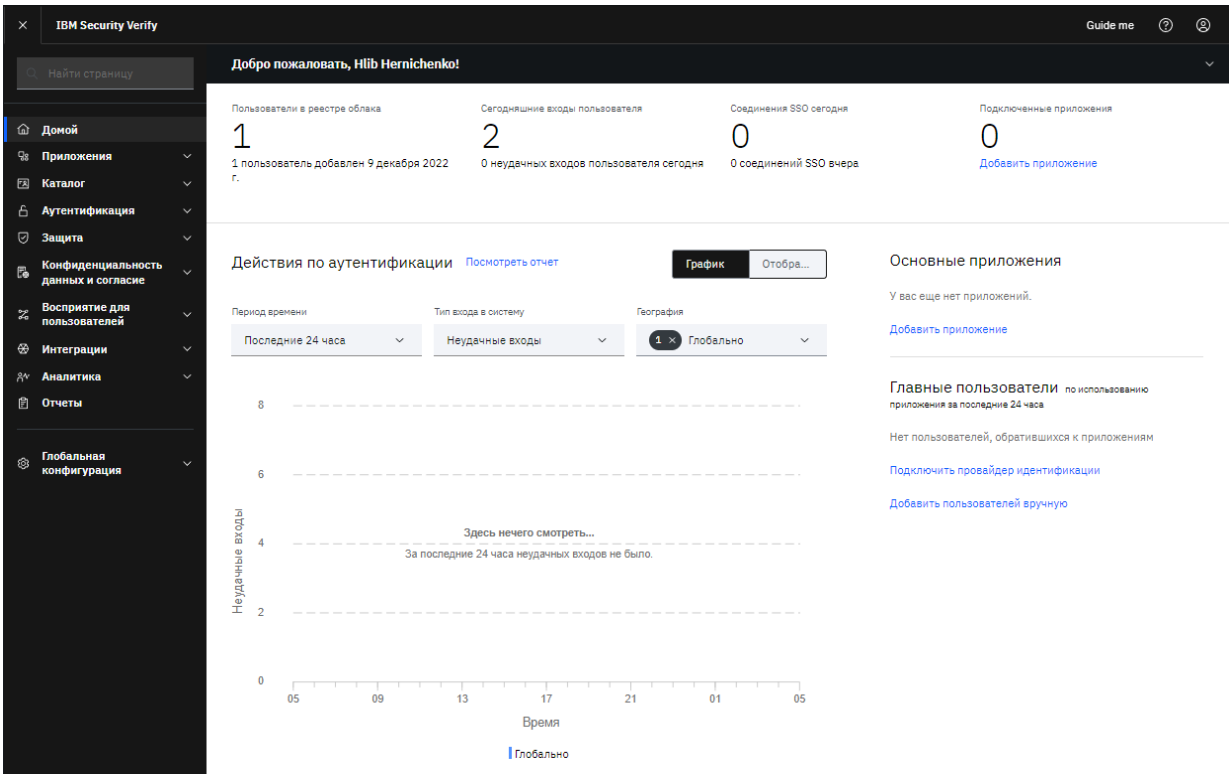

Рис. 2.2. Домашня сторінка IBM Security Verify

Наступною вкладкою після «Додому» йде «Додатки», розкривши її можна побачити наступні підрозділи:

«Додатки» містить каталог з усіма додатками системи;

«Налаштування додатків» надає можливості до конфігурації додатків також надає можливість для загального налаштування OpenID Connect, SAML та динамічної реєстрації клієнта;

«Керування ролями додатків» дозволяє налаштовувати роль додатків та продивлятись надані цими додатками дозволи;

«Профілі додатків» дозволяє створювати та керувати шаблонними профілями;

«Надання результатів» показує операції, що проводяться з додатками, ким вони проводяться та статус операції;

«Сертифікація прав доступу» дозволяє створювати кампанії для координації перевірки доступу.

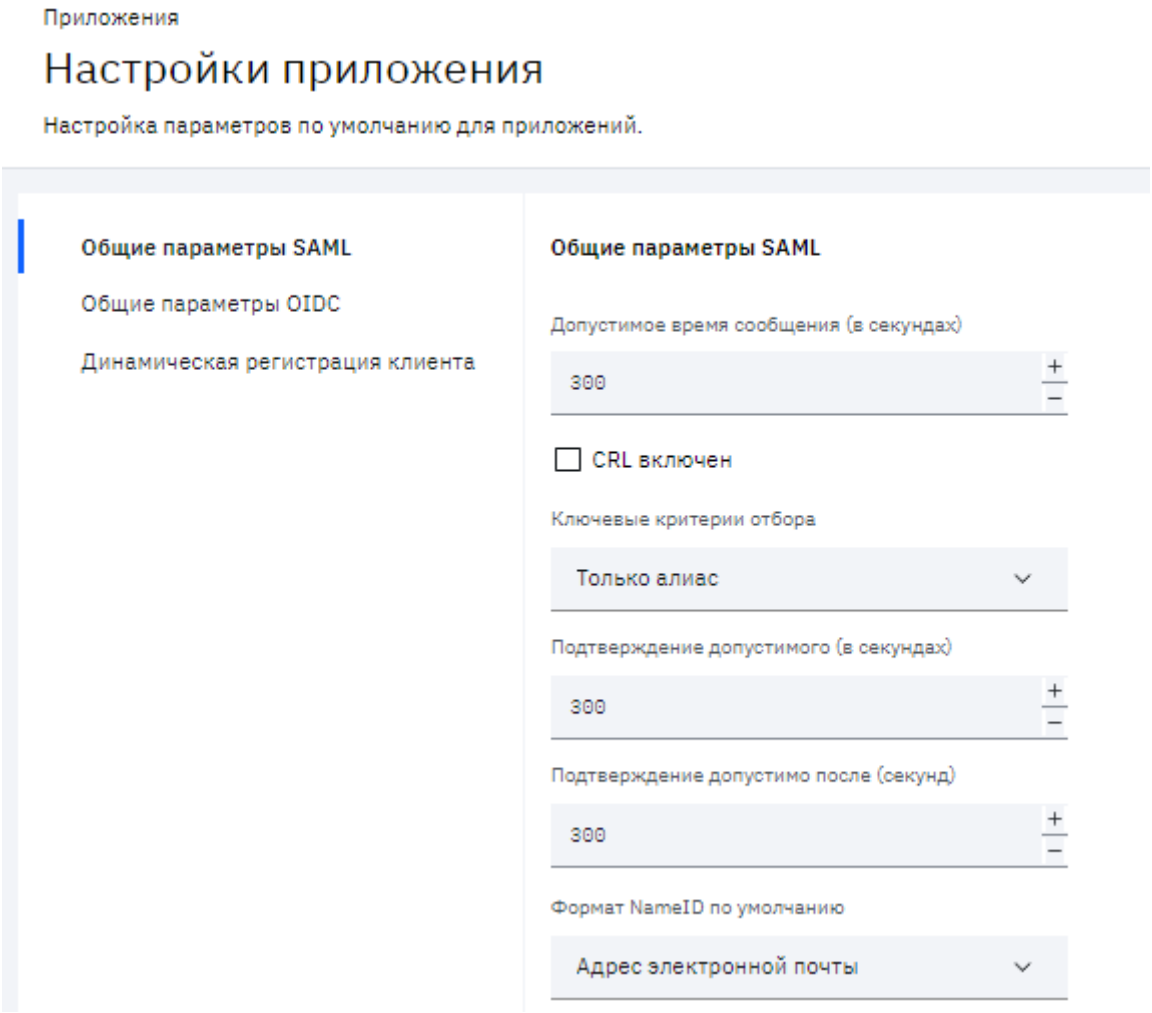

Рис. 2.3. Вигляд меню налаштувань параметрів SAML для додатків

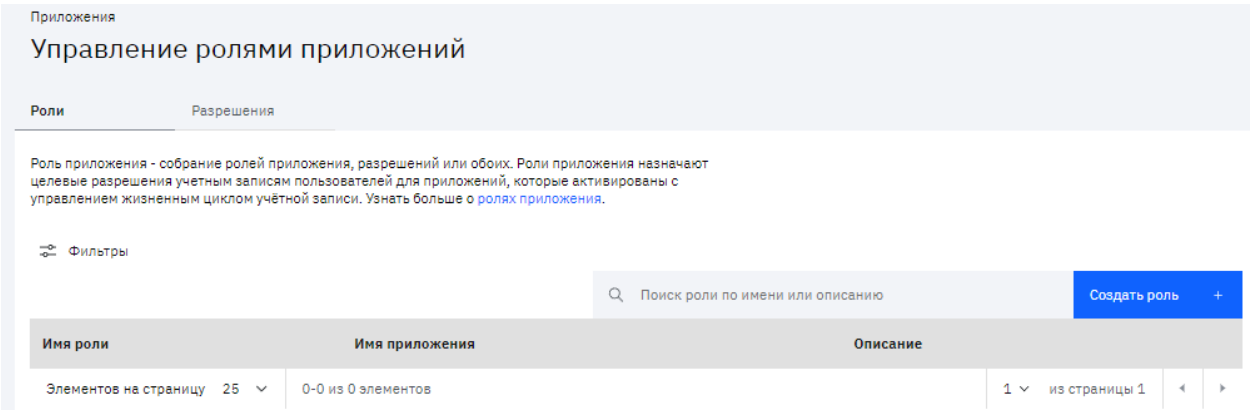

Рис. 2.4. Вигляд поля керування ролями

Наступною йде вкладка «Каталог», розкривши яку можна побачити пвкладки «Користувачі та групи» та «Атрибути», що власне і відповідають за створення, видалення та налаштування користувачів, груп і атрибутів.

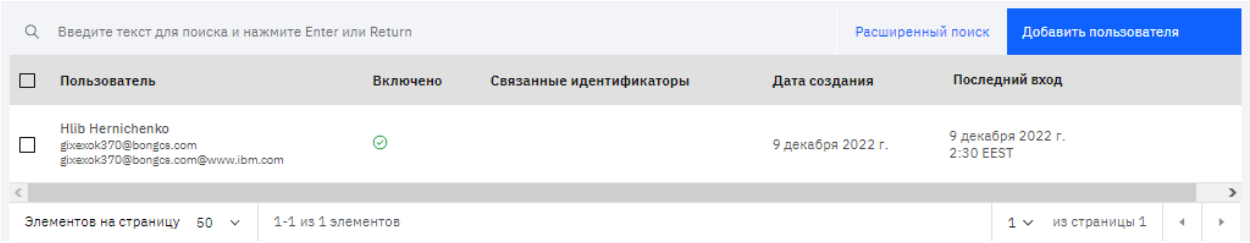

Рис. 2.5. Інтерфейс перегляду користувачів

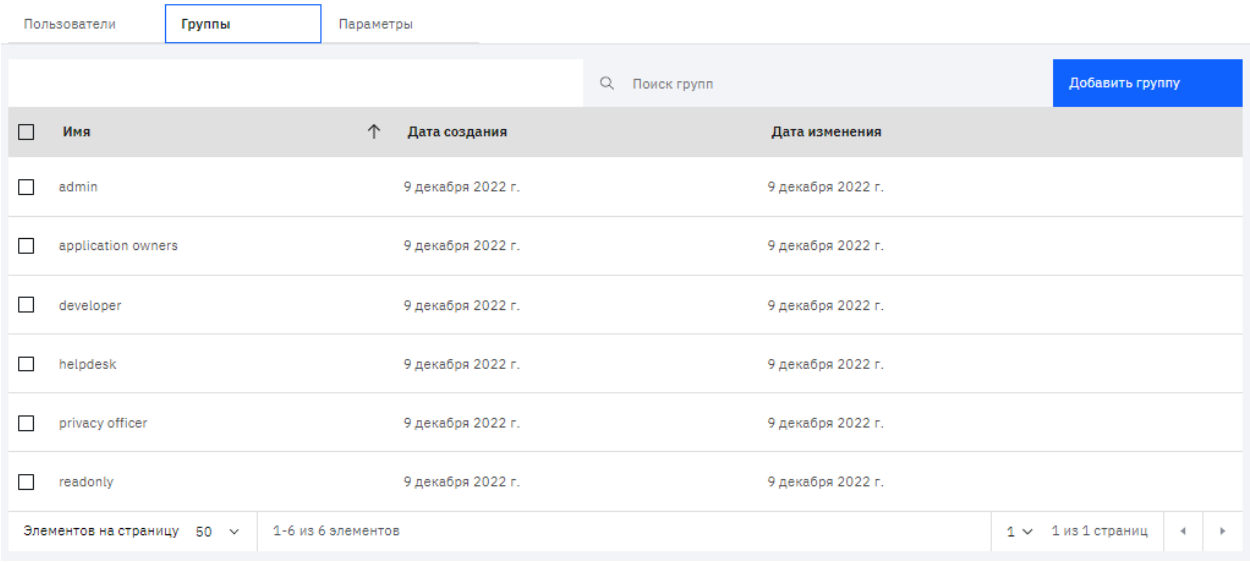

Рис. 2.6. Інтерфейс перегляду груп

Поиск имени атрибута | Добавить атрибут +

Имя	Источник	Описание	Доступно для
department Встроенный атрибут	*department*	Отдел, к которому относится пользователь.	Единая регистрация (Single sign-on, SSO), Предоставление
display_name Встроенный атрибут	*displayName*	Имя пользователя, подходящее для того, чтобы показывать его.	Единая регистрация (Single sign-on, SSO)
email Встроенный атрибут	*email*	Рабочая электронная почта пользователя.	Единая регистрация (Single sign-on, SSO), Предоставление
email_verified Встроенный атрибут	*urn:ietf:params:scim:schemas:extension:ibm:2.0:User:emailVerified*	Поле, указывающее отметку времени, когда была проверена электронная почта пользователя.	–
employee_id Встроенный атрибут	*employee_id*	ID сотрудника пользователя.	Единая регистрация (Single sign-on, SSO), Предоставление
enabled Встроенный атрибут	*enabled*	Логическое значение, указывающее на административное состояние пользователя.	–
external_id Встроенный атрибут	*externalId*	Уникальный идентификатор для пользователя, заданный клиентом предоставления доступа.	–
family_name Встроенный атрибут	*family_name*	Фамилия пользователя.	Единая регистрация (Single sign-on, SSO), Предоставление
fax_number Встроенный атрибут	*fax_number*	Номер факса пользователя.	–

Рис. 2.7. Інтерфейс перегляду атрибутів

Вкладка «Автентифікація» надає можливості конфігурувати провайдерів автентифікації, створювати та керувати менеджерами приладів, назначати поставників сертифікатів, керувати параметрами MFA в цілому та факторами автентифікації, керувати профілями реєстрації та параметрами FIDO2.

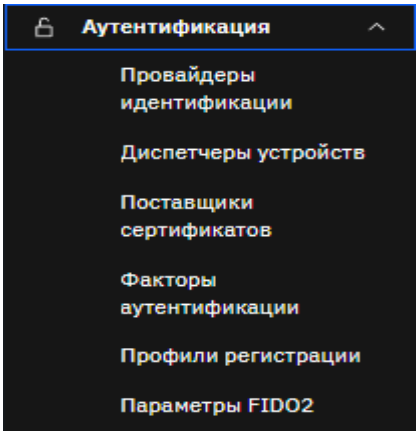

Рис. 2.8. Розгорнута вкладка «Автентифікація»

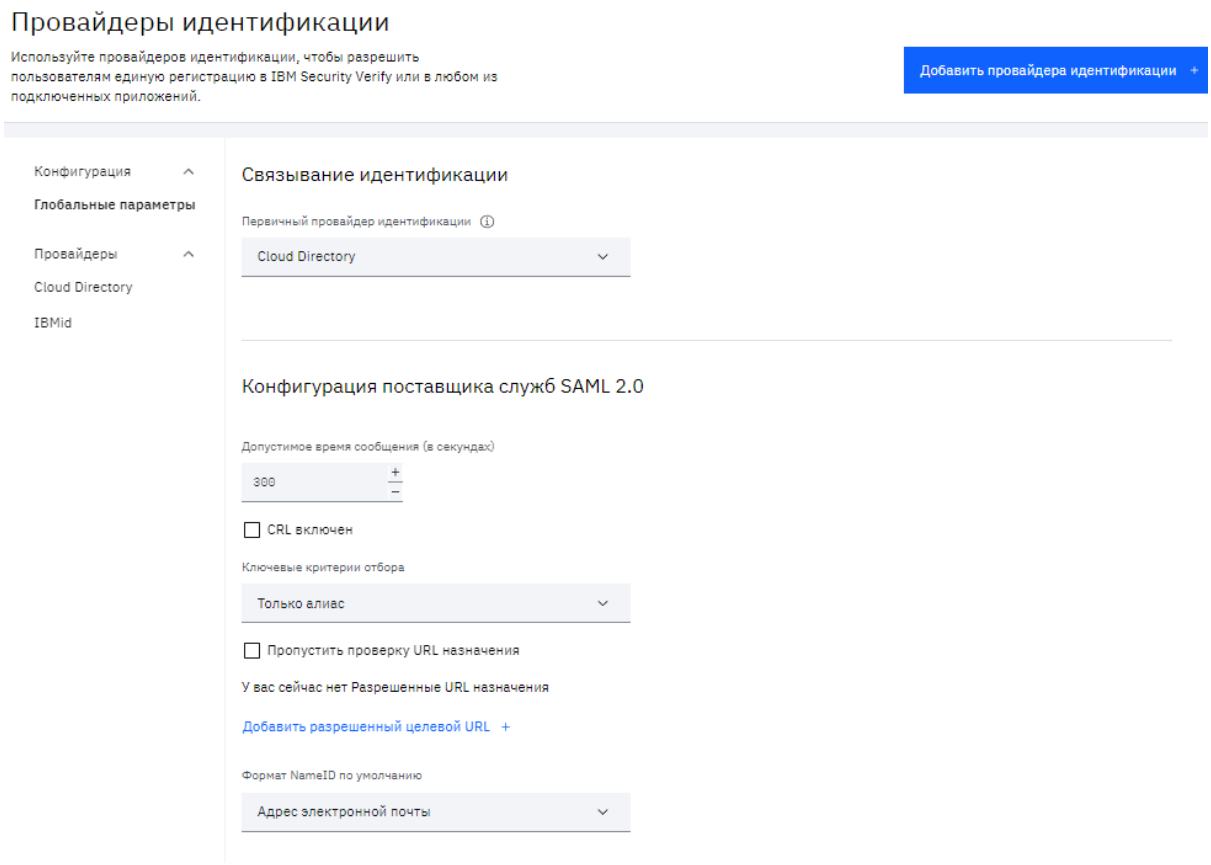

Рис. 2.9. Сторінка керування провайдерами автентифікації

Вкладка «Захист» надає доступ до редактора політик, центром керування доступу до порталу Security Verify, панелі керування токенами OpenID Connect, панелей конфігурації клієнтами API, сертифікатів, дозволів на використання даних, парольних політик, опціями входу.

Добавить политику +

Имя политики	Состояние	Применено к	Тип политики	Последнее изменение
Allow access from all devices	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Allow access from managed devices; others require 2FA	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Allow access from managed devices; others require 2FA each session	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Allow access from compliant devices only; block otherwise	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Allow access from desktops and compliant mobile devices; block otherwise	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Allow access from desktops and managed mobile devices; block otherwise	Активный	–	ООбъединеннная регистрация	22 ноября 2017 г., 18:41:16
Always require 2FA in compliant devices; block otherwise	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37
Require 2FA each session in compliant devices; block otherwise	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37
Allow access from desktops; always require 2FA in compliant mobile devices; block otherwise	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37
Allow access from desktops; require 2FA each session in compliant mobile devices; block otherwise	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37
Allow access from compliant devices only; others require 2FA	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37
Allow access from compliant devices only; others require 2FA each session	Активный	–	ООбъединеннная регистрация	20 апреля 2018 г., 08:10:37

Рис. 2.10. Панель управління політиками доступу

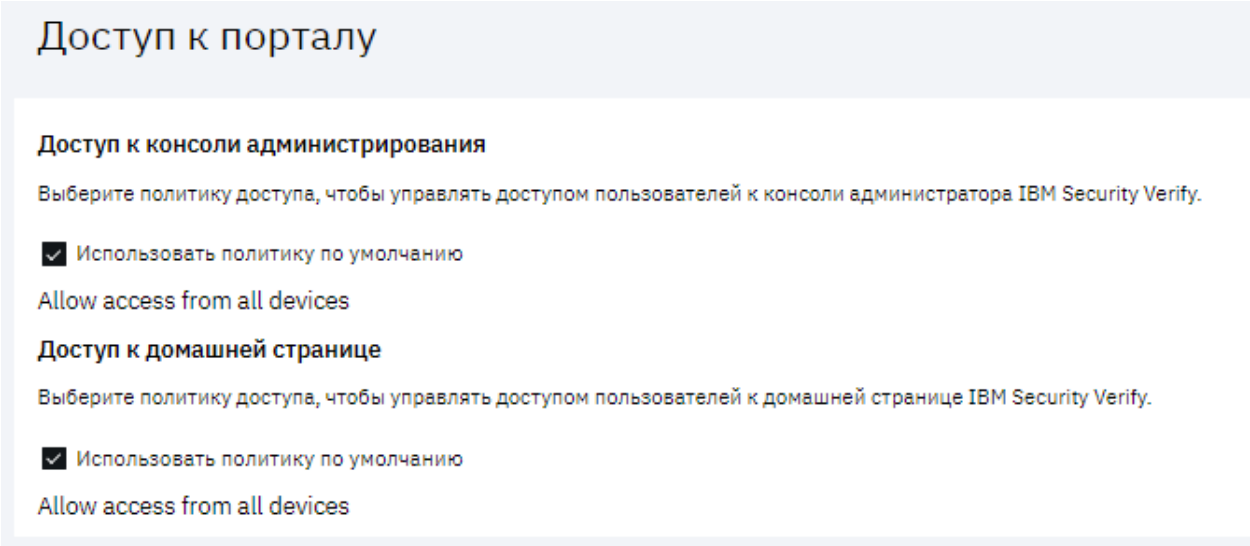

Рис. 2.11. Центр керування доступу до порталу Security Verify

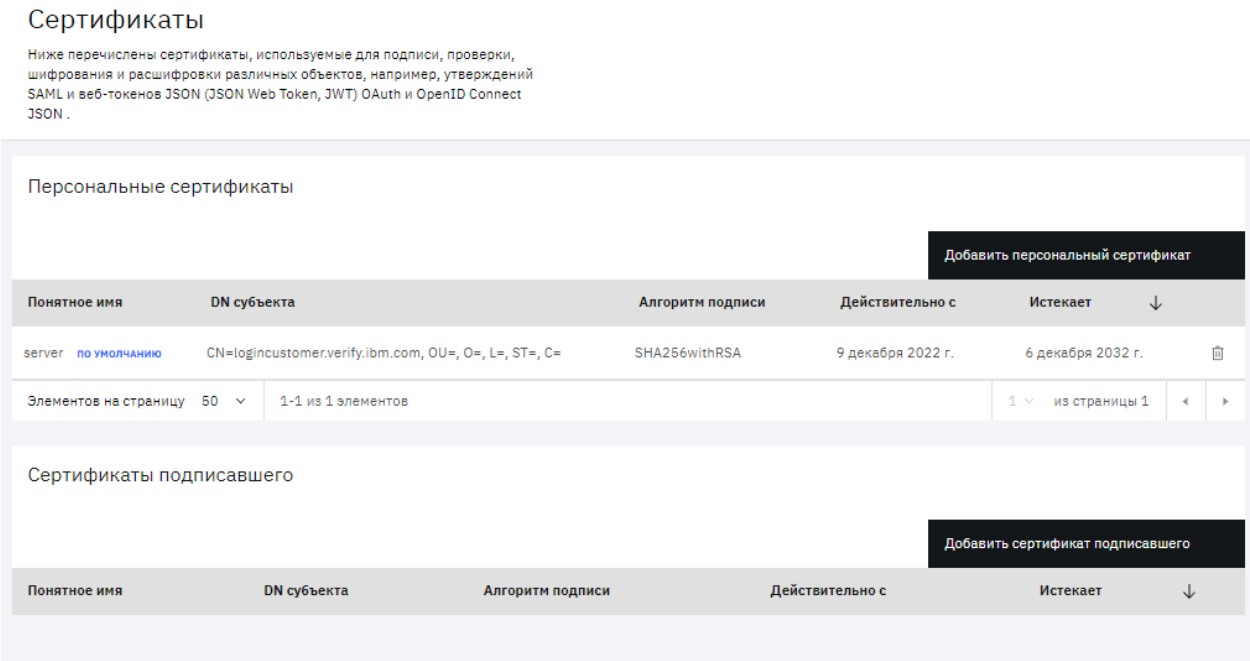

Рис. 2.12. Панель конфігурації сертифікатів

Вкладка «Конфіденційність даних та дозволи» надає функціонал для налаштування призначення даних користувачів, підв’язки користувацьких угод, налаштування профілів та політик конфіденційності та керування користувацьких дозволів.

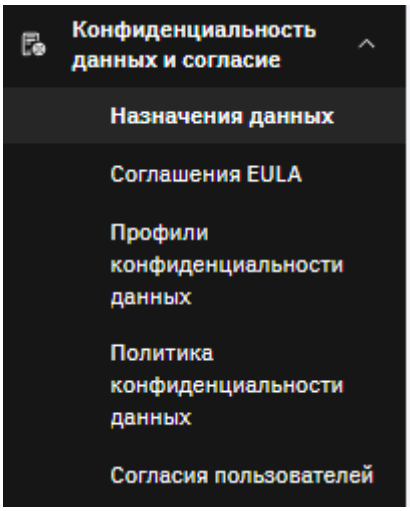

Рис. 2.13. Вкладка «Конфіденційність даних та дозволи»

Наступна вкладка «Сприйняття для користувачів» дає можливість налаштовувати зовнішній вигляд інтерфейсу порталу для користувачів,

створювати уніфіковані на порталі профілі користувачів та налаштовувати шаблони реєстрації.

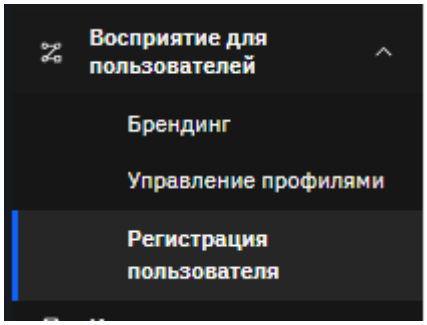

Рис. 2.14. Вкладка «Сприйняття для користувачів»

Вкладки «Інтеграція» та «Аналітика» дозволяють підключити зовнішні сервіси для реагування на інциденти та аналітики загроз та ризиків, провайдерів ідентифікації, служби ReCAPTCHA і керувати ними.

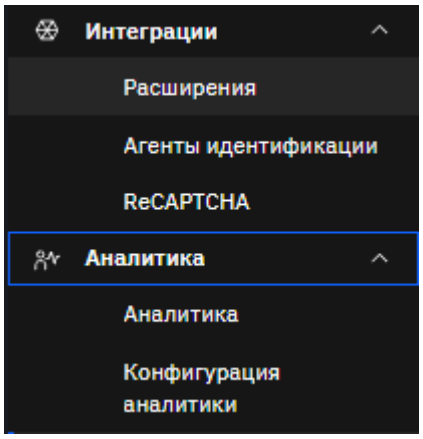

Рис. 2.15. Вкладки «Інтеграція» та «Аналітика»

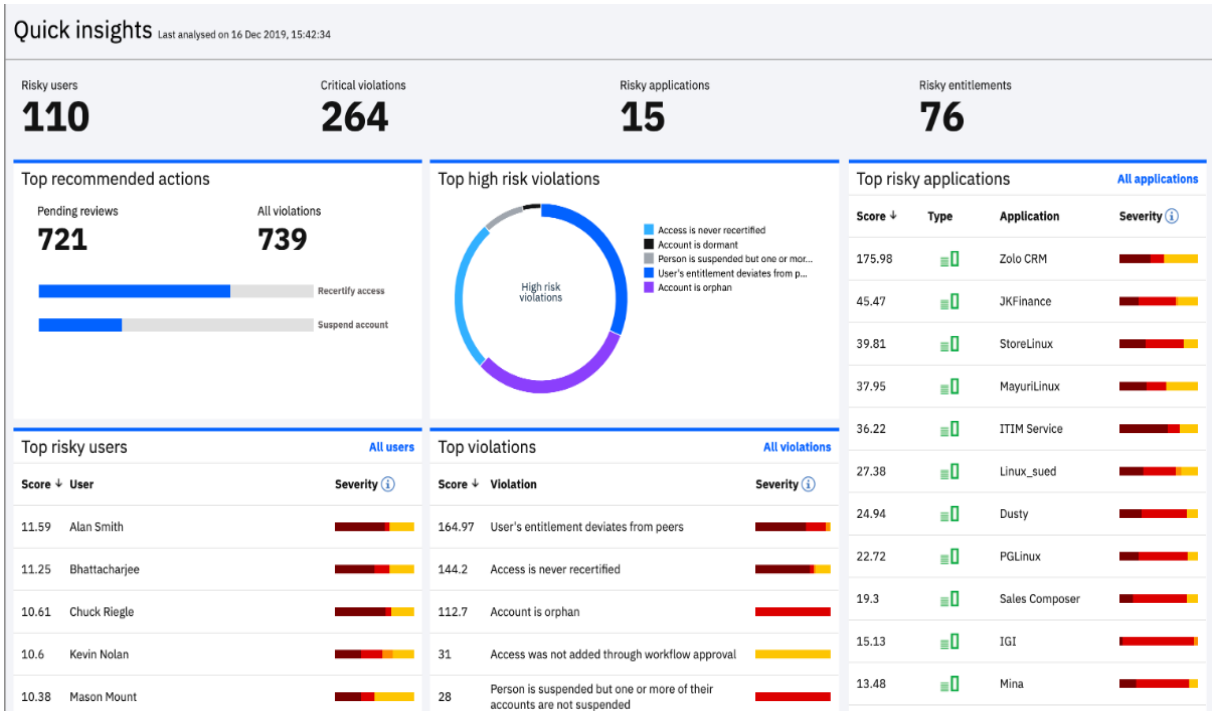

Рис. 2.16. Панель перегляду ризиків та порушень [19]

Вкладка «Звіти» дозволяє продивлятись звіти з подій автентифікації, користування додатками, операцій адміністратора, подій MFA тощо.

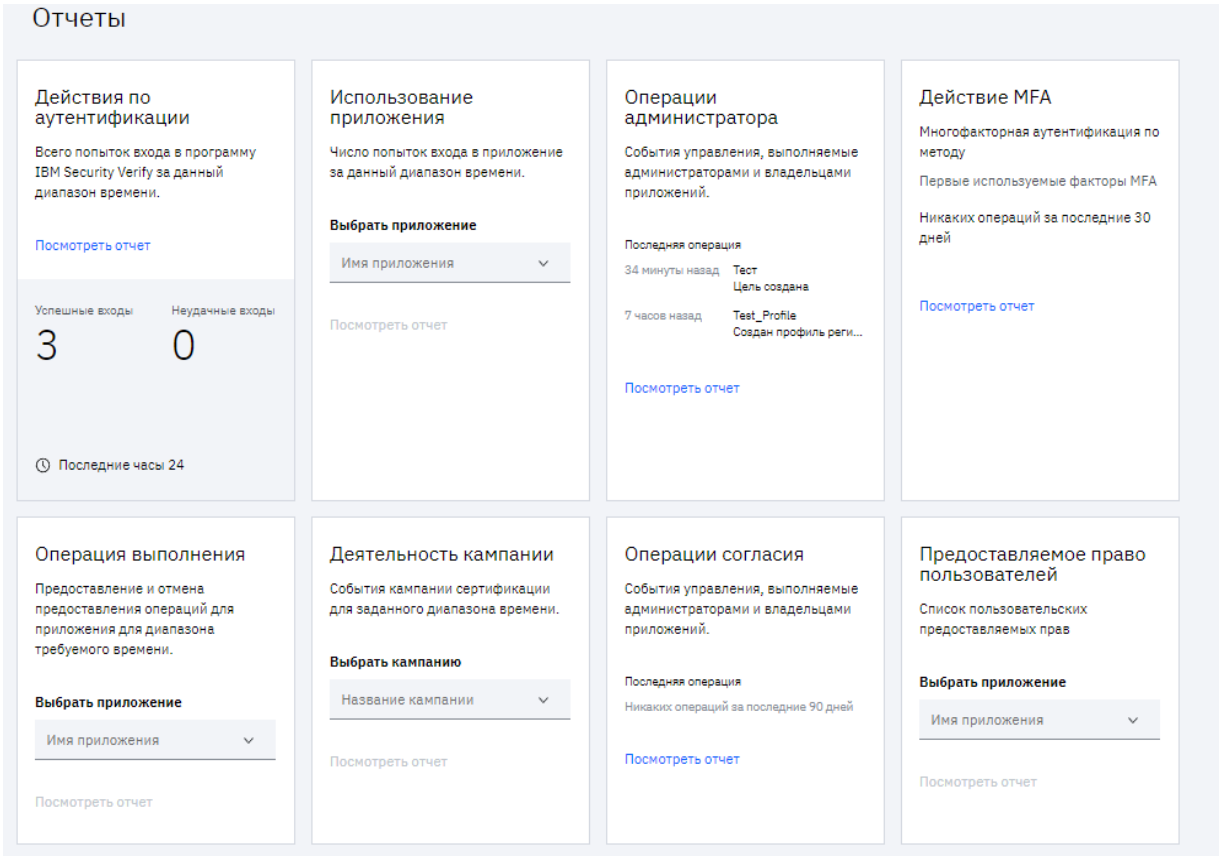

Рис. 2.17. Пропоновані звіти

Далі йдуть елементи інтерфейсу, що дають змогу налаштувати продукт для потреб адміністратора. Вкладка «Глобальна конфігурація» дозволяє налаштовувати ролі адміністратора, оформити елементи зовнішнього вигляду програми(кольори банера, назва продукту на панелі запуску, колонтитул, логотип), продивитись дані про підписку та користування.

На верхній панелі є вкладки «Guide me» та «?», що допоможуть адміністраторові знайти відповідь на свої запитання, отримати зворотній зв'язок та містять корисні посилання. Натиснувши на значок користувача можна продивитись профіль даного адміністратора, переключитись на панель запуску порталу, або ж вийти з системи.

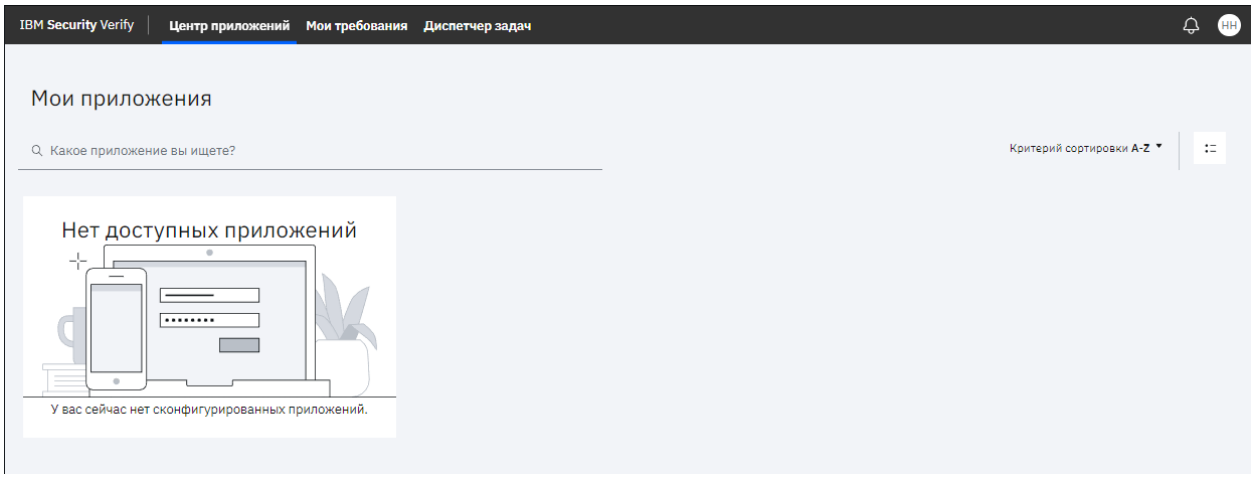

Рис. 2.18. Інтерфейс порталу

2.3. Огляд базового функціоналу IBM Security Verify

Використовуючи описані вище елементи інтерфейсу можна починати огляд основних можливостей даного рішення. Варто відмітити, що за відсутності доступу до корпоративної ІТС організації, представлений далі матеріал є сугубо демонстративним та зробленим в якості зразку, деякі з елементів роботи було взято з документації, що надана компанією IBM.

Першочерговим є додавання користувача у систему, в панелі створення можна обрати провайдера ідентифікації, надати користувачу атрибути, основні з яких: ім’я, прізвище, системне ім’я та електронна пошта.

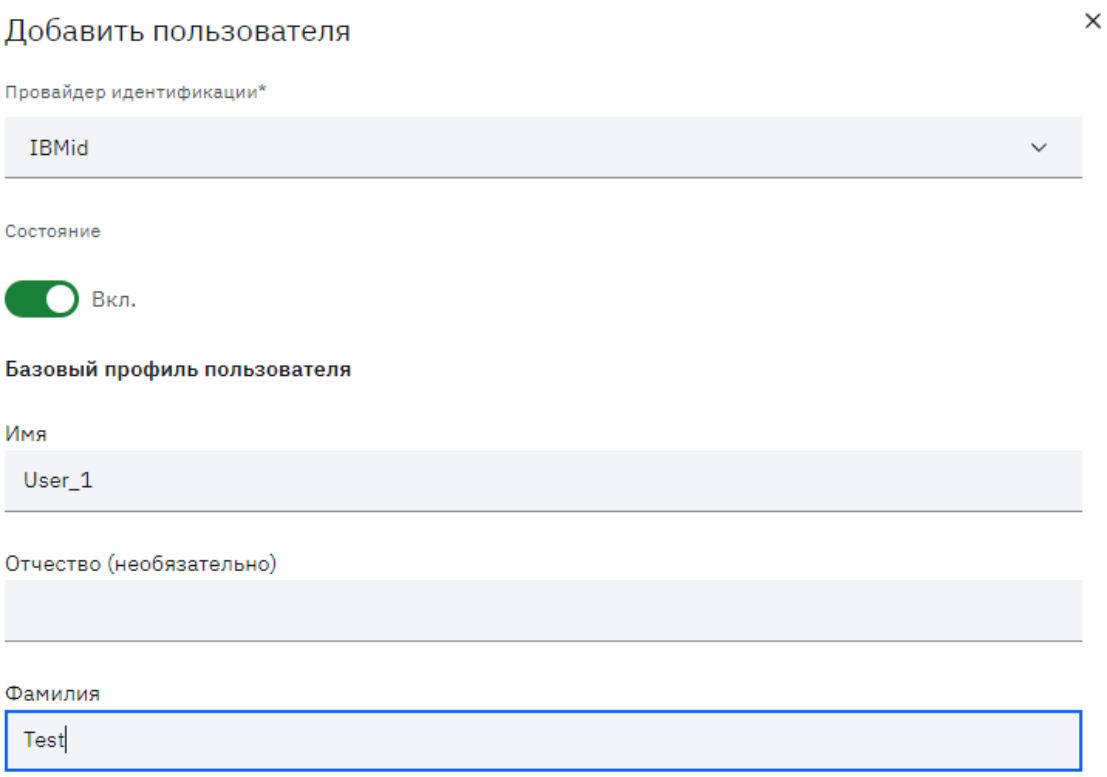

Рис. 2.19. Початок створення користувача

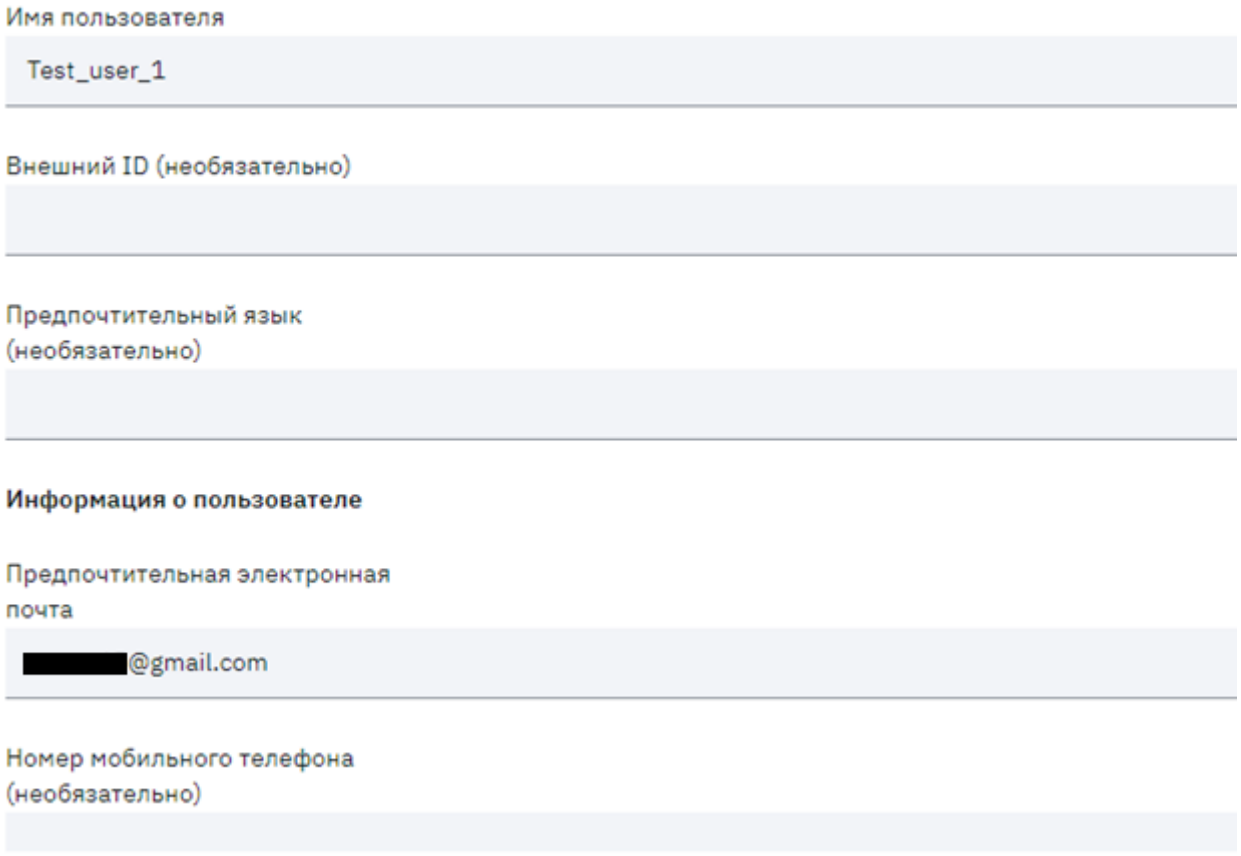

Рис. 2.20. Продовження налаштування користувача

По завершенню процесу створення обліковий запис з’явиться на відповідній панелі, що надає доступ до подальшої конфігурації.

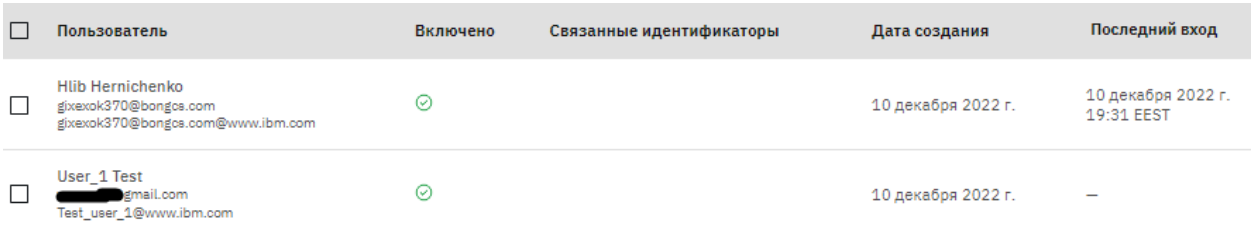

Рис. 2.21. Вигляд користувача на відповідній панелі

Панель з параметрами користувача дозволяє повністю переглянути усі атрибути та прилади користувача, налагодити MFA та провести ряд дій.

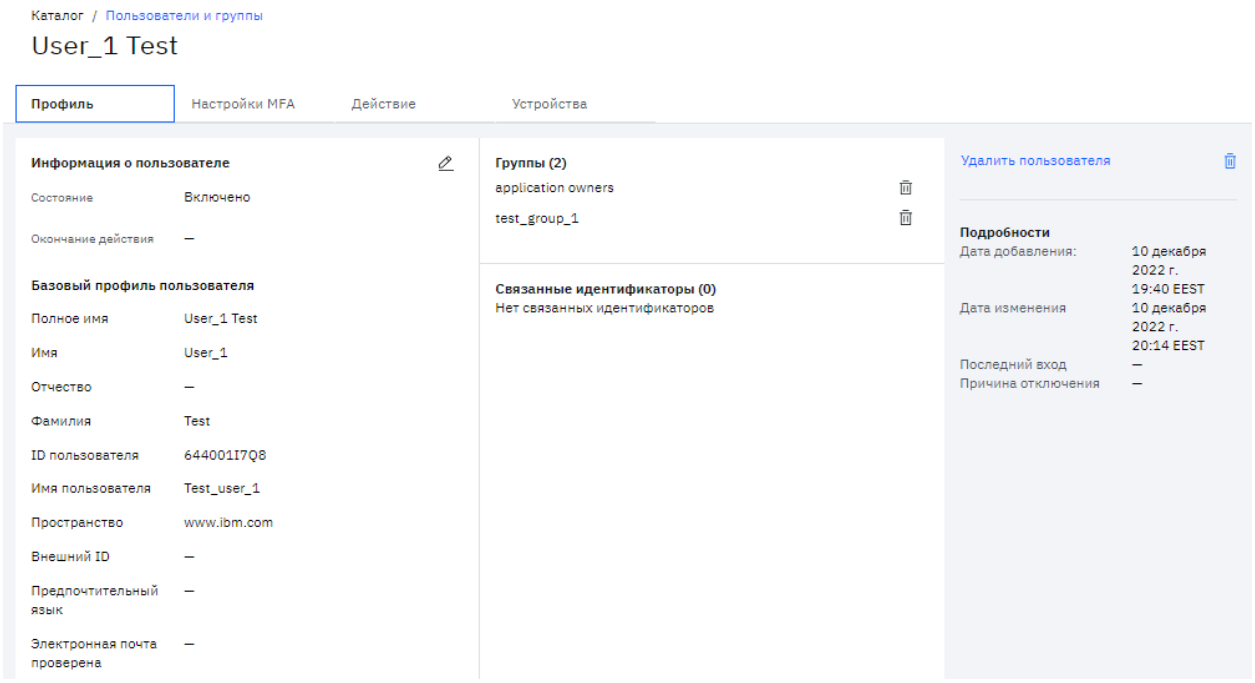

Рис. 2.22. Параметри користувача

Створених користувачів можна об’єднувати в групи, за допомогою спеціального меню. В подальшому, створені групи дозволять приміняти новостворені правила на них.

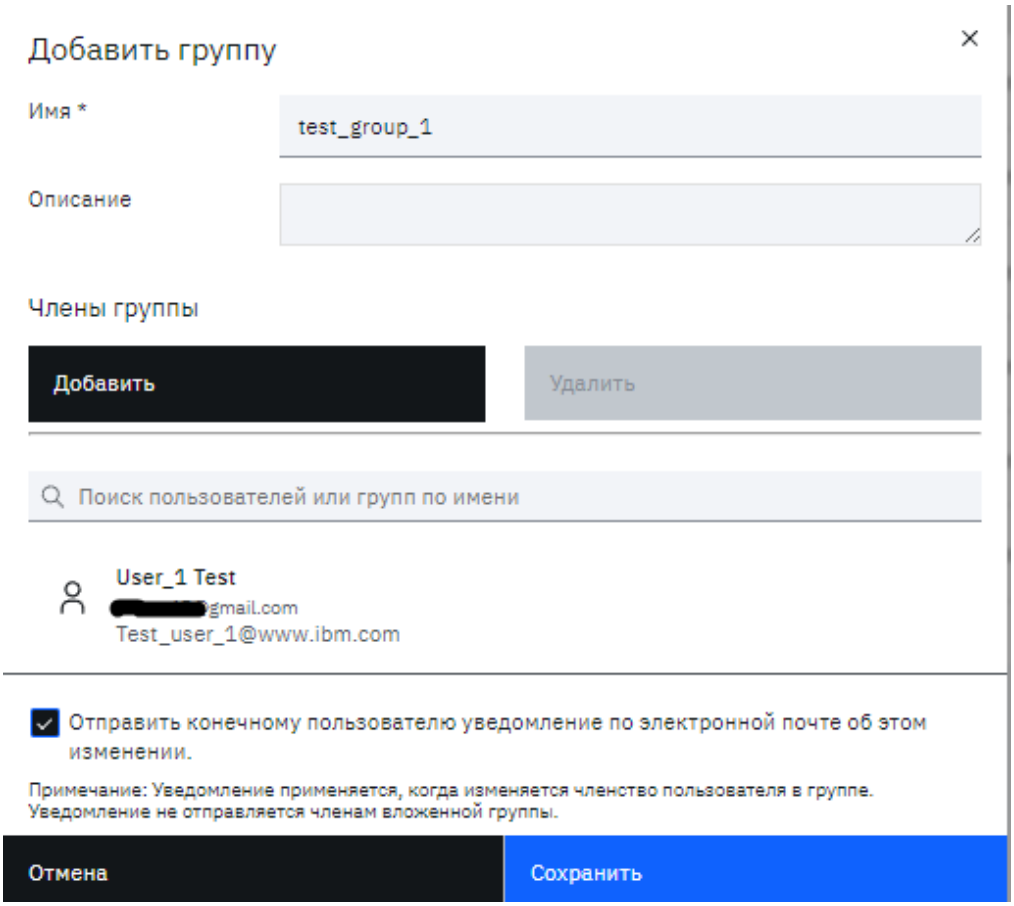

Рис. 2.23. Меню створення групи

Далі йде створення політик доступу до додатків, що дозволяє повністю налаштувати те за якими саме правилами автентифікації буде надано доступ до додатка. Політики діляться на два основних типи: об’єднана політика для отримання доступу до системи та політика доступу до підключених додатків.

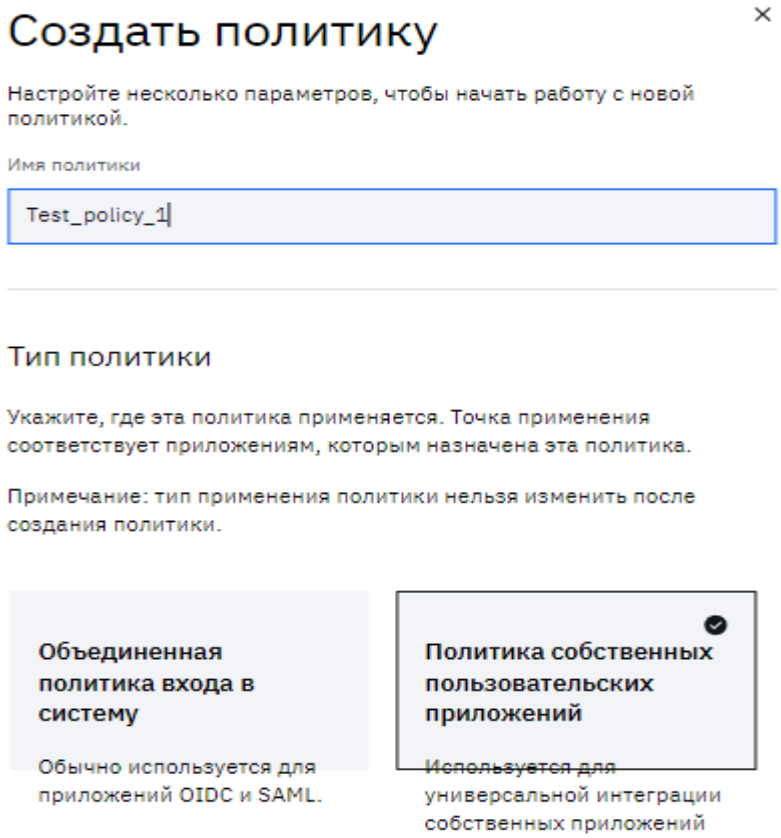

Рис. 2.24. Меню створення політики

Після вибору необхідного типу політики обираються правила для першого контакту користувача з додатком, повторної автентифікації та політик SSO. Керування політиками відбувається завдяки створенню умов, що базуються на параметрах типу “IF”, “AND”, “OR”, “NOT” тощо.

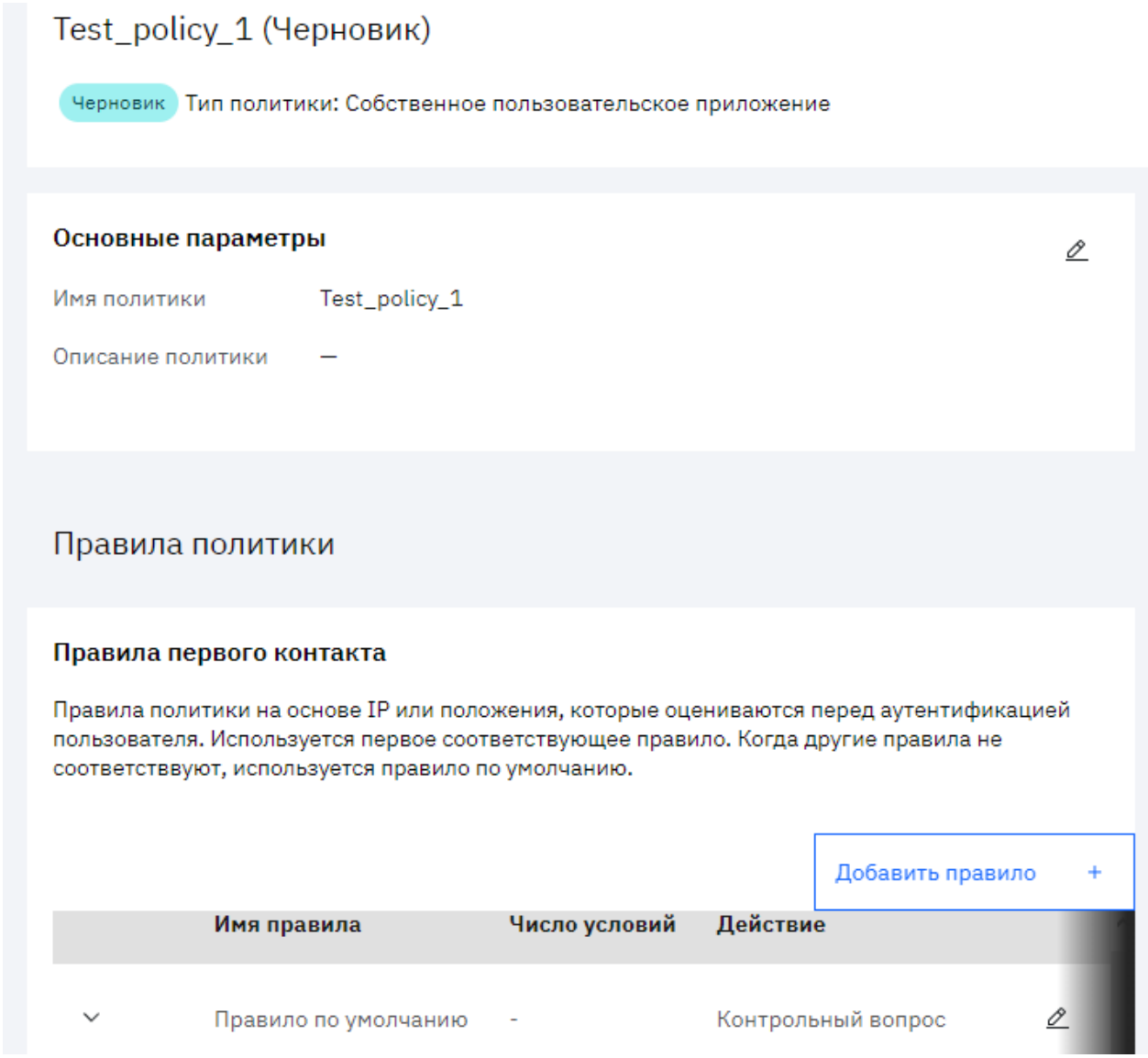

Рис. 2.25. Меню налаштування політики доступу

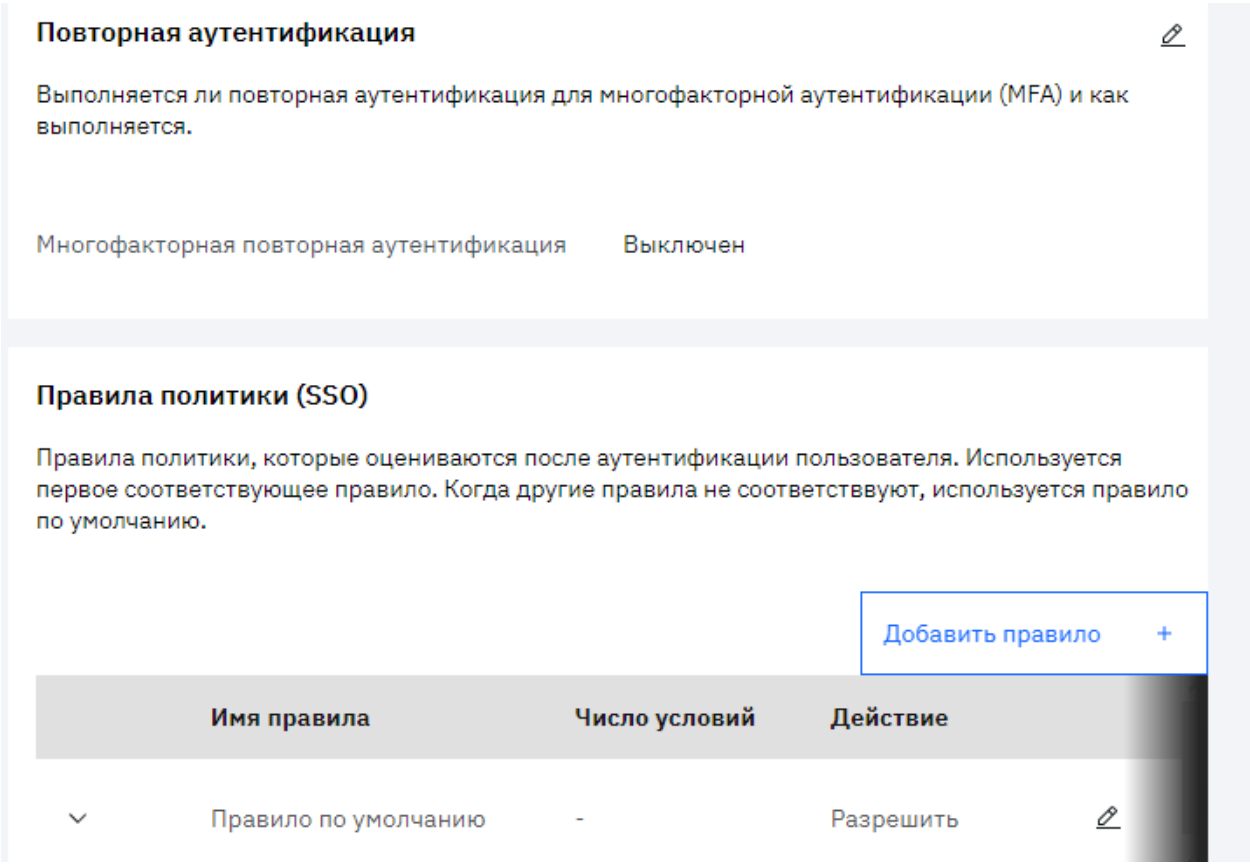

Рис. 2.26. Продовження меню налаштування політики доступу

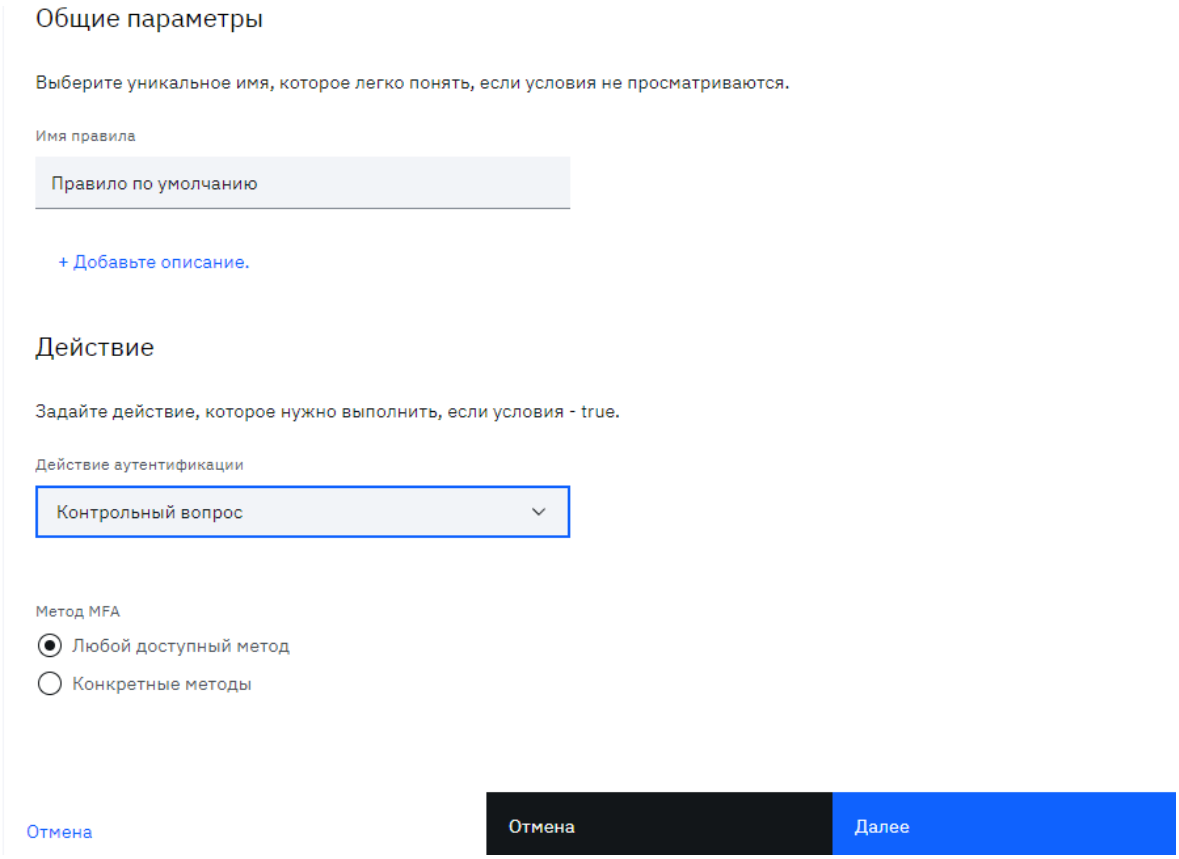

Рис. 2.27. Меню налаштування правила політики доступу

Також важливим функціоналом є керування парольними політиками та MFA. В плані парольних політик можна обрати межі довжини пароля, чи потребує пароль алфавітних символів, чисел та спеццсимволів, максимальний та мінімальний вік пароля, встановити максимальну кількість спроб та активувати можлвість заблокувати акаунт після того, як їх буде вичерпано, й налаштувати функцію відновлення пароля у випадку його забування. В плані налаштування MFA є можливість надати користувачам обрати ті фактори, що будуть для них зручнішими та налаштовувати умови за яких буде запитано MFA.

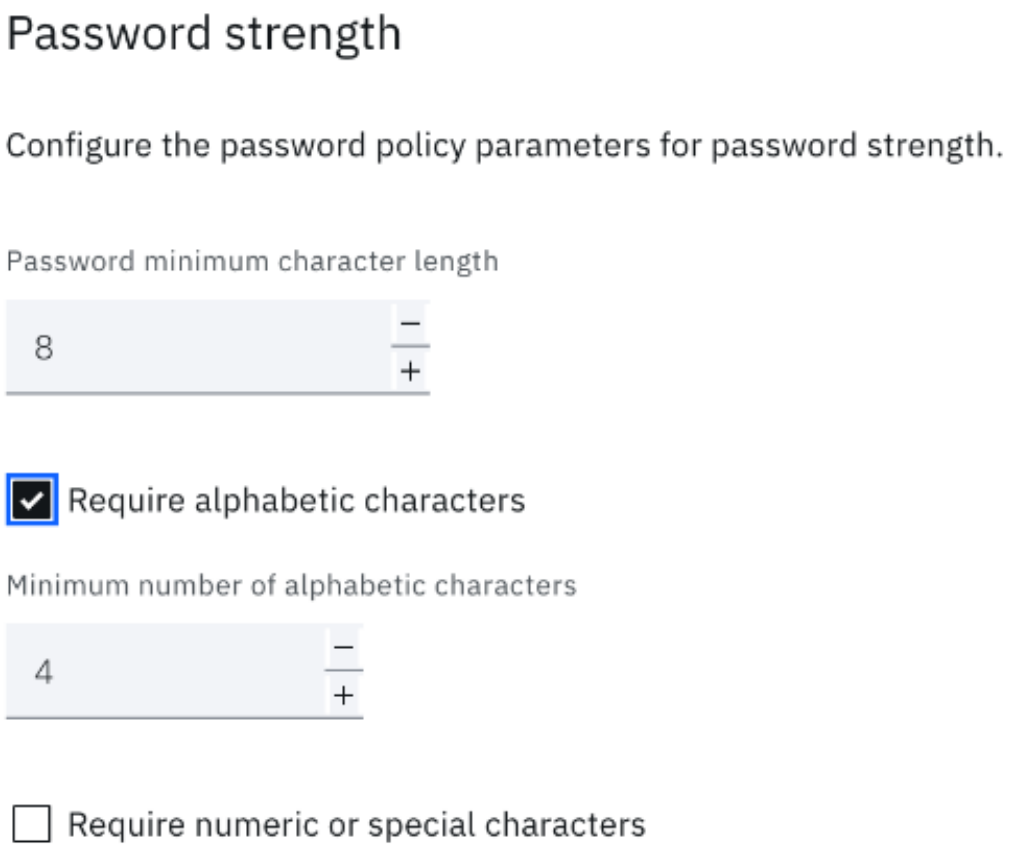

Рис. 2.28. Налаштування парольної політики [19]

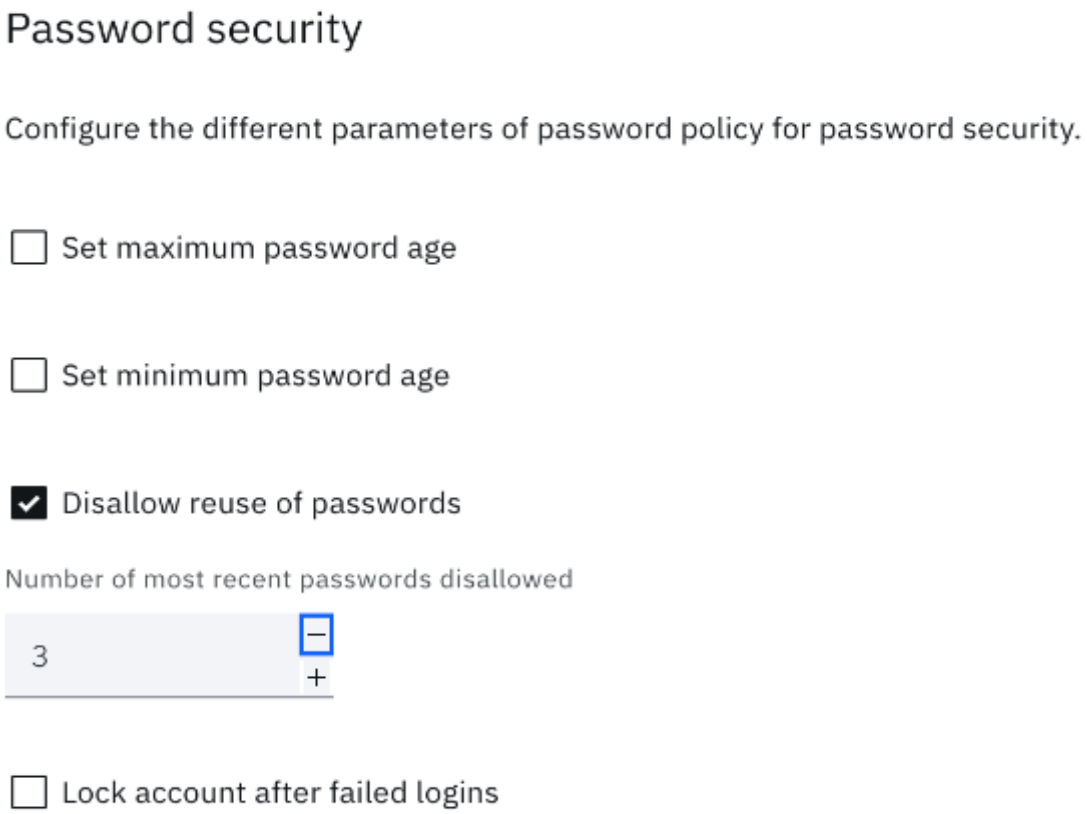

Рис. 2.29. Продовження налаштування парольної політики [19]

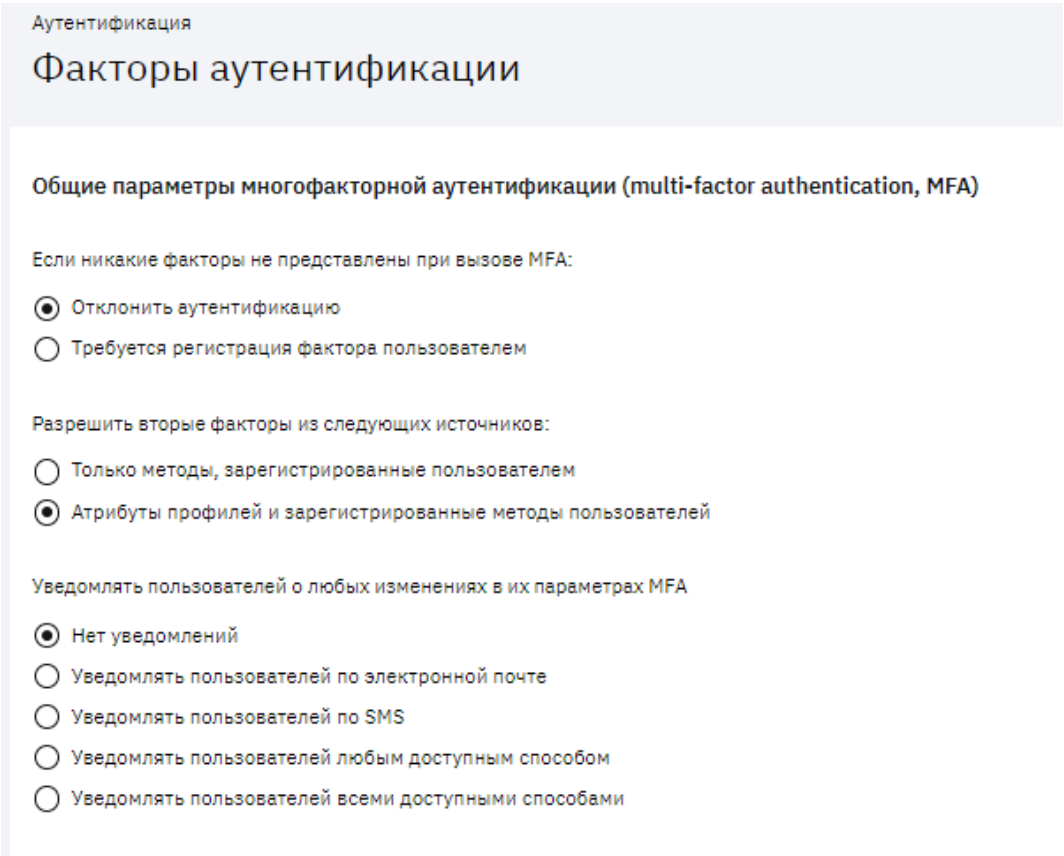

Рис. 2.30. Загальні конфігурації MFA

Додатково для MFA є можливість налагодити фактори автентифікації, як наприклад фактори OTP, обрати чи будуть вони надіслані на електронну пошту чи SMS-повідомленням на мобільний номер, яка в одноразового паролю буде довжина та набір символів. Для OTP, що відправляється електронною поштою можна проставити заборонені домени.

Рис. 2.31. Конфігурації OTP-факторів

Також дуже важливою функцією є можливість зв’язувати джерела ідентифікації під одним акаунтом, що полегшує керування користувачами.

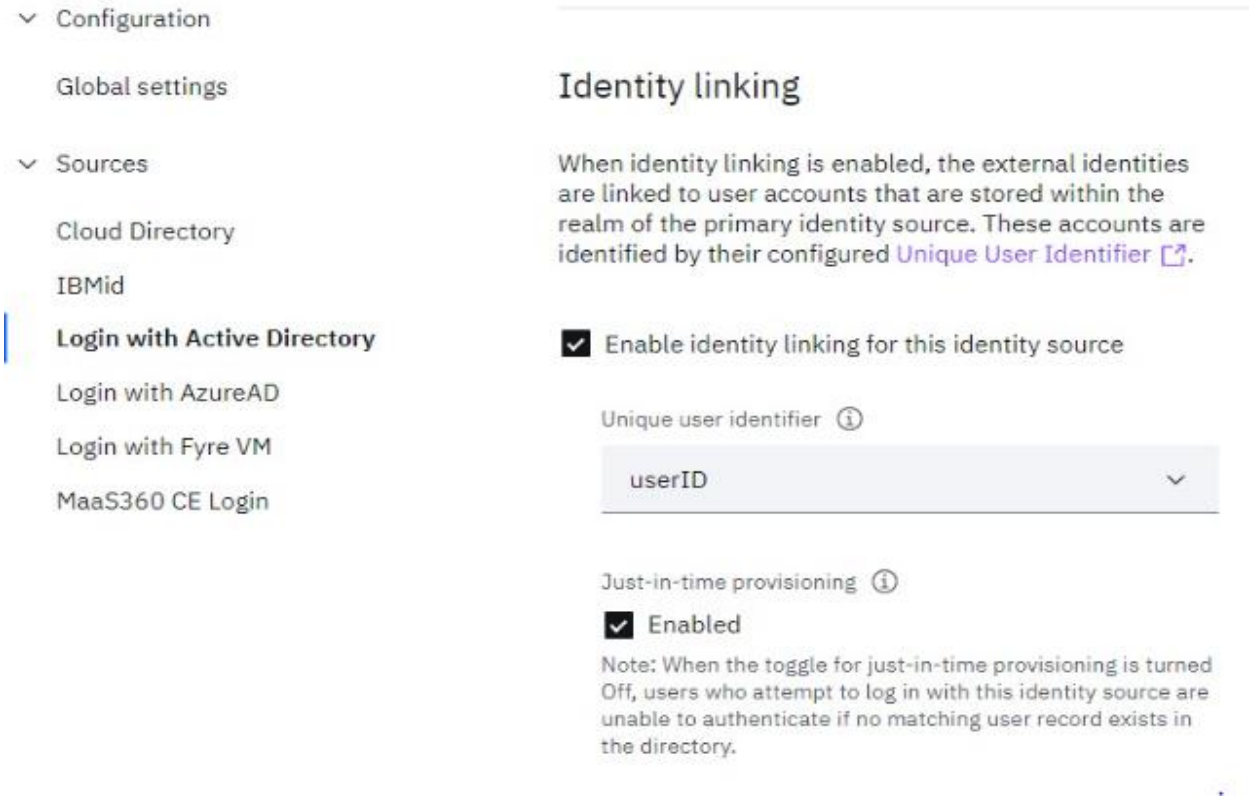

Рис. 2.32. Вибір можливості підв’язати зовнішні сутності до акаунту [19]

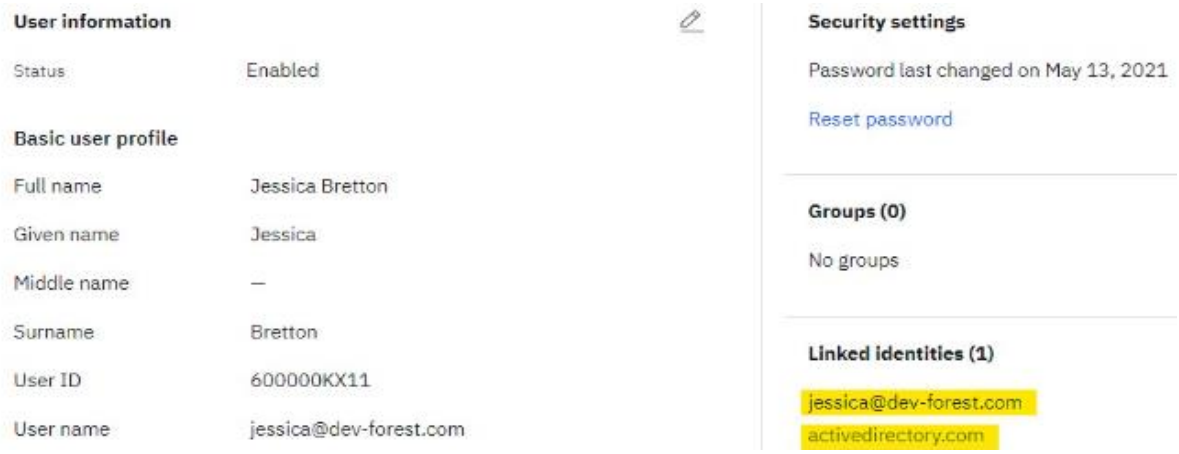

Рис. 2.33. Дані зовнішніх облікових записів на панелі користувача [19]

Загалом, оглянуте рішення має доволі широкий функціонал, що дозволяє налагодити IAM-процеси, чим значно підвищить захист даних та покращить бізнес-процеси в організації.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ КОРИСТУВАЧІВ НА БАЗІ РІШЕННЯ IBM SECURITY VERIFY

3.1. Додавання та конфігурація додатків у системі

Спочатку в систему вноситься додаток, в меню створення додатку є дві опції: використання шаблону, за яким можна внести будь-який додаток; вибір з широкого списку найпопулярніших додатків для бізнесу, освіти, IAM тощо.

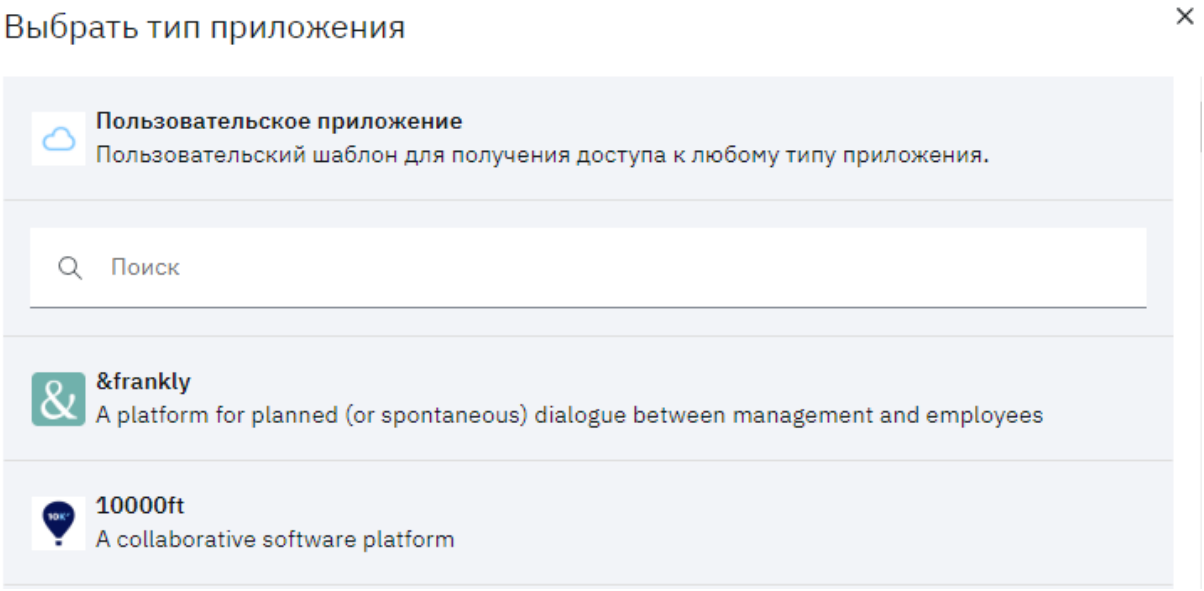

Рис. 3.1. Меню вибору типу додатка

Обравши необхідний тип додатка, вносяться перші необхідні дані: назва додатку в системі; опис; назва компанії, та проводяться необхідні налаштування відображення на панелі запуску, чи буде додаток одразу активовано або деактивовано, додається власник додатка (за потреби).

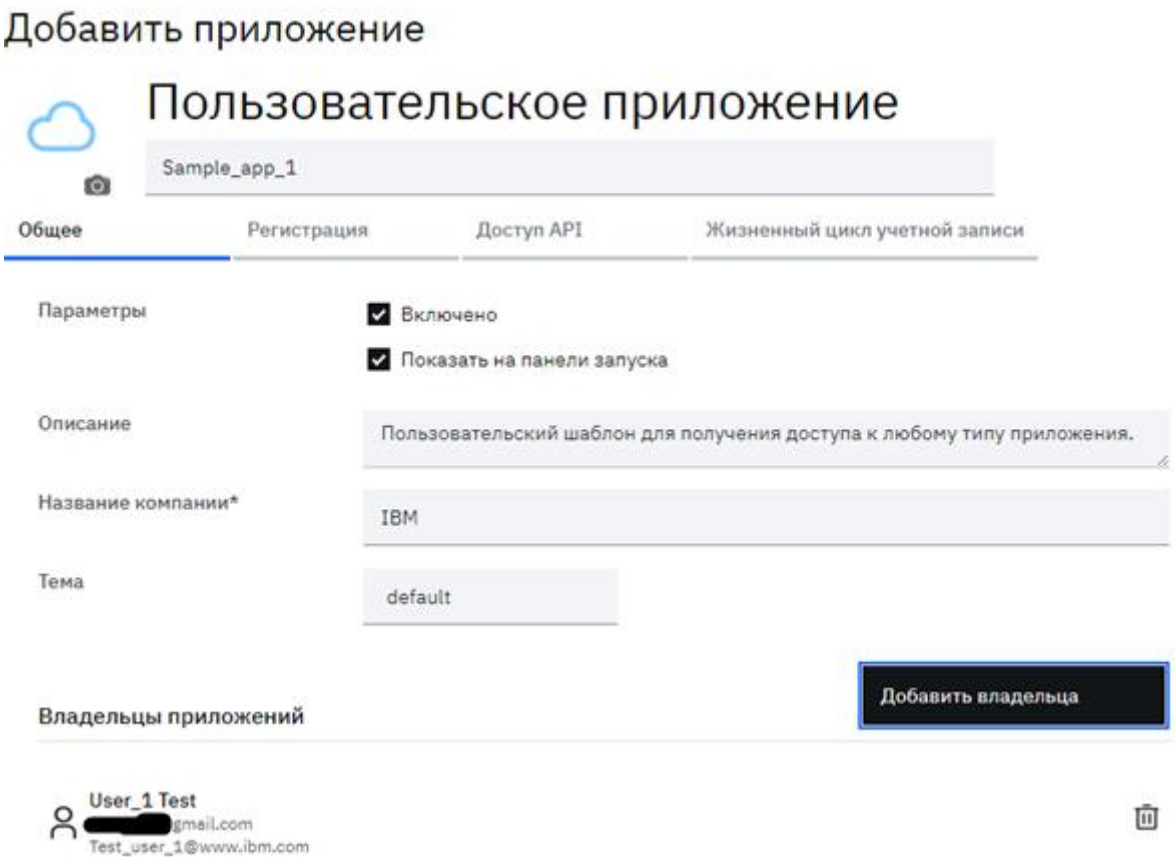

Рис. 3.2. Меню введення загальної інформації про додаток

Для демонстрації роботи деяких функцій IBM надають доступ до додатка-прикладу та інструкцію по зв'язуванню. Для зв'язування зовнішнього додатка з Security Verify потрібно ввести URL-посилання входу та виходу з системи та сертифікат провайдера ідентифікації, взамін додаток надає ідентифікатор провайдера, URL ACS та URL SSO.

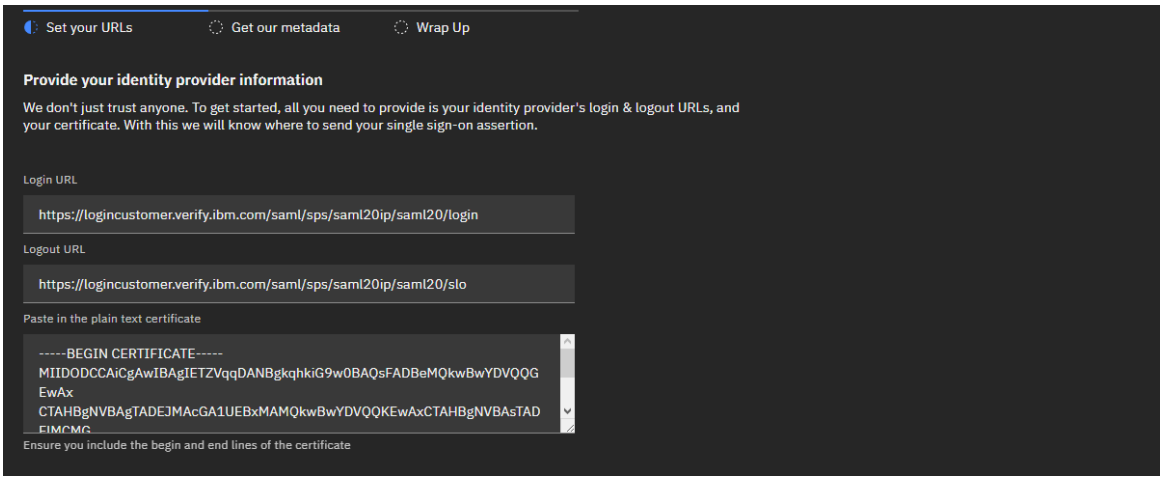

Рис. 3.3. Меню введення посилань та сертифікату

Рис. 3.4. Дані потрібні для підв'язки до Security Verify

Після цього йде процес реєстрації додатка в Security Verify, куди вводяться отримані дані, налаштовуються інші опції та надаються доступи користувачам, в залежності від потреб. Тут можна налаштувати унікальний ідентифікатор додатка(за наявністю), алгоритми та параметри цифрового підпису для забезпечення довіри між провайдером послуг та сервісом Verify, атрибути користувачів, що приймає додаток, з якими провайдерами ідентифікації взаємодіє додаток, налаштувати доступи для користувачів і груп користувачів до даного додатку та обрати які з джерел автентифікації доступні для нього.

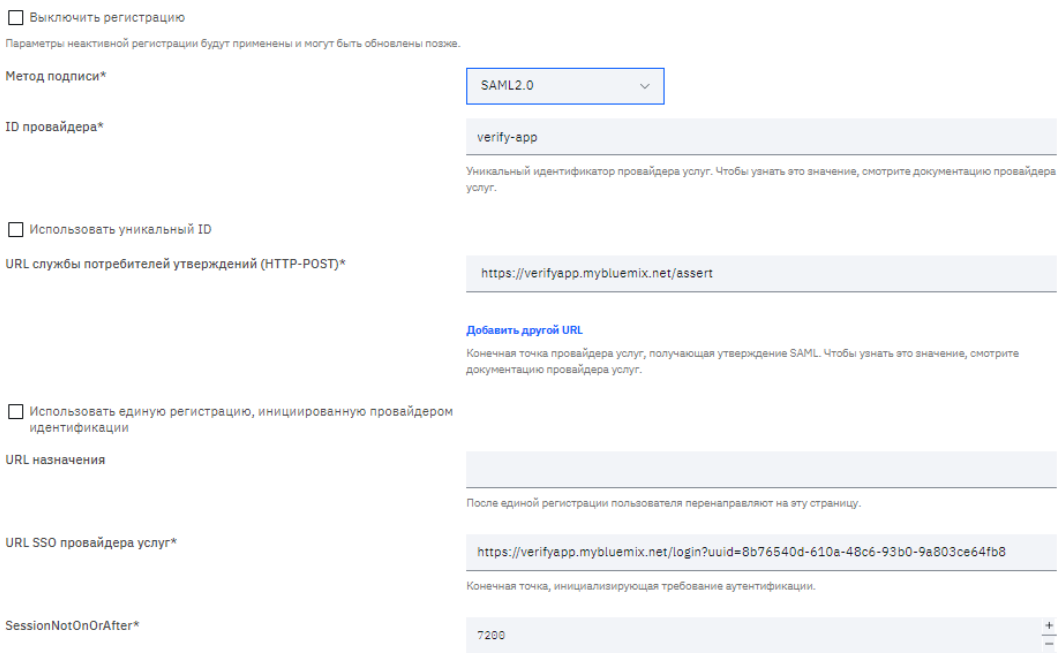

Рис. 3.5. Початок процесу реєстрації додатка в системі

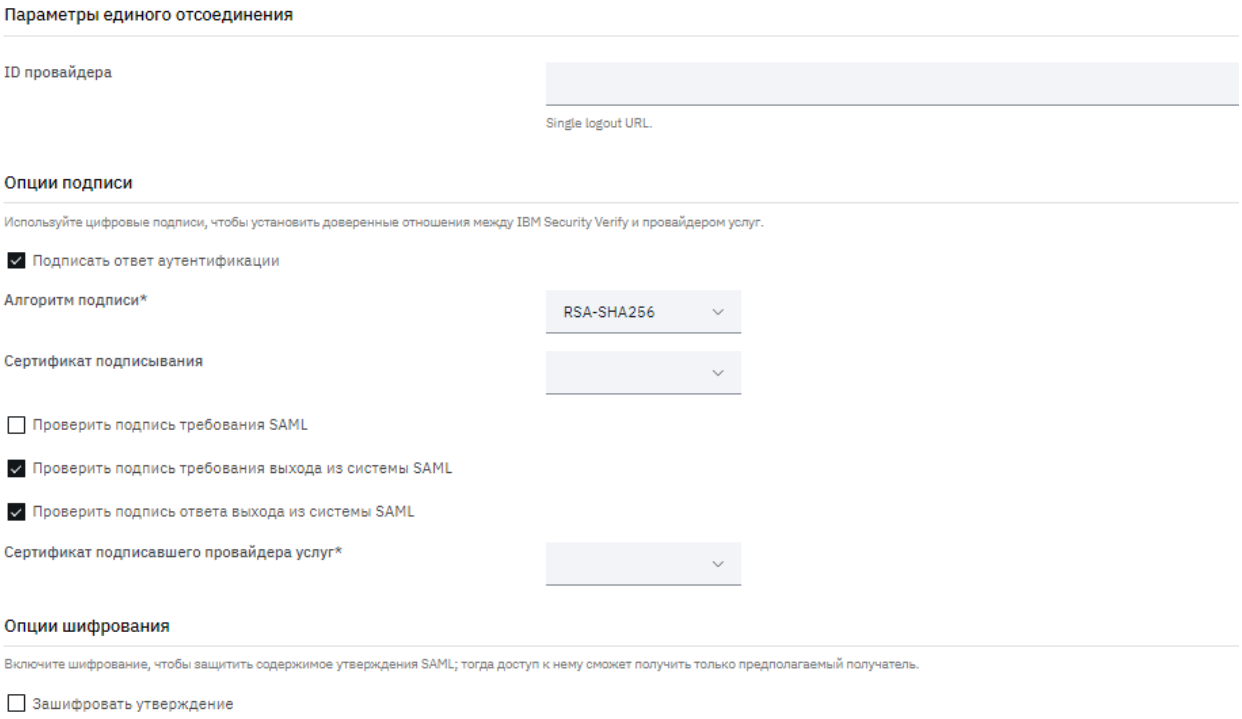

Рис. 3.6. Продовження налаштування реєстрації додатка

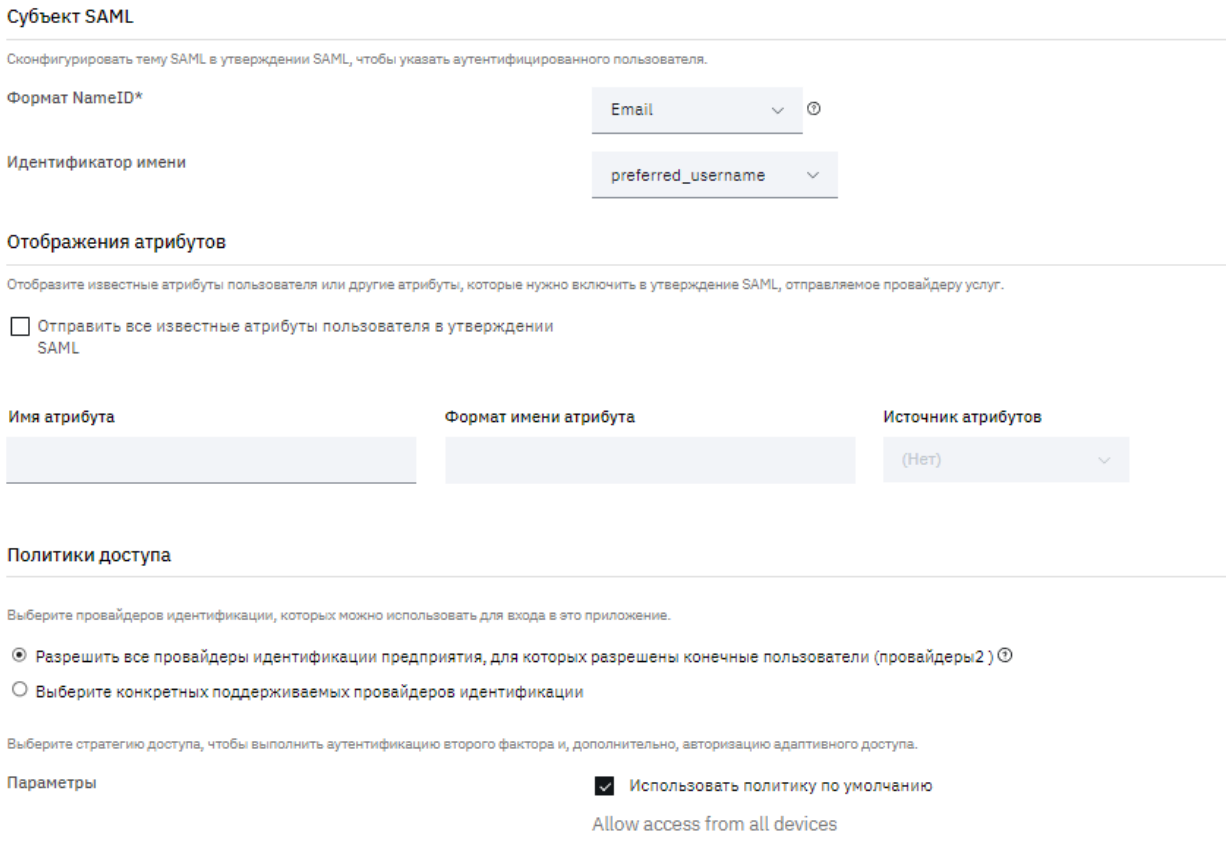

Рис. 3.7. Продовження налаштування реєстрації додатка

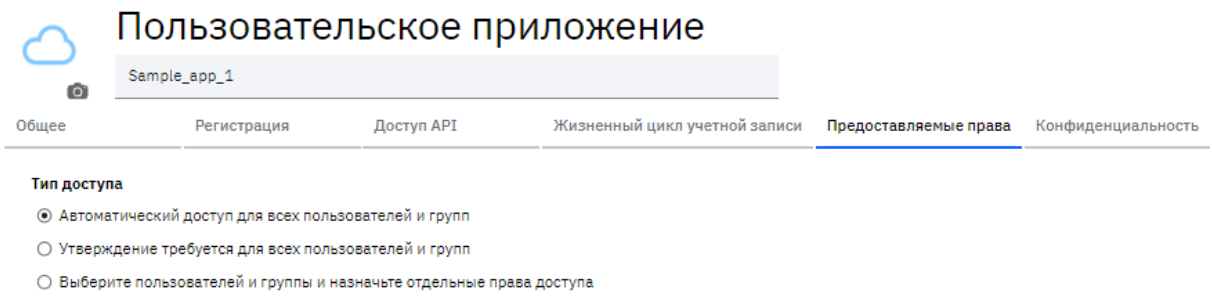

Рис. 3.8. Опції прав доступу користувачів

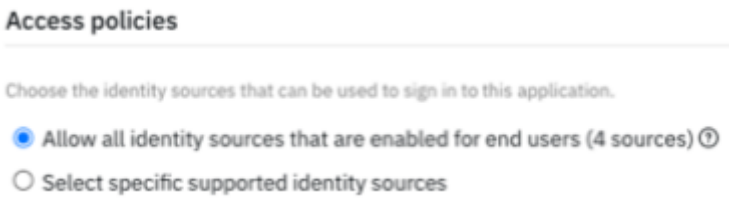

Рис. 3.9. Надання доступу до усіх джерел ідентифікації[19]

Тепер даний додаток відображається на панелі порталу і до нього можна отримати доступ через нього.

Рис. 3.10. Вигляд додатку на порталі

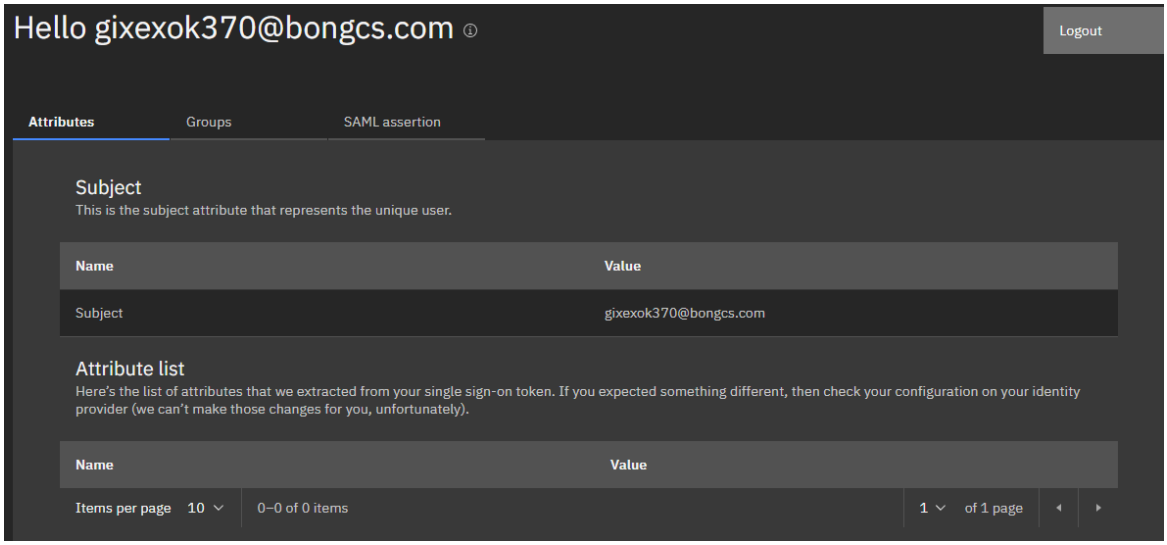

Рис. 3.11. Вигляд демонстраційного додатку

3.2. Реалізація політик доступу у системі

Використовуючи функціонал рішення можна налаштувати політики задля підвищення захисту системи. Наприклад, є група користувачів «Sales», що відповідає з операції пов’язані з процесами продажу товарів та послуг компанії, тому їхні дані вимагають особливого захисту. Однією з мір захисту є запит MFA при заході користувачами до системи з нового девайсу, цей процес реалізується проставлянням відповідних правил та умов при конфігуванні політики. В даному випадку це логічно реалізується наступним чином: за умови існування даного користувача у списку групи, перевіряються атрибути його приладу, якщо виявлено, що відповідний атрибут вказує на новизну даного девайсу у системі, запитується MFA. [19]

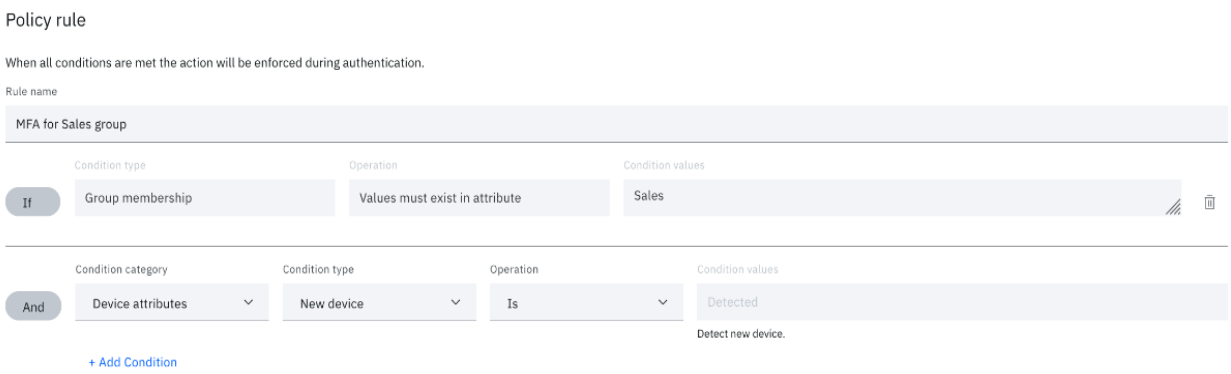

Рис. 3.12. Налаштування правила політики, для групи продаж, що визначає запит MFA при першому заході у систему з девайса [19]

3.3. Додавання сторонніх джерел ідентифікації

Одним з найпоширеніших репозиторіїв, що зберігає облікові дані є Microsoft Active Directory. IBM Security Verify дозволяє підв’язати до себе дане рішення, щоб користувачі більшості систем могли війти до ІТС використовуючи вже наявні там дані.

Для початку роботи з підключення Active Directory до Security Verify спочатку треба розгорнути систему IBM Security Verify Bridge, що може бути

розгорнута у вигляді служби на Windows-сервері, або у вигляді контейнера на Linux-сервері. Security Verify Bridge повинна мати налаштований вихідний зв’язок з контролером доменів AD та стабільний інтернет-зв’язок з вже розгорнутою в хмарі Security Verify.[19]

Спочатку необхідно зібрати LDAP-посилання, сертифікат наданий контролером доменів та дані користувача, що потрібні для його додавання та розпізнавання у системі згідно з нормами підприємства.

Item	Example Value/Format

LDAP URIs for one or more Active Directory domain controllers that will be used for authentication.	`ldaps://dc1.example.com`
	`ldaps://dc2.example.com`
	
	Note: If your Active Directory not configured for secure communication, use `ldap://` instead.

CA certificate that validates the server certificates presented by Domain Controllers on LDAPS connections.	Base64-encoded certificate file. This has format
	`-----BEGIN CERTIFICATE-----`
	`...`
	`-----END CERTIFICATION-----`

Distinguished Name (DN) of an Active Directory account with read permissions. No special permissions required.	`cn=bridge,cn=users,dc=example,dc=com`
Password for the Active Directory account above.	–
Branch in Active Directory where users are stored. Used as LDAP *Base*.	`cn=users,dc=example,dc=com`
Unique Active Directory attribute that end users will use as their username.	Usually `samAccountName` (username) or `userPrincipalName` (username@domain.com)
List of user attributes that you want to make available to IBM Security Verify.	`cn, sn, mail, telephone, memberOf`

Рис. 3.13. Дані необхідні до внесення у відповідні поля в Security Verify[19]

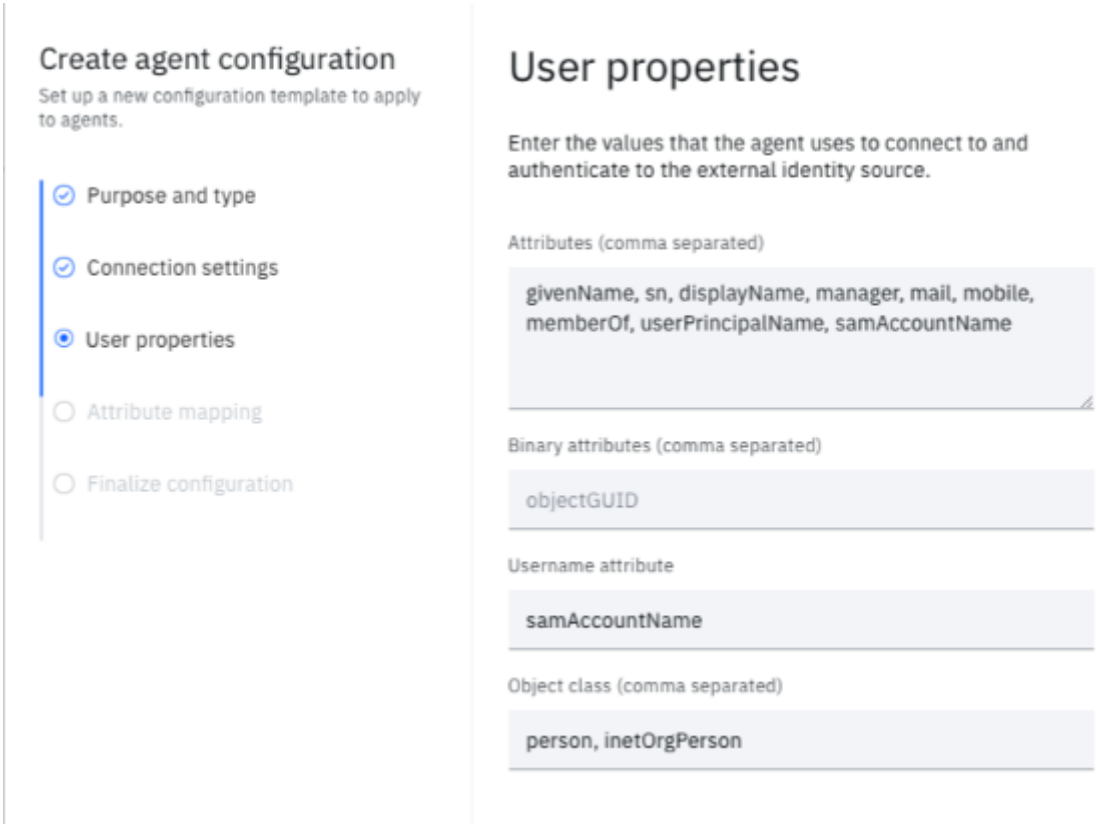

Рис. 3.14. Внесення даних з’єднання Active Directory[19]

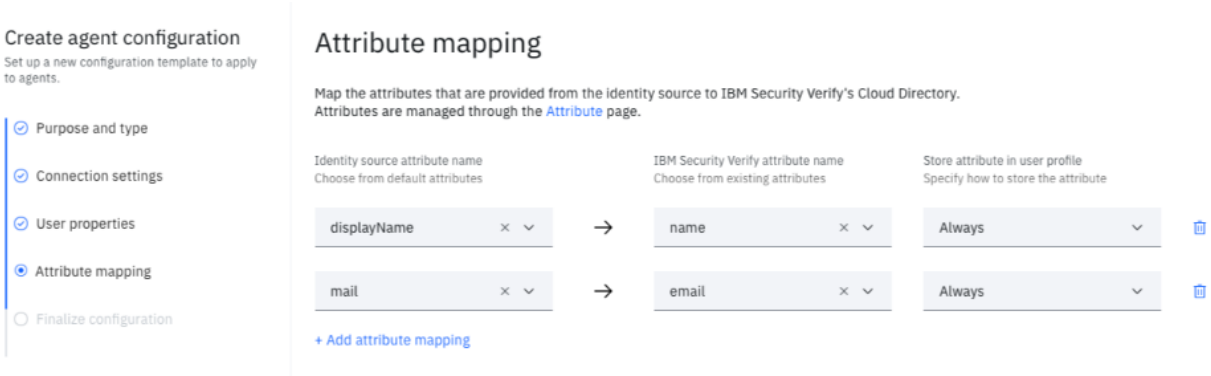

Рис. 3.15. Проставляння атрибутів користувачів[19]

Після зберігання даної сутності агента ідентифікації, буде надано ідентифікатор та секрет даного агента, які вводяться в IBM Verify Bridge після чого починається процес валідації.[19]

```
...
2021-01-12 14:50:37.155:httpmod.go:618: getBearerToken():
expiresAt=2021-01-12 16:50:36.7057442 +0000 GMT m=+7200.071289101
getNewTokenAt=2021-01-12 16:44:36.7057442 +0000 GMT m=+6840.071289101 EX
...
2021-01-12 14:50:37.155:opprocmod.go:363: run(): Waiting for operations
2021-01-12 14:50:37.155:main.go:307: run(): NewConfig event received
...
2021-01-12 14:50:37.462:main.go:332: run(): NewConfig event processing
done
2021-01-12 14:50:37.462:opprocmod.go:363: run(): Waiting for operations
...
2021-01-12 14:50:37.511:ldapauth.go:1193: getLDAPType(): type=Active
Directory
2021-01-12 14:50:37.511:ldapauth.go:1206: getLDAPType(): autoset group
membership attr = memberOf
2021-01-12 14:50:37.511:ldapauth.go:237: setLdapState(OK)
```

Рис. 3.16. Процес валідації в консолі[19]

По завершені процесу валідації адміністратор Security Verify матиме доступ до агента через свій інтерфейс, а користувачі системи зможуть отримати доступ до неї через Active Directory.

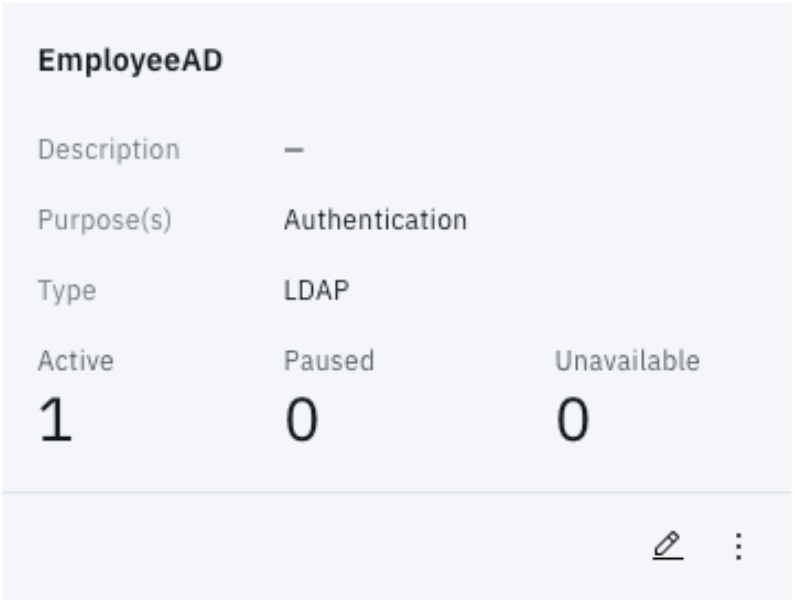

Рис. 3.17. Вигляд агента ідентифікації на інтерфейсі адміністратора[19]

Рис. 3.18. Варіант безпарольної автентифікації через Active Directory у пропонованих варіантах[19]

3.4. Управління доступами та дозволами користувачів через сторонні джерела ідентифікації

Ще однією можливістю є керування дозволами та доступом, через зовнішні провайдери автентифікації. Для реалізації цього спочатку необхідно створити агент ідентифікації та надати йому відповідні параметри: мету агента та спосіб його підключення.

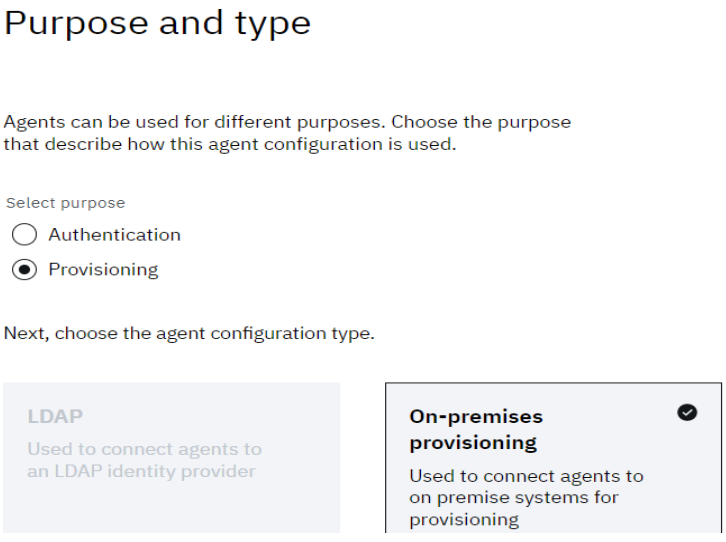

Рис. 3.19. Вибір мети агента конфігурації[19]

Важливою деталлю є те, що Security Verify для налагодження даного процесу використовує модуль Verify Bridge for Provisioning, що вимагає контейнерні образи, що будуть розгорнені в цільовому середовищі. Даний модуль складається з трьох компонентів, які створені для роботи в Docker та інших середовищах оркестрації контейнерів:

Verify Bridge – використовується як проксі, що налагоджує комунікацію між адміністраторським акаунтом Security Verify та цільовим середовищем через агент;

Verify Identity Brokerage – безпосередньо оркеструє процес пошуку та надання доступів та розгалужених дозволів обліковим записам;

Identity Brokerage DB (Postgres) – утримує стан дозволів та профілі конфігурації. [19]

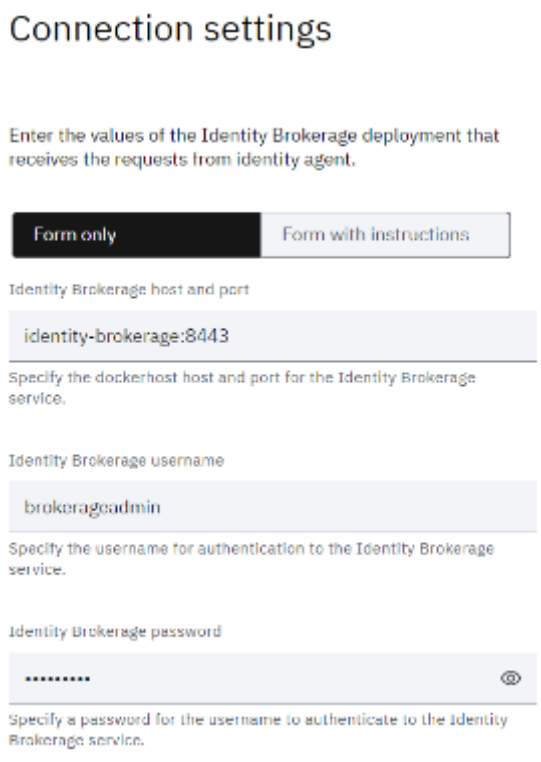

Рис. 3.20. Зв’язування з Verify Identity Brokerage [19]

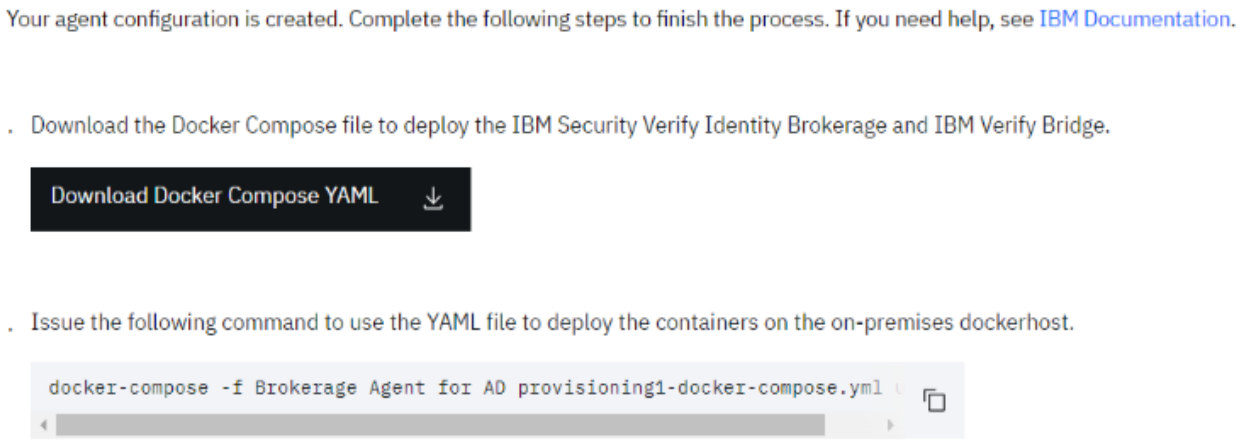

Рис. 3.21. Завершення налаштування, меню завантаження YAML-файла [19]

Далі необхідно мати контейнери для бази даних користувацької інформації, Identity Brokerage, Verify Bridge та відповідний адаптер для зовнішнього джерела ідентифікації. Використавши файл отриманий після налагодження агента налаштовуємо контейнери, а через сайт IBM отримуємо необхідний JAR-файл, в залежності від того, який сервіс потрібен. [19]

```
docker-compose -f docker-compose.yml up -d
[root@xxxxxxxx ~]# docker ps -a
CONTAINER ID        IMAGE
722165e62ae9        ibmcom/verify-bridge:latest
f26aade1cec6        postgres:12-alpine
1b45372dc651        ibmcom/identity-brokerage:latest
[root@xxxxxxxx ~]#

COMMAND                  CREATED STATUS                                          NAMES
"/sbin/bootstrap.sh"     4 months ago                                            verify-bridge
"docker-entrypoint..."   5 months ago      0.0.0.0:5432->5432/tcp                ibdb
"/sbin/bootstrap.sh"     6 months ago      9080/tcp, 0.0.0.0:8443->8443/tcp, 9443/tcp   identity-brokerage
```

Рис. 3.22. Налаштування контейнера у консолі [19]

Після чого необхідно створити профіль додатків та підв’язати відповідні дані, почекати поки профіль ініціалізується та розмістити його.

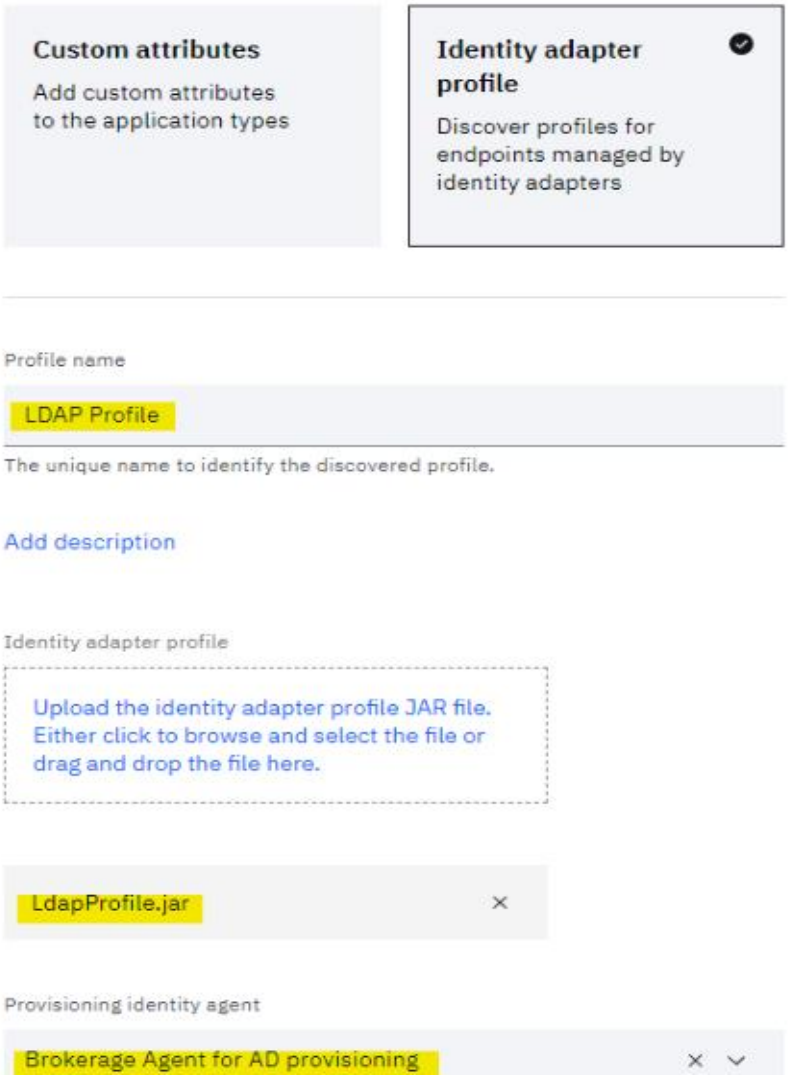

Рис. 3.23. Налаштування профіля додатків[19]

Attributes

Attribute name	Data type	Read-only	Is multi-valued
eruid	string	False	No
erpassword	string	False	No
active	boolean	False	No
l	string	False	No
st	string	False	No
groups[].value	string	True	Yes
groups[].display	string	True	Yes

Рис. 3.24. Атрибути отриманого профіля[19]

Далі на цільовому сервісі встановлюється Identity Adapter RMI Dispatcher, що є ключовим для зв'язку рішення з адаптерами. Після цього, використовуючи ISIM Active Directory Adapter можна налагодити наданням та відключенням прав через Active Directory. [19]

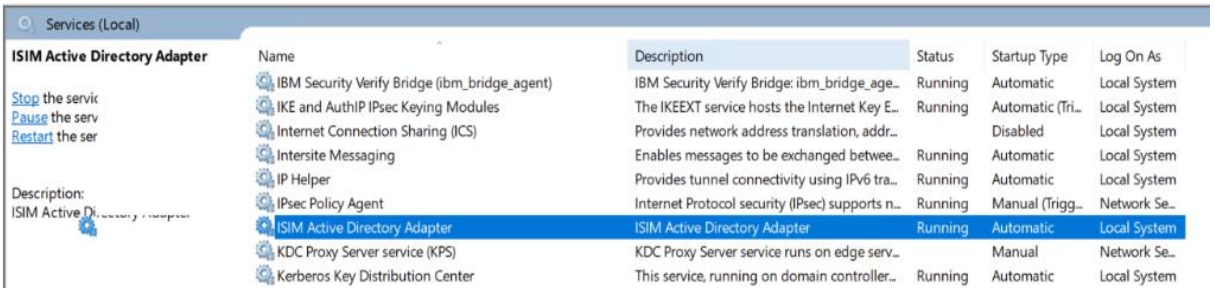

Рис. 3.25. Вигляд ISIM Active Directory Adapter у списку сервісів AD [19]

Додавши Active Directory у список додатків в Security Verify, необхідно проставити відповідні налаштування та підв'язяати адаптер. Після чого можна обрати яким чином буде виконуватись синхронізація даних: відключена автоматична синхронізація; дані в Security Verify оновлюються з підключеного сервісу; значення в сервісі оновлюються згідно введеним адміністратором в Security Verify. [19]

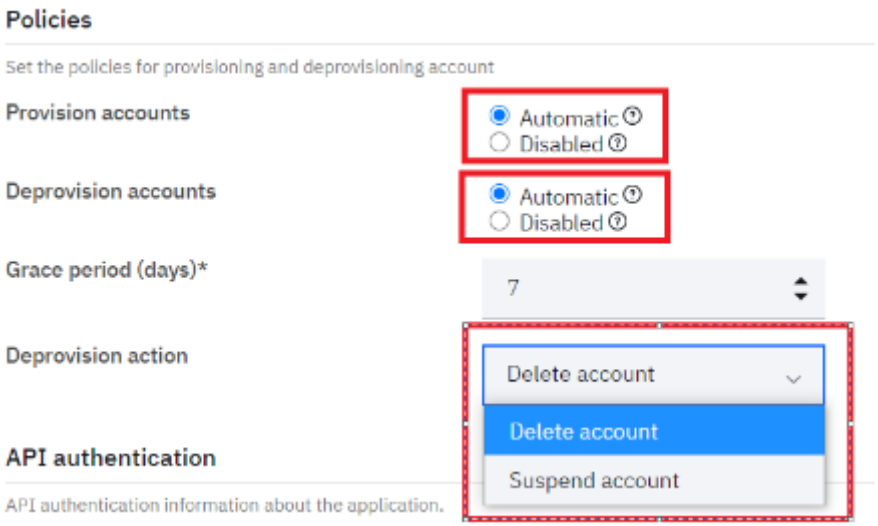

Рис. 3.26. Налаштування політик надання та відбирання доступу, вибір дії при відібранні доступу [19]

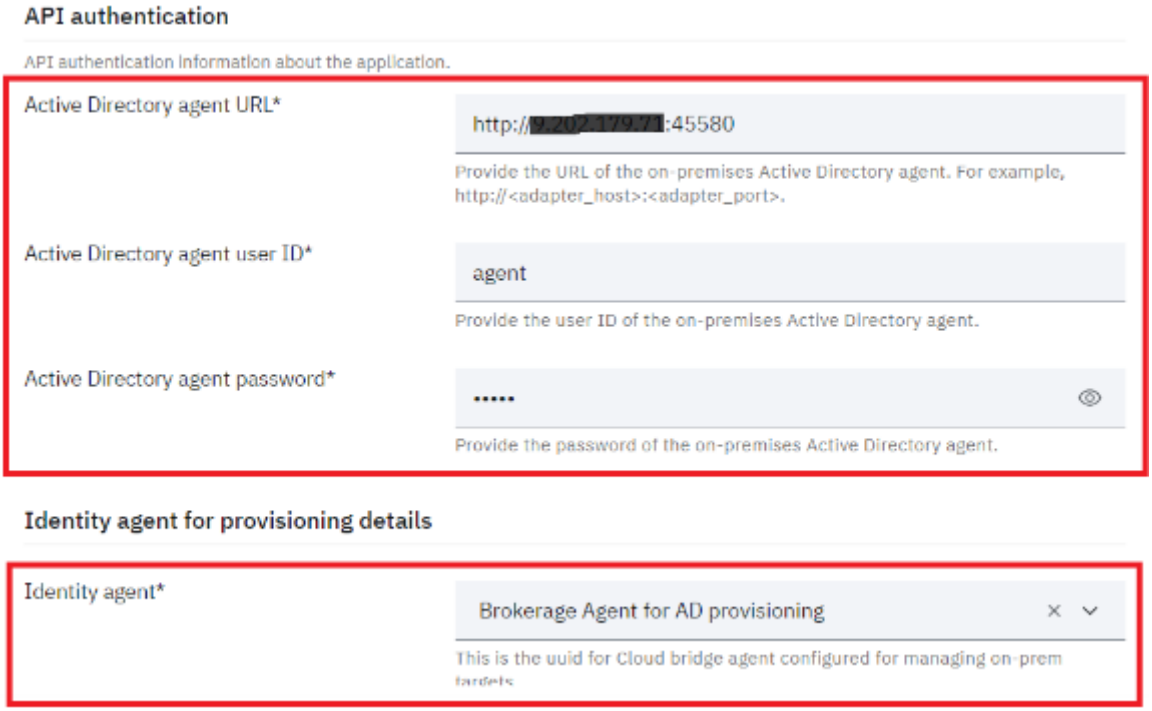

Рис. 3.27. Зв’язування з ISIM Active Directory Adapter [19]

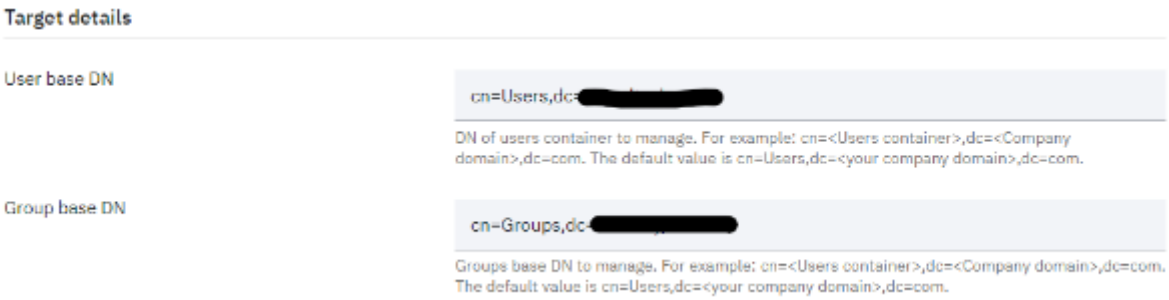

Рис. 3.28. Вибір доменів користувачів та груп [19]

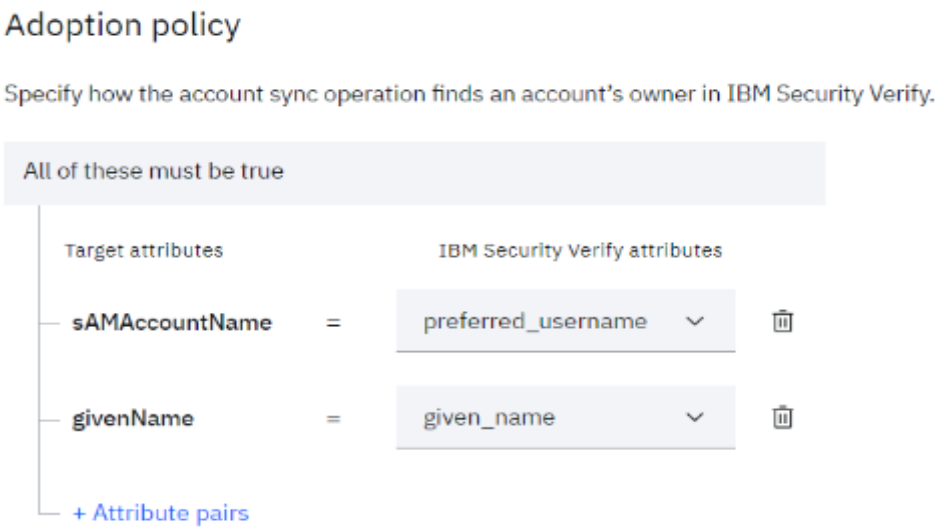

Рис. 3.29. Вибір атрибутів для синхронізації [19]

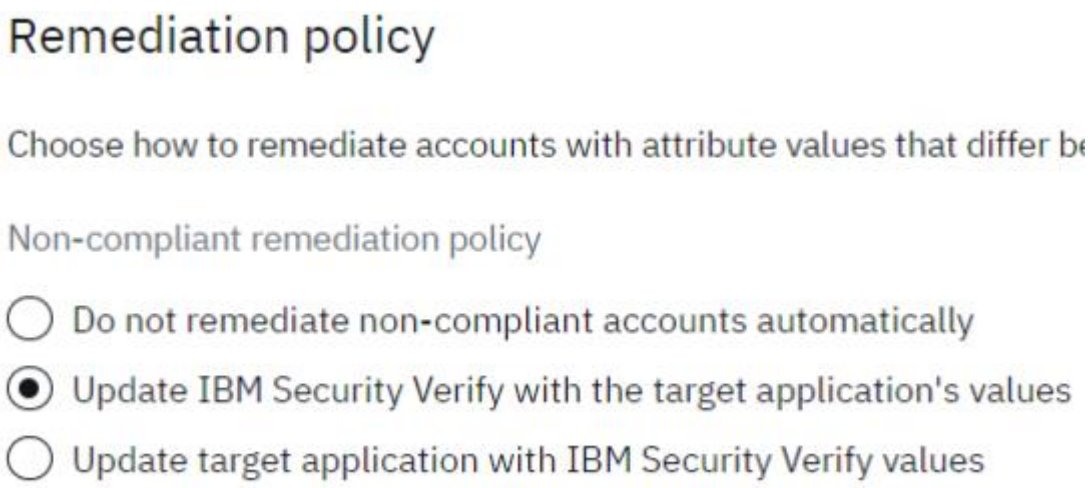

Рис. 3.30. Вибір політики синхронізації даних [19]

Коли усі необхідні налаштування завершено, можна використовувати отримані від AD, дані для надання доступів користувачам.

3.5. Розроблення рекомендацій щодо управління ідентифікацією та доступом користувачів

Проаналізувавши усі вищевказані проблеми та способи і заходи щодо їх вирішення можна вивести наступні рекомендації щодо IAM:

необхідно постійно стежити за тенденціями та змінами в сфері IT;

слід постійно оновлювати та покращувати ІТС організації та відповідні політики;

варто будувати ІТС та політики доступу відповідно до міжнародних та державних стандартів;

необхідно постійно слідкувати за дотриманням користувачами політик безпеки та періодично проводити заходи з підвищення ними обізнаності про інформаційну безпеку;

користувачам не варто використовувати легкі для згадування паролі та використовувати однакові паролі для різних облікових записів;

ІАМ-система повинна постійно оновлюватись та актуалізуватись;

ІАМ-система має базуватись на технічних стандартах обміну ідентифікаційними даними;

слід дотримуватись принципів zero-trust;

необхідно слідкувати за тим, щоб користувачі могли отримувати доступ лише до ресурсів визначених корпоративною необхідністю;

не дивлячись на те, що доступ до ідентифікаційних даних надається в одному хабі, усі репозиторії даних мають бути розгалужені та добре захищені;

адміністратори мають відслідковувати нові, нетипові та підозрілі дії та процеси й оперативно про них інформувати відповідних осіб;

не слід засмічувати систему непотрібними додатками, процесами, користувачами-привидами тощо;

новим користувачам, групам користувачів, політикам, атрибутам, агентам ідентифікації варто давати зрозумілі імена;

необхідно проводити процес зв’язування акаунтів для усіх облікових записів користувача;

користувачам необхідно назначати процедури MFA;

необхідно підв’язувати зовнішні джерела ідентифікації;

варто користуватись системами виявлення ризиків;

варто забезпечити процес валідації певних дій користувачів у системі відповідними працівниками.

ВИСНОВКИ

В роботі проаналізовано проблеми пов’язані з управлінням ідентифікацією та доступом користувачів до інформаційної системи організації, встановлено сутність завдань методів та заходів управління ідентифікації та доступу користувачів.

Проаналізовано існуючі системи управління ідентифікацією та доступом користувачів. Досліджено технологію управління ідентифікацією та доступом на базі рішення IBM Security Verify.

Визначено методи та засоби ідентифікацією та доступом користувачів, що реалізовано в IBM Security Verify.

Визначено основні функції та принципи роботи хмарної технології IBM Security Verify, що являє собою платформу керуванням користувачами, додатками та політиками доступу. Також дане рішення має зручний інтерфейс для управління доступами користувачів.

IBM Security Verify надає гнучку платформу, що дозволяє реалізувати необхідні засоби для управління ідентифікацією та доступом користувачів, такі як: багатофакторна авторизація; система єдиного входу; адаптивний доступ; зв’язування з провайдерами ідентифікації; методи безпарольної ідентифікації тощо.

Розглянуто можливі конфігурації IBM Security Verify для забезпечення нормального управління ідентифікацією та доступом користувачів.

Розроблено рекомендації для фахівців, щодо застосування методів та засобів управління ідентифікацією та доступом користувачів.

Таким чином, правильна реалізація управління ідентифікацією та доступом користувачів на базі рішення IBM Security Verify має забезпечити ефективне керування потоком ідентифікаційних даних, розгалуження доступів та реалізацію політик безпеки в інформаційно-телекомунікаційній системі організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gartner Glossary: Identity and Access Management (IAM) [Електронний ресурс] – Режим доступу: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

2. Герніченко Г.Д. управління ідентифікацією та доступом користувачів до інформаційної системи. Актуальність та проблеми. *Актуальні проблеми кібербезпеки:* матеріали наук.-практ. інтерн.-конф., м. Київ, 27 жов. 2022 р. Київ, 2022. С. 176-178.

3. Recognizing the seven stages of a cyber-attack [Електронний ресурс] – Режим доступу: https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html

4. What is Identity and Access Management (IAM)? [Електронний ресурс] – Режим доступу: https://www.onelogin.com/learn/iam

5. What is identity and access management? Guide to IAM [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

6. Lessons from last year's major data breaches [Електронний ресурс] – Режим доступу: https://www.missioncriticalmagazine.com/articles/94175-lessons-from-last-years-major-data-breaches

7. DATA BREACHES AND IAM TRENDS [Електронний ресурс] – Режим доступу: https://identitymanagementinstitute.org/data-breaches-and-iam-trends/

8. The 5 Worst Data Breaches of All Time [Електронний ресурс] – Режим доступу: https://www.cccp.com/post/the-5-worst-data-breaches-of-all-time/

9. Mismanaged IAM Can Lead to Data Breaches [Електронний ресурс] – Режим доступу: https://securityboulevard.com/2022/04/mismanaged-iam-can-lead-to-data-breaches/

10. Top 8 Identity and Access Management (IAM) Challenges with your Hybrid-Cloud applications [Електронний ресурс] – Режим доступу: https://marketing.global.fujitsu.com/rs/807-GYW-324/images/ECSIAM-Top8Challenges.pdf

11. The Zero Trust Cybersecurity Model [Електронний ресурс] – Режим доступу: https://www.oneidentity.com/what-is-zero-trust/

12. 8 Protocols Used in Identity and Access Management [Електронний ресурс] – Режим доступу: https://www.sailpoint.com/identity-library/identity-management-protocols/

13. 7 Standards every IAM professional should know [Електронний ресурс] – Режим доступу: https://blog.plainid.com/7-identity-access-management-standards-professionals-should-know

14. Preventing Data Breaches with Identity and Access Management (IAM) [Електронний ресурс] – Режим доступу: https://www.pingidentity.com/en/resources/blog/post/preventing-data-breaches-with-iam.html

15. Security best practices in IAM [Електронний ресурс] – Режим доступу: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

16. The Top 10 Identity And Access Management Solutions [Електронний ресурс] – Режим доступу: https://expertinsights.com/insights/top-10-identity-and-access-management-solutions/

17. Best Identity and Access Management (IAM) Solutions for 2022 [Електронний ресурс] – Режим доступу: https://www.esecurityplanet.com/products/best-iam-software/

18. 2022 Gartner® Magic Quadrant™ for Access Management [Електронний ресурс] – Режим доступу: https://www.okta.com/resources/gartner-magic-quadrant-access-management/

19. IBM Security Verify Documentation Hub [Електронний ресурс] – Режим доступу: https://docs.verify.ibm.com/verify

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)