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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Гречук Діани Вадимівни*

академічної групи *125–20–3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо–професійною програмою *Кібербезпека*

на тему *Підсистема керування доступом системи управління закупівель SAP Ariba*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Кагадій Т.С.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	85	добре	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

“_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Гречук Діані Вадимівні*** **академічної групи** ***125–20–3***
(прізвище ім’я по–батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Підсистема керування доступом системи управління закупівель SAP Ariba***

затверджену наказом ректора НТУ “Дніпровська політехніка» від 23.05.2024 № 469–с

Розділ	Зміст	Термін виконання
Розділ 1	Стан авторизаційних концептів систем SAP Ariba і SAP S/4HANA та аналіз проблематики.	15.03.2024
Розділ 2	Аналіз ризиків використання гібридних систем та процедура впровадження технології Єдиного входу.	10.05.2024
Розділ 3	Розрахунок капітальних, експлуатаційних витрат та єфекту від впровадження технології у систему SAP Ariba.	11.06.2024

Завдання видано _____ Тетяна КАГАДІЙ
(підпис керівника) (ім’я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Діана ГРЕЧУК
(підпис студента) (ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка містить 65 сторінок, 14 рисунків, 6 таблиць, 4 додатка та 12 джерел.

Об'єкт розробки: Технологія Єдиного входу для гідридних підсистем на базі системи управління закупівель SAP Ariba.

Мета роботи: впровадження технології Єдиного входу та супутніх параметрів для покращення рівня безпеки в гібридних підсистемах на базі системи управління закупівель SAP Ariba.

У першому розділі кваліфікаційної роботи визначено загальні відомості програмного забезпечення SAP та супутніх продуктів, проаналізовано авторизаційні концепти систем SAP Ariba та SAP S/4HANA та визначено їх недоліки і проблематику.

У спеціальній частині були визначені та проаналізовані ризики пов'язані з недосконалістю стану безпеки у системі SAP Ariba, запропоновано рішення до впровадження технології Єдиного входу та розглянуто кінцеві сценарії реалізації взаємодії систем SAP Ariba та SAP S/4HANA з використанням технології Єдиного входу.

В економічному розділі було визначено витрати на розробку та впровадження технології та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи вдалося у забезпеченні захисту інформації у гібридних підсистемах на базі системи SAP Ariba, що підвищить рівень безпеки інформації та покращить управління доступом до інформації.

АВТОРИЗАЦІЙНИЙ КОНЦЕПТ, ТЕХНОЛОГІЯ ЕДИНОГО ВХОДУ, МОДЕЛІ КЕРУВАННЯ ДОСТУПОМ, АНАЛІЗ РИЗИКІВ, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

Explanatory note: 65 pp., 14 pic., 6 tables, 4 apps, 12 sources.

Object of development: Single sign–on technology for hybrid subsystems based on the SAP Ariba procurement management system.

The purpose of the work: implementation of Single Sign–On technology and related parameters to improve the level of security in hybrid subsystems based on the SAP Ariba procurement management system.

In the first section of the qualification work, the general information of SAP software and related products is defined, the authorization concepts of SAP Ariba and SAP S/4HANA systems are analyzed and their shortcomings and problems are identified.

In a special part, the risks associated with the imperfect state of security in the SAP Ariba system were identified and analyzed, a solution was proposed for the implementation of Single Sign–on technology, and the final scenarios for implementing the interaction of SAP Ariba and SAP S/4HANA systems using Single Sign–on technology were considered.

In the economic section, the costs for the development and implementation of the technology were determined and an analysis of its economic efficiency was carried out.

The practical value of the results of the qualification work was achieved in ensuring the protection of information in hybrid subsystems based on the SAP Ariba system, which will increase the level of information security and improve the management of access to information.

AUTHORIZATION CONCEPT, SINGLE SIGN–ON TECHNOLOGY, ACCESS CONTROL MODELS, RISK ANALYSIS, CYBER SECURITY, INFORMATION SECURITY MANAGEMENT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ABAC – attribute–based access control;

ACS – assertion consumer service;

API – application programming interface;

DAC – discretionary access control;

ERP – enterprise resource planning;

ERS – evaluated receipt settlement;

FCPA – foreign corrupt practices act;

HTTP – hypertext transfer protocol;

IAS – identity authentication service;

IdP – identity provider;

IPS – identity provisioning service;

MAC – mandatory access control;

P2P – peer–to–peer;

RBAC – role–based access control;

RFC – remote function call;

SAML – security assertion markup language;

SOAP – графічний інструмент, який дозволяє надсилати спеціальні запити на

SP – support package;

SSO – single sign–on;

URL адреси https;

ЗМІСТ

с.

ВСТУП

Через значне збільшення кількості великих компанії та корпорації, потреба в програмному забезпеченні для планування ресурсів підприємства є як ніколи актуальною. Саме тому SAP присвятила себе створенню програмних рішень, призначених для вдосконалення процесів компаній та максимізації її потенціалу. SAP є найпопулярнішим серед ERP через свою значну частку ринку. Його використовують близько 39 668 компаній і 75 000 клієнтів у 120 країнах. SAP може відрізнятися за дизайном і впровадженням, починаючи від локальних, хмарних або гібридних систем. Конкретні функції та процеси, якими керує ERP, залежатимуть від унікальних вимог і операцій в організації. Але, головна особливість та перевага SAP це те що воно взаємодіє з великою кількістю модулів, серед яких: фінансовий облік, управління фінансовим ланцюгом поставок, контролінг, управління матеріалами, збут і дистрибуція, виконання логістики, планування виробництва, людські ресурси тощо. І для коректної роботи всіх модулів і продуктів, що входять до них, важливо не нехтувати безпекою.

Саме тому такий важливий авторизаційний концепт, який допомагає правильно керувати безпекою всередині систем. Концепція авторизації в SAP визначає на фундаментальному рівні правила, відповідно до яких користувачі створюються в системі, а також як призначаються ролі та повноваження. Таким чином, ця концепція гарантує, що транзакції та послуги в системі захищені від несанкціонованого доступу.

Ціль цих правил полягає в тому, щоб завжди призначати користувачам саме ті ролі та повноваження, які їм потрібні для виконання завдань, а в ідеалі – лише ці. Це захищає як від ненавмисних помилок, так і від цілеспрямованого неправильного використання. Завдяки добре структурованій концепції авторизації можливі залежності та конфлікти відповідності також враховуються – їх не потрібно перевіряти вручну під час призначення ролей і повноважень. Добре розроблена концепція авторизації створює ясність щодо обов'язків і процесів. Нові співробітники можуть бути легко інтегровані в систему за

допомогою існуючих правил; якщо існуючі користувачі беруться за нові завдання, для них також існують чіткі правила щодо того, як отримати нові повноваження – і як передати ті, які їм більше не потрібні. Складні авторизації та зв'язки можна описати як об'єкти авторизації.

Тому концепція авторизації економить величезну кількість часу та зусиль і вважається центральним стратегічним компонентом цілісного управління ідентифікацією та доступом.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про SAP та його продукти

SAP (System Analysis Program Development) або системні програми та продукти, – це програмне забезпечення, яке широко використовується для планування ресурсів підприємства ERP (Enterprise Resource Planning). SAP створює централізовану систему для бізнесу, яка дозволяє кожному відділу отримувати доступ до загальних даних та обмінюватися ними, щоб створити найкраще робоче середовище для кожного співробітника компанії [1].

SAP є найбільшим виробником програмного забезпечення для планування корпоративних ресурсів на планеті, і вона домінує в серверних IT–системах компаній зі списку Fortune 500 разом із конкурентами Oracle і Microsoft. Але він також підтримує малі фірми, де приблизно 80 відсотків його клієнтської бази становлять представники малого та середнього бізнесу.

SAP, що базується в Німеччині, але має значну присутність у США та інших країнах, є 12–ю за величиною технологічною компанією у світі та має дохід у 7,51 мільярда євро у 2021 році. SAP настільки популярна серед підприємств, тому що компанії можуть отримати комплексний набір інтегрованих міжфункціональних процесів роботи з ним. SAP регулярно досліджує ринкові тенденції та потреби бізнес–підрозділів. Відповідно до попиту, він запускає свої оновлені версії продуктів з найновішими функціями. Тому глобальні компанії будь–якого розміру обирають SAP для свого бізнесу.

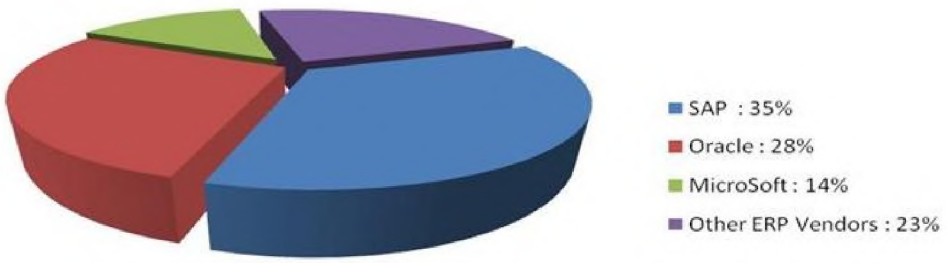

Рисунок 1.1 – Доля використання SAP порівняно з іншими компаніями

Компанія SAP має близько 60 різних продуктів та рішень для різноманітних модулів і ось деякі з них, які будуть проаналізовані та використані для цієї роботи:

1. SAP Ariba:

Платформа для співробітництва у сфері закупівель та поставок. Він об'єднує покупців та постачальників та пропонує рішення для пошуку, закупівель та управління постачальниками.

2. SAP S/4HANA:

Пакет планування ресурсів підприємства (ERP), побудований на базі даних SAP HANA, що зберігається у пам'яті. Він підтримує бізнес–процеси в різних галузях і включає модулі для фінансів, управління ланцюжками поставок, виробництва та багато іншого.

3. SAP HANA:

База даних у пам'яті та аналітична платформа, яка забезпечує обробку та аналіз даних у реальному часі.

4. SAP Cloud Platform:

Платформа як послуга (PaaS), яка дозволяє підприємствам розробляти, інтегрувати та розширювати додатки у хмарі.

1.2 Відомості про SAP Ariba

SAP Ariba – це інтелектуальне хмарне програмне забезпечення для керування постачанням та закупівлями. Воно дозволяє компаніям підвищити ефективність та контролювати витрати за рахунок оптимізації процесу “від закупівель до оплати» (P2P) [2].

SAP Ariba охоплює комплексний процес від джерела до оплати, включаючи стратегічний пошук постачальників, управління постачальниками, закупівлі, оптимізацію оборотного капіталу, управління рахунками та прозорість витрат. Рішення SAP дозволяє покупцям та постачальникам вести бізнес на єдиній платформі, організовуючи та уніфікуючи свою стратегію ланцюжка поставок. Використовуючи програмне забезпечення та пакет рішень для закупівель SAP Ariba, організація може:

– зменшити неефективність завдяки детальній візуалізації робочих процесів;

– керувати відносинами з постачальниками ефективніше;

– використовувати автоматизацію для полегшення рутинних завдань, таких як виставлення рахунків або процес розрахунку кредиторської заборгованості;

– об'єднати процеси керування постачальниками, постачальниками, закупівлями та ланцюжками постачання.

SAP Ariba корисний для середніх та великих організацій зі складними системами закупівель та постачання. Його можна використовувати як автономну платформу, як частину основного програмного забезпечення SAP S/4HANA компанії або в тандемі з користувальницьким масивом інших модулів планування ресурсів підприємства (ERP) SAP, таких як SAP Fieldglass для послуг та зовнішньої праці та SAP Concur для управління витратами та поїздками.

1.3 Контроль доступу: моделі та методи

Для подальшого аналізу авторизаційних концептів систем SAP Ariba та SAP S/4HANA є потреба розглянути моделі контролю доступу, особливо ті що використовують подані системи:

1. Модель обов'язкового контролю доступу, або MAC(Mandatory Access Control), надає керування контролем доступу лише власнику та зберігачу. Це означає, що кінцевий користувач не може контролювати будь–які параметри, які надають будь–кому будь–які привілеї. Зараз існує дві моделі безпеки, пов'язані з MAC: Biba та Bell–LaPadula. Модель Біба зосереджена на цілісності інформації, тоді як модель Белла–ЛаПадули зосереджена на конфіденційності інформації. Biba – це налаштування, за якого користувач із низьким рівнем доступу може читати інформацію вищого рівня (так званий "зчитування»), а користувач із високим рівнем доступу може писати для нижчого рівня доступу (так званий "запис»). Модель Biba зазвичай використовується в компаніях, де співробітники

нижчого рівня можуть читати інформацію вищого рівня, а керівники можуть писати, щоб повідомити співробітників нижчого рівня.

2. Модель дискреційного контролю доступу, або DAC(Discretionary Access Control), є найменш обмежувальною моделлю порівняно з найбільш обмежувальною моделлю MAC. DAC дозволяє окремим особам повністю контролювати будь–які об'єкти, якими вони володіють, а також програми, пов'язані з цими об'єктами. Це дає DAC дві основні слабкості. По–перше, це дає кінцевому користувачеві повний контроль для встановлення налаштувань рівня безпеки для інших користувачів, що може призвести до того, що користувачі матимуть вищі привілеї, ніж вони повинні. По–друге, що ще гірше, дозволи, які має кінцевий користувач, успадковуються в інших програмах, які він виконує. Це означає, що кінцевий користувач може запускати зловмисне програмне забезпечення, не підозрюючи про це, і зловмисне програмне забезпечення може скористатися привілеями потенційно високого рівня, якими володіє кінцевий користувач.

3. Модель управління доступом з урахуванням ролей, чи RBAC(Role–based access control), забезпечує контроль доступу з урахуванням посади, яку людина обіймає у організації. Таким чином, замість того, щоб призначати користувачу дозволи як менеджер безпеки, посада менеджера безпеки вже має призначені їй дозволи. Насправді, користувачу просто знадобиться доступ до профілю менеджера безпеки. RBAC полегшує життя системного адміністратора організації. Велика проблема з цією моделлю управління доступом полягає в тому, що якщо користувачу потрібен доступ до інших файлів, повинен бути інший спосіб зробити це, оскільки ролі пов'язані лише з позицією; в іншому випадку менеджери безпеки з інших організацій можуть отримати доступ до файлів, до яких вони не мають повноважень.

4. Контроль доступу на основі атрибутів (ABAC– Attribute–Based Access Control), також відомий як контроль доступу на основі політики або контроль доступу на основі вимог, – це методологія авторизації, яка встановлює та забезпечує виконання політик на основі таких характеристик, як відділ,

місцезнаходження, менеджер, і час доби. Використовуючи булеву логіку, ABAC створює правила доступу з операторами if–then, які визначають користувача, запит, ресурс і дію. Наприклад, якщо запитувач є продавцем, йому надається доступ для читання та запису до рішення для керування взаємовідносинами з клієнтами, на відміну від адміністратора, який має права перегляду лише для створення звіту.

1.4 Авторизаційний концепт SAP Ariba

SAP Ariba використовує контроль доступу на основі атрибутів (ABAC), щоб забезпечити динамічний і гнучкий підхід до керування доступом, підвищуючи безпеку, враховуючи різні атрибути, пов'язані з користувачами, ресурсами та середовищем.

Рисунок 1.2 – Схема моделі контролю доступу в системі SAP Ariba

Для забезпечення достатнього рівня безпеки інформації під час роботи в системі Ariba, SAP розробили наступний алгоритм процесу роботи:

1. "Спостерігачі» інформуються про запит, але не схвалюють та не відхиляють документ.

2. “Затверджуючі особи» повинні схвалити чи відхилити документ. Якщо будь–який затверджуючий документ відхиляє, відхиляється весь документ.

3. “Послідовна маршрутизація» надсилає документ першому затверджуючому і чекає на його затвердження перед відправкою другому.

4. Затвердження гілок “паралельної маршрутизації» з відправкою його декільком стверджуючим одночасно.

5. “Групи» можуть бути стверджуючими. Групи надають користувачам доступ до функцій у рішеннях SAP Ariba Strategic Sourcing і Supplier Management і SAP Ariba Procurement. Членство в групах дозволяє користувачам виконувати певні дії в інтерфейсах кінцевого користувача та адміністратора Ariba. Наприклад, лише члени групи Customer Administrator можуть використовувати Ariba Administrator для імпорту, експорту та керування всіма типами даних.SAP Ariba включає низку стандартних або визначених системою груп. Також можна додавати унікальні групи.

6. “Користувачів» можна додавати до потоку затвердження, щоб затверджувати як окремі особи.

Рисунок 1.3 – Схема процесу роботи у системі SAP Ariba

Згідно з цією схемою одну з важливих ролей відіграють відносини Користувач–Група. Група може містити багато користувачів. Наприклад, агент із закупівель містить трьох різних користувачів: Користувач 1, Користувач 2, Користувач 3.

Користувача можна віднести до багатьох груп. У цьому прикладі Користувач 2 належить до груп, показаних на слайді вище. Агент із закупівель,

Менеджер з контрактів та Адміністратор звітів є системними групами. Штаб–квартира – це спеціально створена група, яка допомагає організувати Кірка та ідентифікувати його як користувача у штаб–квартирі організації.

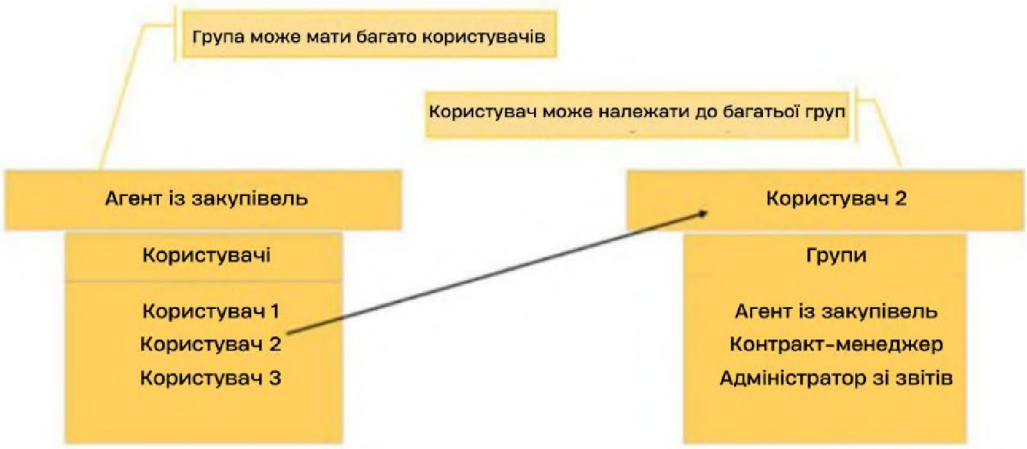

Рисунок 1.4 – Схема відносин між користувачем та групою

Групи можуть бути двох видів –Батьківські та Дочірні. У цьому прикладі керована група Ariba “Лондонські аналітики” є дочірньою системною групою “Старший аналітик”. Крім того, група під управлінням Ariba “Аналітики Бостона” є дочірньою групою американських аналітиків під управлінням Ariba.

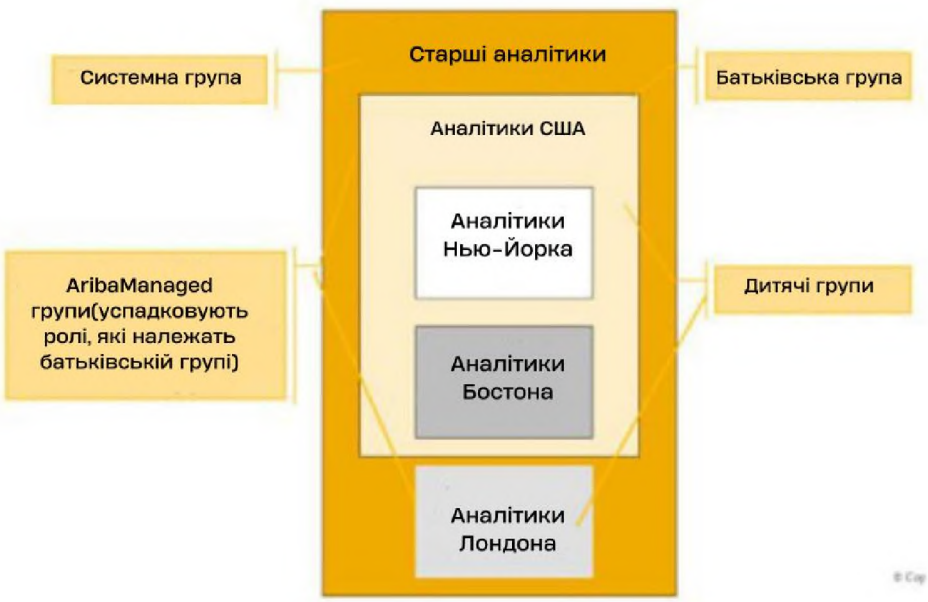

Рисунок 1.5 – Приклад батьківських та дочірніх груп

Загалом, групи надають користувачам доступ до функцій хмарних рішень SAP Ariba. Кожна група має опис групи, де перераховані функціональні можливості, доступні членам цієї групи. Описи груп надають список дій, які можуть виконувати члени групи.

1.5 Авторизаційний концепт SAP S/4HANA

SAP S/4HANA в основному використовує рольовий контроль доступу (RBAC) як основну систему контролю доступу, хоча він також підтримує елементи контролю доступу на основі атрибутів (ABAC) для підвищення гнучкості та безпеки.

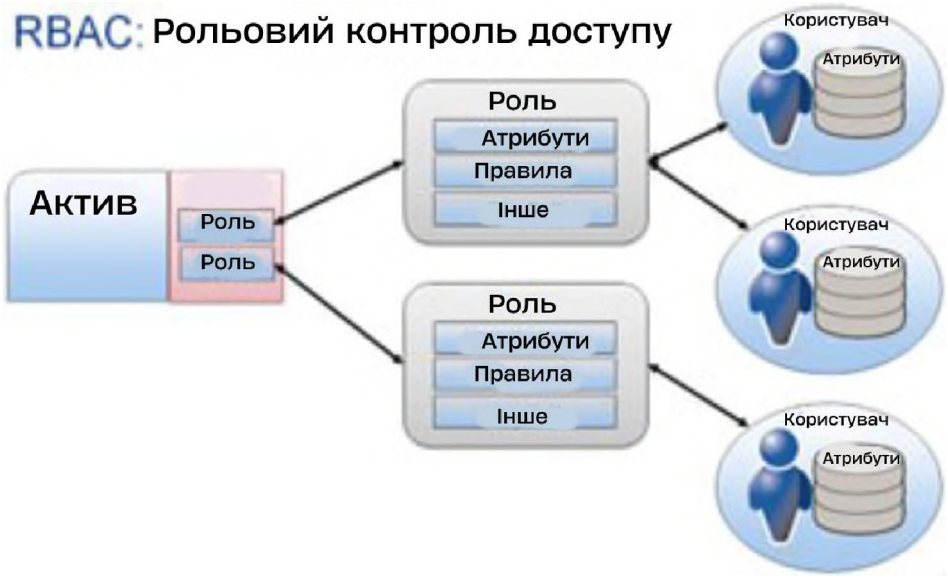

Рисунок 1.6 – Схема моделі контролю доступу в системі SAP S/4HANA

Авторизаційний концепт SAP S/4HANA містить наступні компоненти:

1. Об’єкти авторизації

Об’єкти авторизації дозволяють комплексні перевірки, які включають кілька умов. Умови дозволяють користувачеві виконати дію. Умови вказані в полях авторизації для об’єктів авторизації та пов’язані і для перевірки. Авторизація завжди пов’язана лише з одним об’єктом авторизації та містить значення для полів для цього об’єкта авторизації. Авторизація – це дозвіл на виконання певної дії в системі SAP. Дія визначається на основі значень для окремих полів об’єкта авторизації. Наприклад, авторизація B на малюнку для

об’єкта авторизації S_USER_GRP дозволяє відображати всі основні записи користувачів, які не призначені групі користувачів SUPER. Проте авторизація 1 дозволяє відображати записи для цієї групи користувачів.

Для одного об’єкта може бути декілька авторизацій. SAP надає деякі авторизації, але більшість авторизацій створюється спеціально для вимог клієнта.

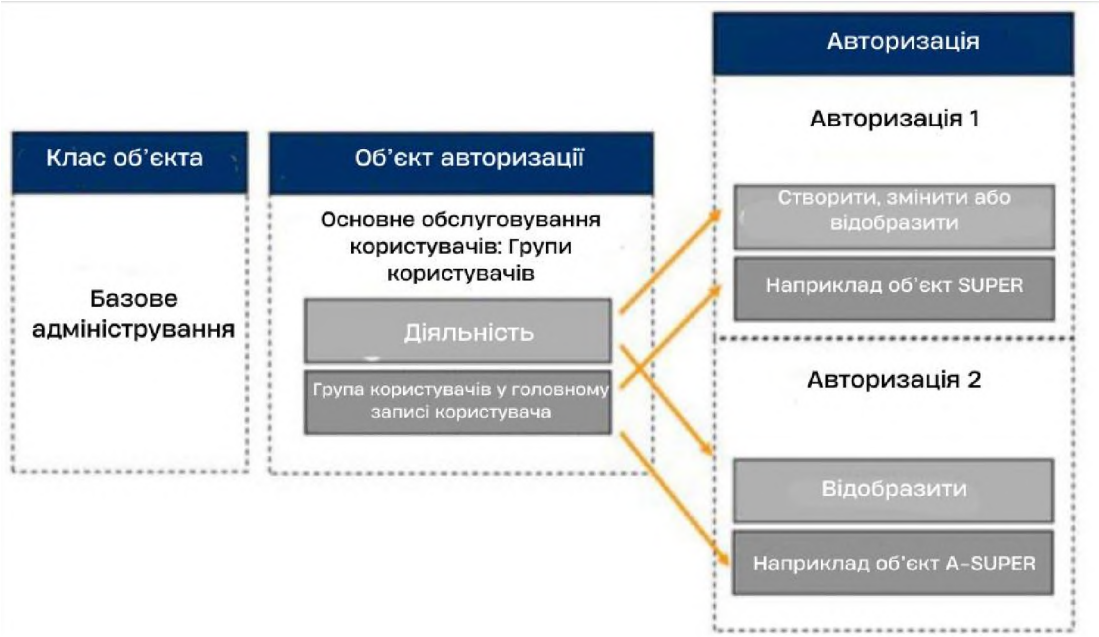

Рисунок 1.7 – Приклад зв’язку між об’єктом авторизації та дозволеними діями

2. Перевірка авторизації

Коли користувач входить до клієнта системи SAP, його або її повноваження завантажуються в контекст користувача. Контекст користувача знаходиться в буфері користувача сервера додатків.

Коли користувач викликає транзакцію, система перевіряє, чи має користувач авторизацію в контексті користувача, яка дозволяє йому або їй викликати вибрану транзакцію. Перевірка авторизації використовує авторизацію в контексті користувача.

Якщо користувачеві призначаються нові повноваження, йому може знадобитися знову ввійти в систему SAP, щоб мати можливість використовувати ці нові повноваження.

Якщо перевірка авторизації для виклику транзакції пройшла успішно, система відображає початковий екран транзакції. Залежно від транзакції користувач може створювати дані або вибирати дії. Коли користувач завершує свій діалоговий крок, дані надсилаються до диспетчера, який передає їх робочому процесу діалогу для обробки.

Якщо контекст користувача містить усі необхідні авторизації для перевірок, дані та дії обробляються, і відображається наступний екран. Навіть якщо одного авторизації немає, дані та дії не обробляються, і користувач отримує повідомлення про те, що його або її авторизації недостатньо. Значення коду повернення контролює цей крок. У цьому випадку значення коду повернення не дорівнює 0.

Усі авторизації є дозволами. Немає дозволів на заборону. Заборонено все, що прямо не дозволено. Це можна назвати концепцією позитивної авторизації.

Рисунок 1.8 – Алгоритм перевірки авторизації у системі

3. Комбіновані ролі(функціональні ролі)

Комбіновані ролі складаються з окремих ролей. Користувачам, яким призначено складну роль, під час порівняння автоматично призначаються

відповідні окремі ролі. Складені ролі самі по собі не містять даних авторизації. Налаштування складених ролей корисно, наприклад, якщо декому з співробітників потрібен дозвіл на кілька ролей. Є можливість створити складену роль і призначити її користувачам замість того, щоб поміщати кожного користувача в кожну необхідну окрему роль.

4. Індивідуальна роль

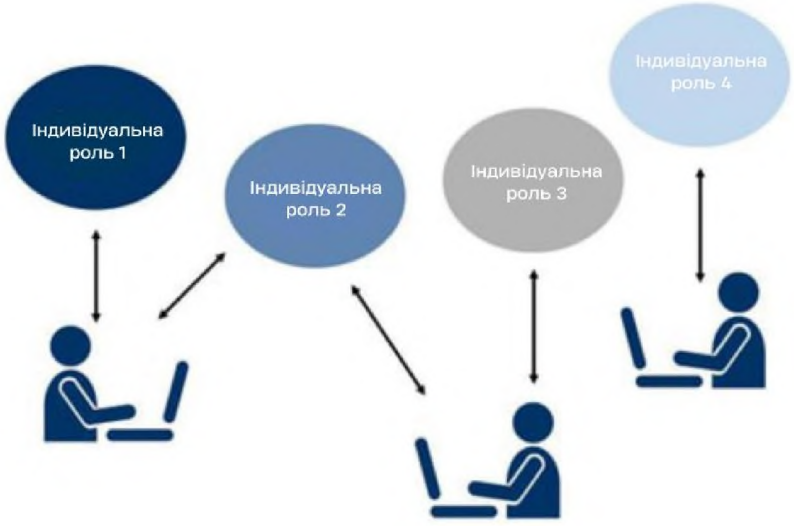

Рисунок 1.9 – Приклад зв'язку користувачів та індивідуальних ролей

Індивідуальна роль – це контейнер даних для групи кодів транзакцій. Користувачам SAP призначаються окремі ролі, щоб вони могли виконувати коди транзакцій. Різні підходи до призначення доступу називають методологією ролей.

5. Обслуговування ролі

Обслуговування ролей спрощує створення авторизацій та їх призначення користувачам. При обслуговуванні ролі вибираються транзакції, які належать до точки зору компанії. Обслуговування ролі створює авторизації з обов'язковими значеннями полів для об'єктів авторизації, які перевіряються у вибраних транзакціях. Роль можна призначати різним користувачам. Таким чином, зміни в

ролі впливають на кількох користувачів. Користувачам можна призначати різні ролі.

6. Профілі

Профілі – це набори об'єктів авторизації, які визначають певні дозволи. Вони пов'язані з ролями та надають користувачам необхідні дозволи для виконання своїх завдань.

1.6 Опис взаємодії SAP Ariba з іншими системами та проблематика

Якщо розглядати авторизаційний концепт Ariba окремо, то він не представляє проблем як самостійний продукт, але оскільки всі продукти SAP в більшості випадків використовуються в поєднанні з іншими продуктами, Ariba помітно програє. У першу чергу через те, як було сказано вище, має систему контролю доступом на базі атрибутів на відміну від інших рішень SAP, які мають часто рольову модель доступу або гібридну. Також, оскільки Ariba спочатку розроблялася окремо від SAP сторонньою компанією, система має іншу структуру і вид авторизаційного концепту, що відрізняється від решти лінійки компанії. Відповідно до вищепереліченних причин, Ariba має деякі слабкі сторони при використанні з іншими системами:

1. Неузгоджені ідентифікатори користувачів. Деякі ідентифікатори користувачів, визначені в системі, яка відрізняється від SAP, не були визначені відповідно до вимог унікального ідентифікатора користувача підприємства або не були засновані на активному каталозі. Це призводить до того, що деякі ідентифікатори користувачів не розпізнаються на етапі завантаження та призводять до помилок завантаження даних.

2. Неправильні записи під час перетворення даних. Етап перетворення даних виконується вручну та призводить до появи деяких неправильних записів у файлах завантаження даних.

3. Недокументовані вимоги до конфігурації. Деякі вимоги до конфігурації, особливо для налаштування групи з'єднувачів для систем, які відрізняються від SAP, вимагають, щоб тип з'єднання залишався порожнім [6].

1.7 Висновок до першої частини

У даному розділі були наведені загальні відомості про систему SAP та її продукти. Окремо були визначені загальні відомості які відносяться до системи SAP Ariba. Був наведений детальний опис моделей контролю доступу та які з них використовуються у продуктах компанії. Проаналізовано авторизаційні концепти систем SAP Ariba та S/4HANA та наведено детальний опис алгоритму роботи двох концептів. Проаналізовано та визначено єфект від взаємодії двох систем та поточну проблематику.

Все це дає фундамент для визначення ризиків від використання гібридних систем без належного алгоритму взаємодії між користувачами, компонетами та ін. А також дає можливість запропонувати та впровадити підходящу технологію, яка зможе дати належний доступ до вільної взаємодії двох систем у питанні безпеки та доступу до тої чи іншої інформації.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз ризиків в роботі SAP Ariba з іншими системами

В ході аналізу системи, через недосконаліть авторизаційного концепту SAP Ariba при роботі з іншими системами (S/4HANA в даному випадку), були виявленні наступні ризики:

1. Користувач створює основний запис фіктивного постачальника, а після створення постачальника обробляє рахунок постачальника для цього фіктивного постачальника.

За допомогою цього конфлікту користувач може обійти належні процеси керування Procure to Pay/Master Data і випадково чи зловмисно виконати такі дії:

Виконання невідповідних дій (тобто підтримка фіктивного постачальника та ввід рахунок–фактуру, який буде включено до автоматичного циклу платежів), що може призвести до ризиків: привласнення вихідних платежів, невідповідності стратегії випуску платежів постачальника та несанкціонованого введення та розміщення документів, що може поставити під загрозу цілісність обробки, точність даних і збільшити ймовірність шахрайства та помилок.

2. Користувач може створити платіжний документ (тобто рахунок–фактуру), а після обробки створити несанкціонований документ (тобто кредитове авізо) для компенсації рахунку–фактури. Той самий користувач може змінити умову ціни для певного клієнта/продукту, щоб неналежним чином надати клієнту більш вигідну ціну.

За допомогою цього конфлікту користувач може обійти належні процедури “Замовлення в готівку» та випадково чи зловмисно вчинити такі дії, як: Ризик зміни ціни продажу для виставлення рахунків–фактур. У результаті користувач може обійти елементи керування, щоб неналежним чином змінити платіжні документи (тобто рахунок–фактуру) і умови цін, що може призвести до сприятливого ціноутворення та коригування дебіторської заборгованості для клієнтів.

3. Перекриття відбувається, коли працівник краде готівку, відволікаючи платіж від одного клієнта, а потім приховує крадіжку, перенаправляючи готівку від іншого клієнта, щоб компенсувати дебіторську заборгованість від першого клієнта. Цей користувач, який може перенаправляти вхідні платежі, а також вести основні записи клієнтів, створює потенціал для шахрайства. Цей тип шахрайства може здійснюватися безперервно, оскільки нові платежі постійно використовуються для оплати старих боргів, тому жодна дебіторська заборгованість, пов'язана з шахрайством, ніколи не здається такою старою. Лепінг найлегше виконувати, коли працівник бере участь у всіх завданнях з обробки готівки та реєстрації (у цьому прикладі він може обробляти вхідні платежі та вести основні записи клієнтів).

За допомогою цього конфлікту користувач може обійти належні процедури замовлення готівки/вхідних платежів/керування основними даними та випадково чи зловмисно виконати такі дії:

Створення фіктивного основний запис клієнта, обробка фіктивного

замовлення клієнта, а потім перенаправлення вхідніх платежів на банківський рахунок, який було зареєстровано в основному записі клієнта.

4. Перекриття відбувається, коли працівник краде готівку, відволікаючи платіж від одного клієнта, а потім приховує крадіжку, перенаправляючи готівку від іншого клієнта, щоб компенсувати дебіторську заборгованість від першого клієнта. Цей користувач, який може перенаправляти вхідні платежі, а також вести основні записи клієнтів, створює потенціал для шахрайства. Цей тип шахрайства може здійснюватися безперервно, оскільки нові платежі постійно використовуються для оплати старих боргів, тому жодна дебіторська заборгованість, пов'язана з шахрайством, ніколи не здається такою старою. Лепінг найлегше виконувати, коли працівник бере участь у всіх завданнях з обробки готівки та реєстрації (у цьому прикладі він може обробляти вхідні платежі та вести основні записи клієнтів). Крім того, користувач може створити фіктивний основний запис клієнта та створити угоду купівлі–продажу, згідно з якою умови та продукти є дійсними для всіх контрактів або замовлень на продаж,

які клієнт створює з посиланням на угоду купівлі–продажу. Це аналогічно загальному замовленню на купівлю, створеному в процесі закупівлі для оплати. Користувач може обробити цю загальну угоду про продаж і визначити угоду без кінцевої дати/періоду дії, що призведе до незавершеного контракту з фіктивним клієнтом і можливості перенаправляти вхідні платежі клієнта цьому фіктивному клієнту.

За допомогою цього конфлікту користувач може обійти належні процедури замовлення готівки/вхідних платежів/керування основними даними та випадково чи зловмисно виконати такі дії:

Створення фіктивного основного запису клієнта, обробка фіктивної угоди купівлі–продажу, а потім перенаправлення вхідних платежів на банківський рахунок, який було записано в основному записі клієнта.

5. Платежі державним службовцям/посадовцям впливають на багато компаній, що призводить до дотримання вимог FCPA та належної обачності навколо головного постачальника та забезпечення обробки платежів. Користувач може створити фіктивного постачальника, створити замовлення на купівлю, вступити в змову зі співробітником, щоб неналежним чином опублікувати вхідний товарний чек, а також незаконно привласнити запаси для особистого використання/вигоди.

За допомогою цього конфлікту користувач може обійти належне керування основними даними та обробку Procure to Pay і випадково чи зловмисно зробити такі дії:

Створити фіктивного постачальника та ініціювання покупки в цього постачальника. Як наслідок, користувач може обійти елементи керування, щоб неналежним чином обробити покупки, що може призвести до крадіжки активів і недотримання політики постачальника/закупівлі.

6. Користувач створює фіктивне замовлення на купівлю, і після змови з колегою оприлюднення товарного чека призводить до відхилення (тобто кількості на замовлення на поставку до отриманої кількості). Оприлюднення товарного чека занижує фактичну вхідну кількість товарів, і користувач може

виправдати блокування рахунку–фактури через відхилення в SAP. Тепер користувач може зняти блокування вручну через розбіжності та покрити незаконне привласнення товарів.

За допомогою цього конфлікту користувач може обійти належну обробку Procure to Pay і випадково чи зловмисно виконати такі дії:

Управління фіктивним замовленням на купівлю та виконання розблокування вручну, щоб приховати відхилення в кількості замовлення на купівлю та отриманій кількості. Як наслідок, користувач може обійти елементи керування, щоб неналежним чином обробляти функції закупівель і виставлення рахунків, що може призвести до крадіжки вхідних товарів і недотримання політики закупівель.

7. Створення фіктивний матеріал у головному записі(master data), а після додавання основного запису маніпулювання загальною угодою купівлі–продажу, включивши цей матеріал до угоди купівлі, яку підтримує/створює користувач.

Конфіденційний доступ: доступ до ведення основних записів матеріалів повинен бути обмежений уповноваженим персоналом. Основні записи матеріалів можуть бути обмежені кодом компанії, щоб зменшити ризик створення неавторизованими користувачами фіктивних даних про матеріал. Користувачі, які зберігають основні дані, не повинні мати можливість обробляти транзакції в рамках процесу Procure to Pay. Крім того, створення загальних замовлень на закупівлю має бути строго обмежено уповноваженим персоналом, оскільки вони використовуються для розрахунків за оціненими квитанціями (ERS), що усуває потребу в рахунку–фактурі, дозволяючи покупцеві авторизувати постачальника платіж після підтвердження надходження товару (тобто усуває потребу в тристоронньому збігу, який вимагає зіставлення замовлення на купівлю зі звітом про отримання та рахунком–фактурою).

За допомогою цього конфлікту користувач може обійти належні процеси Procure to Pay і випадково чи зловмисно зробити такі дії, як:

Додати товар до основного файлу матеріалу або основного файлу послуги, а потім шахрайським шляхом додати ці елементи до угод про купівлю. У

результаті користувач може обійти засоби контролю, щоб неналежним чином вести основні записи про матеріали та маніпулювати процесом угоди про закупівлю, щоб приховати крадіжку активів і потенційну змову з постачальником.

Більшість ризиків виникає через роздрібленість систем у питаннях контролю авторизації та автентифікації, а саме за відсутності технології Єдиного входу яка об'єднує права користувача у двох системах завдяки чому надає правильний доступ до читання та змінення інформації.

2.2 Загальний алгоритм налаштування Єдиного входу до SAP Ariba

Для подальшого вирішення актуальних проблем та зниження ризиків почнемо конфігурацію рішення "Єдиного входу» або Single sign–on. Єдиний вхід (SSO) – це процес автентифікації та авторизації, який дозволяє користувачеві отримувати доступ до кількох корпоративних програм за допомогою одного набору облікових даних (ім'я користувача та пароль). Постачальник послуг (SP) розміщує послугу (наприклад, SAP Ariba Buying), до якої користувач хоче отримати доступ. Цей постачальник послуг (SP) довіряє постачальнику ідентифікаційних даних (IdP) (наприклад, SAP IAS або Microsoft Entra ID), який контролює доступ користувача. SSO підтримує різноманітні протоколи, як–от Security Assertion Markup Language (SAML) або OpenID Connect [8].

Попередні умови:

- в обліковому записі sap cloud identity services –identity authentication мають бути як тестові, так і тенанти організації. організація повинна виконати кроки налаштування "аутентифікація особи» , а адміністратор повинен мати там ролі, що дозволяють керувати конфігураціями клієнтів і користувачами;
- на сайті sap ariba мають бути створені користувачі;
- щоб увімкнути єдиний вхід до sap ariba за допомогою saml 2.0, повинен бути користувач із типом стороннього корпоративного користувача (ariba) та членом групи адміністраторів клієнтів.

Єдиний вхід до автентифікації особистості SAP Ariba необхідний для включення інформації про профіль постачальника на панелі керування постачальниками на сайті SAP Ariba . Він також контролює керування постачальниками SAP Ariba під керуванням SAP – видимість додатків SAP S4/HANA та ролі робочих процесів за допомогою призначення групи автентифікації особистості.

2.2.1 Рекомендації та вимоги до налаштування

У рамках конфігурації Єдиного входу між сайтом SAP Ariba та SAP Cloud Identity Services – Identity Authentication повинні підтримуватися паралельні об'єкти користувачів в обох розташуваннях.

Доступ внутрішніх користувачів до сайту SAP Ariba, далі Керування постачальниками SAP Ariba, далі Платформа бізнес–технологій SAP . Програми, керовані SAP, такі як зведення профілю постачальника та пошук та спільна робота по подіях, за допомогою Єдиного входу через автентифікацію особи . Для ввімкнення функцій, які використовують ці програми, потрібне налаштування Єдиного входу.

Для Єдиного входу потрібен кожен внутрішній користувач (користувач типу Enterprise User з Адаптер Пароля1) у SAP Ariba , щоб мати відповідного користувача в SAP Cloud Identity Services – Identity Authentication. При створенні цих паралельних об'єктів користувача є наступні вимоги і міркування:

1. Ім'я входу для кожного користувача в автентичності має точно збігатися з його ім'ям користувача (Унікальне ім'я) на сайті SAP Ariba . При Єдиному вході як ідентифікатор користувача використовується значення ідентифікатора імені суб'єкта в перевірці автентичності особи, яке має збігатися з ім'ям суб'єкта. Унікальне ім'я SAP Ariba.

2. Для автентифікації особи потрібна унікальна адреса електронної пошти для кожного користувача, чого немає на сайті SAP Ariba.

3. Аутентифікація особи також вимагає, щоб кожне ім'я входу було унікальним для всіх типів користувачів. Для сайту SAP Ariba потрібне лише

унікальне ім'я користувача для кожного типу користувача (покупець, постачальник або третя особа).

4. Якщо планується завантажити дані користувача з сайту SAP Ariba як основу для створення нових користувачів у Identity Authentication, обов'язково вносяться усі необхідні виправлення, щоб дані відповідали вимогам Identity Authentication.

В даний час для пошуку та спільної роботи над подіями зовнішні користувачі (контакти постачальника) та сторонні користувачі доступні в результатах із записів постачальників SAP Ariba про ризики постачальників і можуть бути додані до групи аналізу. Вони використовують посилання в повідомленнях електронною поштою про результати, куди вони додаються, для створення облікових записів автентифікації та доступу до цих результатів.

В організаціях, де налаштовано Єдиний вхід (SSO) з корпоративною автентифікацією, користувач може увійти в систему з одним ім'ям користувача та паролем для доступу до кількох програм, включаючи рішення SAP Ariba Procurement та рішення SAP Ariba для стратегічного постачання.

Системи SSO зберігають облікові дані користувачів для кількох програм і автоматично передають ці облікові дані від імені користувачів, коли це необхідно. Користувачі входять до системи один раз, а не повторно, використовуючи окремий набір облікових даних для кожної програми, до якої вони звертаються. Єдиний вхід із корпоративною автентифікацією також може забезпечити централізований контроль та дотримання політик корпоративної автентифікації. Щоб використовувати Єдиний вхід з корпоративною автентифікацією, адміністратор мережі повинен увімкнути зв'язок між системою автентифікації користувачів і рішенням SAP Ariba .

2.3 Початковий етап конфігурації Єдиного входу

Перш за все підключимо технологію Постачальника ідентифікаційної інформації, яка є у складі технології Єдиного входу.

2.3.1 Постачальник ідентифікаційної інформації (IdP)

Вимоги до системи, що відповідає за аутентифікацію користувача:

– унікально ідентифікує користувача;

– містить сховище користувачів із додатковими атрибутами користувача (ім'я, пошта, членство в групі, ...);

– містить облікові дані користувача (ім'я користувача/пароль);

– видає додаткові атрибути користувача (ім'я, пошта, членство в групі,..);

– довіряє одному або декільком постачальникам послуг (SP);

– постачальник послуг (SP).

Система делегує автентифікацію користувача постачальнику ідентифікаційної інформації (IdP) на наступних принципах:

– покладається на ідентифікатор користувача та атрибути користувача від постачальника ідентифікаційної інформації (IdP);

– довіряє єдиному постачальнику ідентифікаційної інформації (IdP).

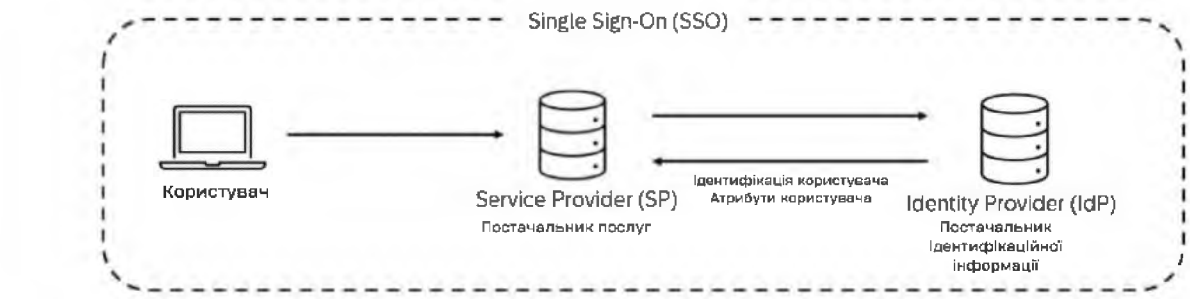

Рисунок 2.1 – Зв'язок користувача з постачальником послуг та постачальником ідентифікаційної інформації

SAP Cloud Identity Services – це продукт SAP для автентифікації та Єдиного входу (SSO) у хмарі, який також називається SAP IAS (Identity Authentication Service). Для відповідності найновішим рішенням SAP Ariba "Next Generation» обов'язковим є Єдиний вхід рішень SAP Ariba (SSO) за допомогою SAP IAS (Test або Production). SAP IAS можна налаштувати як постачальника ідентифікаційної інформації (IdP), щоб він слугував проксі–сервером постачальника ідентифікаційної інформації (IdP Proxy) для іншого

постачальникаідентифікаційна інформація керується клієнтом (наприклад, ідентифікаційна інформація Microsoft Entra ID). У цьому сценарії автентифікації передбачається збереження сховища користувачів і облікових даних користувача в постачальнику ідентифікаційної інформації (IdP) – SAP IAS. Таким чином, інформація про користувача має бути доступною, активованою, із згенерованими обліковими даними в Identity Provider (IdP) – SAP IAS.

Для належного створення умов для впровадження Єдиного входу (SSO):

– метадані потрібно отримати від постачальника послуг (SP) – SAP Ariba;

– програму, яка представляє постачальника послуг (SP) – SAP Ariba, потрібно створити в Identity Provider (IdP) – SAP IAS, використовуючи метадані, отримані від постачальника послуг (SP) – SAP Ariba;

– метадані потрібно отримати від постачальника ідентифікаційної інформації (IdP) – SAP IAS;

– SSO потрібно налаштувати в постачальника послуг (SP) – SAP Ariba за допомогою метаданих, отриманих від постачальника ідентифікаційної інформації (IdP) – SAP IAS.

Якщо виконання Єдиного входу(SSO) ініційовано IdP:

– користувач отримує доступ до постачальника послуг (SP) – SAP Ariba URL;

– постачальник послуг (SP) – SAP Ariba перешле автентифікацію постачальнику ідентифікаційних даних (IdP) – SAP IAS;

– Identity Provider (IdP) – відображається вікно входу SAP IAS із запитом облікових даних користувача;

– користувача автентифікує постачальник ідентифікаційних даних (IdP) SAP IAS на основі введених облікових даних, а відповідь із ідентифікатором користувача та атрибутами користувача надсилається постачальнику послуг (SP) SAP Ariba.

2.3.2 Ідентифікаційне об'єднання з проксі–сервером постачальника ідентифікаційної інформації (проксі–сервер IdP)

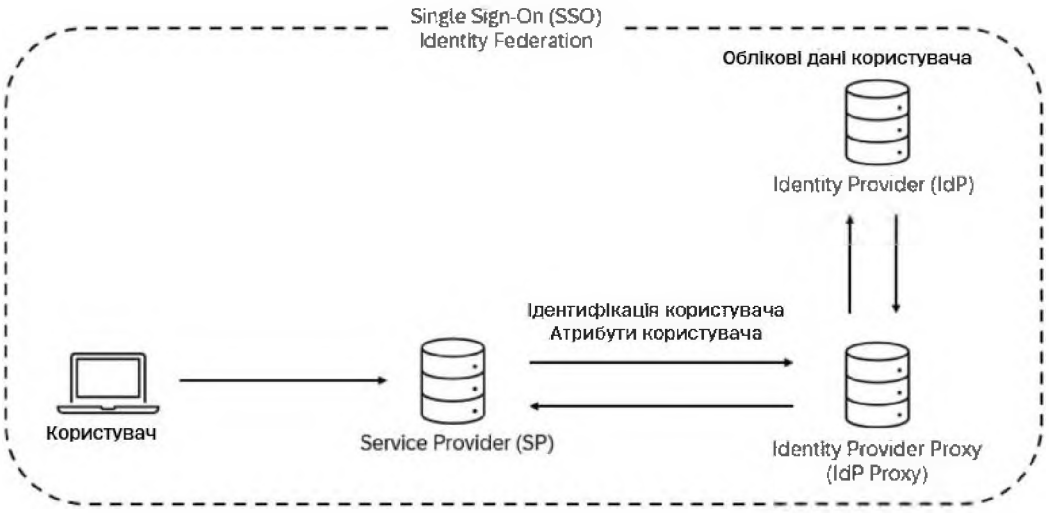

Рисунок 2.2 – Зв'язок між користувачем з постачальником послуг, постачальником ідентифікаційної інформації та проксі

Налаштування проксі–серверу постачальника ідентифікаційної інформації може включати наступне:

– система, відповідальна за автентифікацію користувача, з умовною асоціацією ідентифікації з постачальником ідентифікаційної інформації (IdP);

– унікально ідентифікує користувача або делегує його постачальнику ідентифікаційної інформації (IdP);

– може містити сховище користувачів і додаткові атрибути користувача або делегувати їх постачальнику ідентифікаційної інформації (IdP);

– може містити облікові дані користувача або делегувати їх постачальнику ідентифікаційної інформації (IdP);

– видає додаткові атрибути користувача (ім'я, пошта, членство в групі тощо) або делегує їх постачальнику ідентифікаційної інформації (IdP);

– довіряє одному або декільком постачальникам послуг (SP);

– можна довіряти одному чи кільком постачальникам ідентифікаційної інформації (IdP).

SAP IAS має бути налаштовано як постачальника ідентифікаційної інформації (IdP) також у випадку сценарію автентифікації об'єднання ідентифікаційної інформації, оскільки федерація ідентифікаційної інформації як проксі–сервер постачальника ідентифікаційної інформації (проксі–сервер ідентифікаційної інформації) є конфігурацією розширення самого постачальника ідентифікаційної інформації (IdP).

У цьому сценарії автентифікації передбачається, що збереження облікових даних користувача знаходиться за межами SAP IAS у ідентифікаторі, керованому клієнтом (наприклад, ідентифікатор ідентифікатора Microsoft Entra ID). Сховище користувачів (що містить атрибути користувача) може бути в SAP IAS або за межами SAP IAS у ідентифікаторі, керованому клієнтом (наприклад, ідентифікатор ідентифікатора Microsoft Entra ID). Облікові дані користувача не потрібно підтримувати в SAP IAS, оскільки автентифікація пересилається за межі SAP IAS у керованому клієнтом IdP (наприклад, Microsoft Entra ID IdP).

Якщо в SAP IAS потрібне сховище користувачів (наприклад, для SAP Ariba SAP Task Center або обмеження доступу до групи SAP IAS), користувачів потрібно імпортувати в SAP IAS. Одним із можливих способів є використання автоматизованого рішення через Identity Provisioning (SAP IPS – SAP Identity Provisioning Service).

Щоб встановити SSO за допомогою проксі–сервера постачальника ідентифікаційної інформації (проксі–сервера IdP) потрібно:

– виконати кроки вище Постачальник ідентифікаційної інформації (IdP) "Сценарій автентифікації», щоб налаштувати систему Єдиного входу між постачальником послуг (SP) – SAP Ariba та проксі–сервером постачальника ідентифікаційної інформації (проксі–сервер IdP) – SAP IAS;

– метадані потрібно отримати від проксі–сервера постачальника ідентифікаційної інформації (проксі–сервер IdP) – SAP IAS;

– Identity Provider Proxy (IdP Proxy) – SAP IAS потрібно створити як постачальника послуг (SP) в Customer Managed IdP за допомогою метаданих, отриманих із Identity Provider Proxy (IdP Proxy) – SAP IAS;

– метадані потрібно отримати від постачальника ідентифікаційної інформації, керованого клієнтом;

– постачальника корпоративної ідентифікації, що представляє керований клієнтом IdP, потрібно створити в Identity Provider Proxy (IdP Proxy) – SAP IAS, використовуючи метадані, отримані з Customer Managed IdP.

Виконання Єдиного входу(SSO) з проксі–сервером постачальника ідентифікаційної інформації (проксі–сервер IdP):

– користувач отримує доступ до SAP Ariba Service Provider (SP) – SAP Ariba URL;

– постачальник послуг (SP) – SAP Ariba перешле автентифікацію до проксі–сервера постачальника ідентифікаційної інформації (IdP) – SAP IAS;

– Identity Provider Proxy (IdP Proxy) – SAP IAS (на основі додаткової умови) пересилає запит на автентифікацію до Identity Provider (IdP) – Customer Managed IdP;

– постачальник ідентифікаційних даних (IdP) – відображається вікно входу, кероване клієнтом IdP (наприклад, Microsoft Entra ID IdP), із запитом на введення облікових даних користувача;

– користувача автентифікує постачальник ідентифікаційної інформації (IdP) – керований клієнтом ідентифікатор на основі введених облікових даних, а відповідь із ідентифікатором користувача та атрибутами користувача надсилається до проксі–сервера постачальника ідентифікаційної інформації (проксі–сервер IdP) – SAP IAS;

– автентифікація користувача за допомогою ідентифікатора користувача та атрибутів користувача далі надсилається з проксі–сервера постачальника ідентифікаційної інформації (проксі–сервера ідентифікатора) – SAP IAS до постачальника послуг (SP) – SAP Ariba.

2.3.3 Автентифікація, ініційована постачальником послуг (SP) проти постачальника ідентифікаційної інформації (IdP)

Користувач може отримати доступ до ресурсу, представленого постачальником послуг (SP), за допомогою одного з наведених нижче підходів. Постачальник послуг (SP) має ініціювати автентифікацію:

– постачальник послуг (SP) і постачальник ідентифікаційної інформації (IdP) повинні обмінятися сертифікатами підпису (частиною метаданих);

– користувач отримує доступ до URL–адреси постачальника послуг (SP);

– постачальник послуг (SP) пересилає автентифікацію постачальнику ідентифікаційної інформації (IdP);

– постачальник ідентифікаційної інформації (IdP) автентифікує користувача та перенаправляє до постачальника послуг (SP).

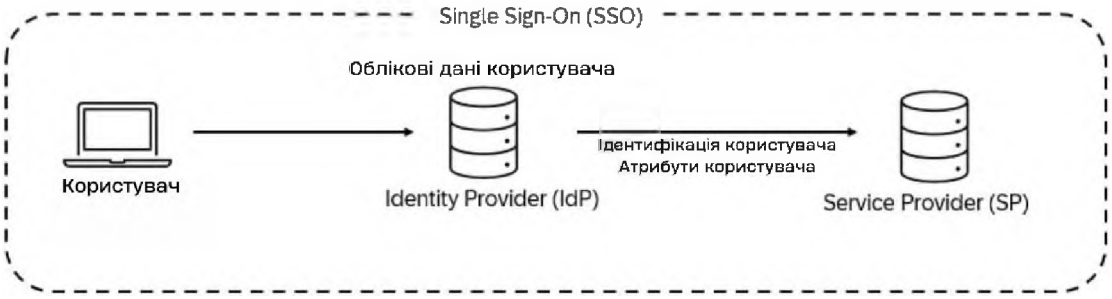

Рисунок 2.3 – Зв’язок користувача з постачальником послуг та постачальником ідентифікаційної інформації

Постачальник ідентифікаційної інформації (IdP) має ініціювати автентифікацію наступним чином:

– постачальник послуг (SP) повинен мати налаштований сертифікат підпису постачальника ідентифікаційної інформації (IdP) (частина метаданих);

– сертифікат підпису постачальника послуг (SP) не потрібно налаштовувати в постачальника ідентифікаційної інформації (IdP) у разі автентифікації, ініційованої IdP;

– у постачальника ідентифікаційної інформації (IdP) потрібно ввімкнути автентифікацію, ініційовану IdP.

– користувач отримує доступ до URL–адреси постачальника ідентифікаційної інформації (IdP) із переданим ідентифікатором постачальника послуг (SP) ;

– постачальник ідентифікаційної інформації (IdP) автентифікує користувача та перенаправляє до постачальника послуг (SP).

2.4 Конфігурація SAP Ariba SSO із службами SAP Cloud Identity – авторизація і автентифікація особи

Конфігурація самообслуговування автентифікації SAP Ariba SAML (PLICM–871)

Починаючи з випуску 2402 функції “PLICM–871: можливість налаштувати параметри автентифікації SAML в інтелектуальному диспетчері конфігурацій», клієнти можуть отримати файл метаданих SAP Ariba як самообслуговування. У разі налаштування SSO для SAP Ariba Sourcing, SAP Ariba Contracts, SAP Ariba Supplier Lifecycle and Performance для клієнтів, інтегрованих у пакет, установку SSO та, отже, отримання метаданих потрібно виконати на SAP Ariba закупівельному клієнті . У разі налаштування конфігурації SAP Ariba з декількома ERP (інакше як Federated Process Control FPC) конфігурація SSO та отримання метаданих повинні відбуватися для батьківського клієнта.

Для окремого (не інтегрованого в пакет) SAP Ariba Sourcing Tenant потрібно:

– користувач SAP Ariba з типом стороннього корпоративного користувача (Ariba);

– користувач SAP Ariba з членством у групі адміністратора клієнта.

Щоб налаштувати автентифікацію SAML SAP Ariba за допомогою SAP IAS:

– введення клієнта SAP Ariba згідно з приміткою вище, використовуючи URL–адресу для входу стороннього корпоративного користувача (Ariba);

– перехід до Manage –> (Core Administration – for SAP Ariba procurement tenant або Administration for SAP ariba sourcing tenant) –> Intelligent Configuration Manager –> Manage Configurations –> [Continue] –> Authentication –> [Update];

– завантаження файлу метаданих SAP IAS;

– далі– “Увімкнути автентифікацію SAML» на “Так», щоб увімкнути SSO (усі дані попередньо налаштовано з імпортованого файлу метаданих SAP IAS) та [Надіслати].

Якщо для параметра “Увімкнути автентифікацію SAML» встановлено значення “Так», SAP Ariba використовуватиме для автентифікації облікові дані (паролі), збережені в SAP IAS, а не облікові дані (паролі), збережені в SAP Ariba. Тому бізнес–користувачів SAP Ariba потрібно буде запросити до SAP IAS, активувати їхні облікові записи та створити облікові дані користувача (паролі). Якщо для параметра “Увімкнути автентифікацію SAML» встановлено значення “Ні», SAP Ariba використовуватиме для автентифікації облікові дані (паролі), збережені в SAP Ariba.

2.4.1 Конфігурація автентифікації SAP IAS SAML

Щоб налаштувати автентифікацію SAP IAS SAML за допомогою SAP Ariba:

– вхід до консолі адміністрування SAP IAS через https://<ідентифікатор клієнта SAP IAS>.accounts.ondemand.com/admin;

– перехід до Application & Resources –> Application –> [Create], щоб створити додаток для SAP Ariba як постачальника послуг (SP);

– введення відображуваного ім’я, вибір рішення SAP Ariba як тип, SAML 2.0 як тип протоколу та натиснути [Створити].

Щоб перевірити статус SAP Ariba SSO Setup, потрібне виконання одного із наведених нижче варіантів.

– перевірка SAP Ariba SSO за допомогою інтелектуального керування конфігурацією;

– перевірка SAP Ariba SSO, перейшовши за URL–адресою SAP Ariba у браузері/

Передумови: Користувач SAP Ariba з членством у групі адміністратора клієнта.

Для перегляду наявного налаштування SSO SAP Ariba потрібне виконання наступних пунктів:

– введення тенанта SAP Ariba;

– перехід до Manage –> (Core Administration – для SAP Ariba procurement tenant або Administration for SAP ariba sourcing tenant) –> Intelligent Configuration Manager –> Manage Configurations –> [Продовжити] –> Authentication;

– перевірка конфігурації SAP Ariba SSO для Test або Production.

Далі йде перевірка налаштування системи Єдиного входу SAP Ariba, перейшовши за URL–адресою SAP Ariba через веб–переглядач – за допомогою URL–адреси доступу бізнес–користувача. Наведені нижче тести не працюватимуть, якщо використовується сертифікат браузера, а бізнес–користувач увійшов до SAP Ariba без введення облікових даних.

2.4.2 Налаштування постачальника послуг SAML 2.0

Зв’язок налаштовується шляхом завантаження метаданих постачальника послуг або введення інформації вручну. Ведення вручну ім'я постачальника послуг, його кінцеві точки та сертифікат підпису. Можливе додання двох сертифікатів підпису. Обидва сертифікати підпису приймаються відповідно до терміну дії сертифіката. Є можливість вибрати сертифікат постачальника посвідчень, який буде використовуватись для підпису кожної програми. Ідея можливості вибору сертифіката IdP полягає в тому, що коли є можливість змінити сертифікат IdP за замовчуванням, всі програми простоюватимуть, оскільки програми довіряють поточній програмі за умовчанням на стороні програми. Таким чином, при додаванні нового сертифіката IdP можна по одному змінити програми, щоб вони довіряли новому сертифікату.

Щоб настроїти довіреного постачальника послуг SAML 2.0 у консолі адміністрування SAP Cloud Identity Services , потрібно виконати наступні дії:

– вхід у консоль адміністрування для SAP Cloud Identity Services;

– у розділі “Програми та ресурси» перехід до додатку “Програми»;

– вибір програми, яку потрібно редагувати;

– у розділі єдиного входу вибір Конфігурація SAML 2.0;

– завнтаження XML–файл метаданих постачальника послуг, використовуючи URL–адресою метаданих або введення параметрів зв’язку, узгоджені між автентифікацією ідентифікації та постачальником послуг.

Коли метадані постачальника посвідчень завантажуються або використовується URL–адреса метаданих, поля заповнюються проаналізованими даними з XML–файлу. Мінімальна конфігурація – заповнити поле “Ім'я».

Таблиця 2.1 – Параметри для налаштування постачальника послуг SAML

Поле	Опис
Вибрати: 1. Файл метаданих 2. URL–адреса метаданих	1. XML–файл метаданих постачальника послуг. 2. URL–адреса з метаданими постачальника послуг.
Назва	Ідентифікатор організації постачальника послуг.
Кінцева точка обслуговування клієнтів Assertion	URL–адреса кінцевої точки SP, яка отримує відповідь із твердженням SAML від ідентифікаційної автентифікації. Можливі такі варіанти: 1. URL–адреси для потоку браузера – дозволений домен для потоків браузера. 2. URL–адреса для основного розповсюдження – URL–адреса необхідна для основних сценаріїв розповсюдження до додатків ABAP відповідно до RFC 7522. Правильну URL–адресу можна знайти в документації програми, що надає. Під час автентифікації кінцевій точці ACS надається запит. Через потік автентифікація ідентифікації видаляє атрибути запиту, а під час відповіді вона порівнює кінцеву точку ACS із тим, що налаштовано в конфігурації SAML 2.0 програми.

Продовження таблиці 2.1

	Ідентифікаційна автентифікація шукає точну відповідність, і якщо такої відповідності немає, автентифікація буде невдалою.
Єдина кінцева точка виходу	URL–адреса кінцевої точки постачальника послуг, яка отримує відповідь або запит на вихід із системи (для сценарію з кількома постачальниками послуг) від ідентифікаційної автентифікації для припинення всіх поточних сеансів. Це поле має такі атрибути: 1. Прив'язка – визначає зв'язування SAML, яке підтримується кінцевою точкою виходу. 2. HTTP–POST 3. HTTP–ПЕРЕСПРАВЛЕННЯ 4. SOAP – Кінцева точка SOAP викликається лише після зміни пароля користувача. 5. URL – вказує розташування кінцевої точки виходу. 6. URL–адреса відповіді – (необов'язково) вказує інше місце, куди мають надсилатися повідомлення відповіді про вихід із системи.
Сертифікат підпису	Сертифікат у кодуванні base64, який використовується постачальником ідентифікаційної інформації для перевірки підписів повідомлень протоколу SAML, створених постачальником послуг. Натиснути кнопку "Додати», щоб додати другий сертифікат підпису. Якщо є два сертифікати, вибираємо стандартний, щоб позначити основний сертифікат. Основний сертифікат завжди перевіряється спочатку. Якщо його перевірка не вдається, то використовується вторинний сертифікат.

Таблиця 2.2 – Налаштування параметрів підпису для програми

Параметр	Конфігурація за замовчуванням
Підпис твердження	Увімкнено
Підпис відповіді автентифікації	Вимкнено
Підпис окремого повідомлення про вихід із системи	Увімкнено
Обов'язкові підписані запити автентифікації	Вимкнено

Продовження таблиці 2.2

Обов'язкове підписання одноразових повідомлень про вихід із системи	Увімкнено

У розділі "Сертифікат шифрування» додаємо сертифікат, якщо сертифікати шифрування не додані або потрібно додати новий сертифікат.

Вибрати елементи для шифрування зі списку, що розкривається:

– ніякого– варіант за замовчуванням;
– ідентифікатор імені суб'єкта;
– ідентифікатор імені суб'єкта та атрибути;
– атрибути.

Метод шифрування – aes–128–cbc. Збереження вибору. Після зміни програми система відображає повідомлення Програма <назва програми> оновлена.

Далі, налаштування з'єднання на стороні постачальника послуг.

1. Завантаження метаданих SAML 2.0 ідентифікаційної автентифікації.
2. Налаштування постачальника послуг на довіру автентифікації особи.

2.4.3 Альтернативний постачальник послуг OpenID

Також є можливість використати іншого постачальника послуг – OpenID для встановлення Єдиного входу. Довіра налаштовується шляхом введення інформації вручну. Є можливість вручну ввести ім'я клієнта (довіряючої сторони) та URI його перенаправлення. Щоб налаштувати довірену програму OpenID Connect на консолі адміністрування для SAP Cloud Identity Services, необхідне виконання таких дій:

– вхід у консоль адміністрування для SAP Cloud Identity Services;
– у розділі "Програми та ресурси» вибрати додаток "Програми»;
– вибрати програму, яку потрібно редагувати;
– вибрати вкладку Довіра;
– у розділі Єдиного вхіду вибрати Конфігурація підключення OpenID;
– введення параметрів зв'язку, узгоджені між автентифікацією особи та клієнтом.

Таблиця 2.3 – Параметри для налаштуваня постачальника послуг OpenID

Параметр	Опис
Назва(обов'язково)	Вказати назву на вибір.
URI перенаправлення (обов'язково)	URI перенаправлення, на які можна надіслати відповідь. Є можливість додати до 20 URI перенаправленнь.
Front–Channel Logout URIs	(Необов'язково) URI, які будуть потрібні для виходу. Є можливість додати до 20 URI.
Back–Channel Logout URI	(Необов'язково) URI, які будуть потрібні для виходу. Є можливість додати до 20 URI.

– У розділі "Сертифікат постачальника посвідчень» виберіть сертифікат, який буде використовуватись.

– Вибрати такі типи грантів:

Таблиця 2.4 – Типи грантів

Тип Гранту	Примітки
Код авторизації	Для потоку коду авторизації.
Код авторизації Код авторизації / Застосування PKCE (S256)	Для потоку коду авторизації з PKCE.

Для кожного потоку потрібно вибрати відповідний тип гранту. Всі інші типи грантів можна скасувати, якщо вони не потрібні програмі. Збрегти вибір і після зміни програми система відображає повідомлення Програма <назва програми> оновлено.

Налаштовуємо базову автентифікацію HTTP для програми. Щоб отримати додаткові відомості про конфігурацію, див. Налаштування секретів для автентифікації API. Увімкніть параметр загальнодоступних потоків клієнта для цієї програми. У консолі адміністрування виберіть "Автентифікація клієнта OpenID Connect» на вкладці "Довіра» "Увімкнути потоки загальнодоступного клієнта» у розділі "Public Client» . Є можливість налаштувати групи дозволів API. Щоб отримати додаткові відомості, див. Використання API з інших програм.

2.5 Кінцеві можливі сценарії робочого процесу двох систем з допомогою технології Єдиного входу.

2.5.1 Автоматизація Source–to–Pay за допомогою мережі Ariba

“Automation of Source–to–Pay with Ariba Network» дає змогу безперешкодно підключатися від SAP S/4HANA до постачальників у SAP Business Network. Є можливість надіслати запит на пропозиції, запитуючи інформацію про ціну та кількість, а також витрати на доставку. Також є можливість надсилати електронні замовлення на купівлю та товарні квитанції своїм постачальникам за допомогою SAP Business Network, а також отримувати електронні підтвердження замовлення на матеріали, розширені сповіщення про доставку та рахунки–фактури в SAP S/4HANA від постачальників. Є можливість надсилати повідомлення про оплату в електронній формі своїм постачальникам у SAP Business Network. Усі дані направляються через SAP Integration Suite, керований шлюз для управління витратами та SAP Business Network.

Як можна побачити на рисунку 2.4 користувач більше не може створити платіжний документ, а після обробки створити несанкціонований документ для компенсації рахунку–фактури та не може змінити умову ціни для певного клієнта/продукту, щоб неналежним чином надати клієнту більш вигідну ціну через ряд перевірок та затверджень(наприклад: Рисунок 2.4, пункт 8 та 12). Через більшу кількість перевірок та правильній синронізації двох систем.

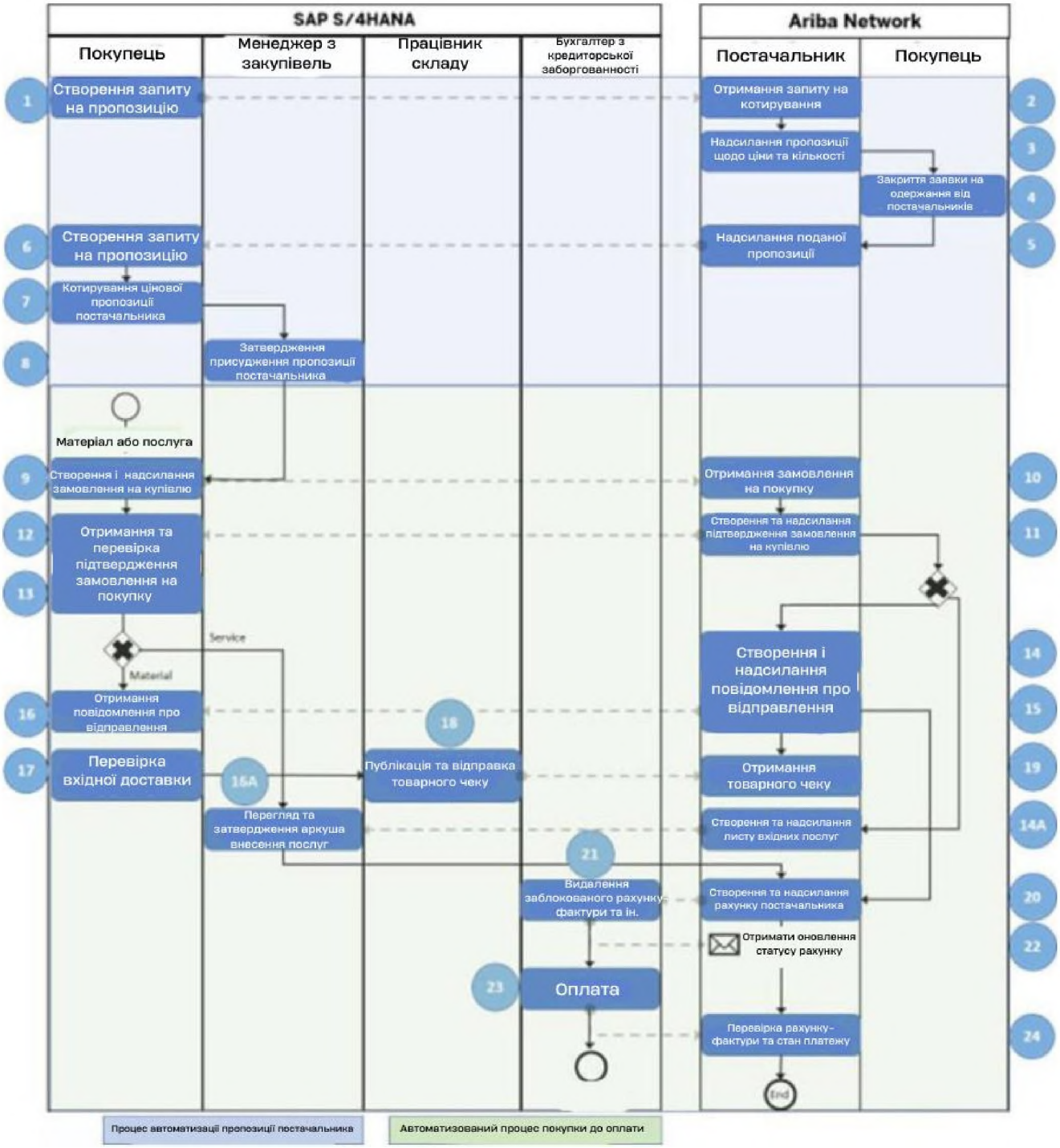

Рисунок 2.4 – взаємодії систем SAP S/4HANA та Ariba для сценарію Автоматизація Source–to–Pay

У наступній таблиці описані етапи процесу та служби SOAP, на кожному етапі процесу:

Таблиця 2.5 – Опис процесу взаємодії двох систем у рамках сценарію Автоматизація Source–to–Pay

Крок процесу №	Деталі процесу
1. Створення запиту на пропозицію	У SAP S/4HANA покупець створює запит пропозиції, запитуючи інформацію про ціну та кількість матеріальних одиниць, а також витрати на доставку.
2. Отримання запиту на котирування	Запит на пропозицію передається від SAP S/4HANA до мережі Ariba.
3. Надсилання пропозиції щодо ціни та кількості	У SAP Business Network постачальники можуть надсилати свої відповіді.
4. Закриття заявки на одержання від постачальників	У SAP Business Network покупці можуть закрити пропозиції постачальників до закінчення періоду, наприклад, якщо вони отримали достатню кількість заявок.
5. Надсилання поданої пропозиції	Відповіді постачальників надсилаються до SAP S/4HANA.
6. Отримання поданмх пропозицій	Відповідні пропозиції постачальників автоматично створюються в SAP S/4HANA та можуть відображатися покупцями.
7. Котирування цінової пропозиції постачальника	Покупець надає цінову пропозицію постачальника в SAP S/4HANA.
8. Затвердження присудження пропозиції постачальника	Присудження пропозиції постачальника може бути затверджено, наприклад, менеджером із закупівель.
9. Створення і надсилання замовлення на купівлю	Покупець створює замовлення на купівлю, яке надсилається з SAP S/4HANA до SAP Business Network. Для кожного товару покупець може попросити постачальника надіслати підтвердження замовлення на купівлю або сповіщення про відправку після отримання замовлення на купівлю в SAP Business Network. Замовлення на купівлю може містити матеріальні елементи, мінімальні послуги або розширені обмеження. Зміни в замовленнях на

Продовження таблиці 2.5

	купівлю або скасування також можна перенести в SAP Business Network.
10. Отримання замовлення на покупку	Постачальники отримують замовлення на купівлю або зміни чи скасування замовлення на купівлю в SAP Business Network.
11. Створення та надсилання підтвердження замовлення на купівлю	Постачальники можуть повністю або частково підтверджувати замовлення на купівлю або окремі позиції та надсилати підтвердження замовлення на купівлю покупцям у SAP S/4HANA. Вони також можуть відхилити або замовити окремі позиції та кількість або відхилити повне замовлення на купівлю, якщо потрібно.
12 і 13 Отримання та перевірка підтвердження замовлення на покупку	Покупці можуть отримувати підтвердження замовлення на купівлю від своїх постачальників через SAP Business Network і відображати їх у SAP S/4HANA.
14 і 15 (14a) Створення і надсилання повідомлення про відправлення або: Створення та надсилання листу вхідних послуг	У випадку матеріальних товарів постачальники можуть надсилати покупцям повідомлення про відвантаження. У разі мінімальних послуг або розширених лімітів постачальники можуть створити та надіслати аркуш введення послуг. Для позицій посиленого ліміту можна вказати опис послуги, кількість, одиницю виміру, ціну за одиницю виміру та термін виконання.
16(16a) Отримання повідомлення про відправлення або: Перегляд та затвердження аркуша внесення послуг	У SAP S/4HANA розширені сповіщення про доставку створюються для повідомлень про доставку, отриманих від їхніх постачальників через SAP Business Network. Для економних послуг або розширених лімітів покупці можуть переглянути та затвердити або відхилити аркуш введення послуг. Якщо аркуш введення послуг необхідно змінити, покупці можуть надіслати редагований аркуш введення послуг постачальникам. Після того, як постачальник надсилає новий аркуш введення послуг, оригінальний аркуш введення послуг замінюється.
17. Перевірка вхідної доставки	Покупець може перевірити в замовленні на купівлю, чи створено документ вхідної доставки.
18. Публікація та відправка товарного чеку	Після отримання товару працівник складу створює товарну квитанцію.

Продовження таблиці 2.5

19. Отримання товарного чеку	Постачальник отримує товарний чек через SAP Business Network.
20. Створення та надсилання рахунку постачальника	Постачальник створює рахунок–фактуру та надсилає його до SAP S/4HANA з SAP Business Network.
Отримання рахунку постачальника	Бухгалтер із кредиторської заборгованості отримує рахунок–фактуру в SAP S/4HANA. Далі, отримує статус залежно від налаштувань, зроблених у елементі конфігурації Ariba Network Integration for Buyers (SOAP).
Надсилання оновлень статусу рахунків–фактур	Оновлення статусу для рахунків–фактур постачальників надсилаються постачальникам у SAP Business Network, коли рахунок–фактура опубліковано або закріплено.
Отримування оновлення статусу рахунку постачальника	Постачальник бачить змінений статус рахунку–фактури в SAP Business Network.
21. Видалення заблокованого рахунку–фактури та ін.	Бухгалтер з кредиторської заборгованості обробляє рахунок–фактуру. Рахунок–фактуру можна оплатити, скасувати, узгодити або розблокувати заблокований рахунок–фактуру. Ці дії змінюють статус рахунку–фактури.
22. Отримання оновлення статусу рахунку постачальника	Постачальник бачить змінений статус рахунку–фактури в SAP Business Network.
23. Оплата	Є можливість надіслати повідомлення про оплату постачальникам через SAP Business Network.
24. Перевірка рахунку–фактури та стан платежу	Постачальник бачить змінений статус рахунку–фактури в SAP Business Network. Статус змінюється на платний.

2.5.2 Можливість керованих закупівель за допомогою SAP Ariba Buying

Можливість керованих закупівель SAP Ariba Buying дає змогу поєднувати вказівки для заявників, надані керованими закупівлями, з перевіреними процесами закупівель, які надає SAP S/4HANA. У цьому сценарії співробітники створюють запити на елементи каталогу, наявні матеріали, заплановані ощадливі послуги, ліміт елементів на матеріали та послуги або елементи вільного тексту,

додаючи їх до запиту в керованій покупці. Потім запит реплікується в SAP S/4HANA, де створюється заявка на придбання. У запиті співробітники можуть бачити номери наступних документів, створених у SAP S/4HANA [12].

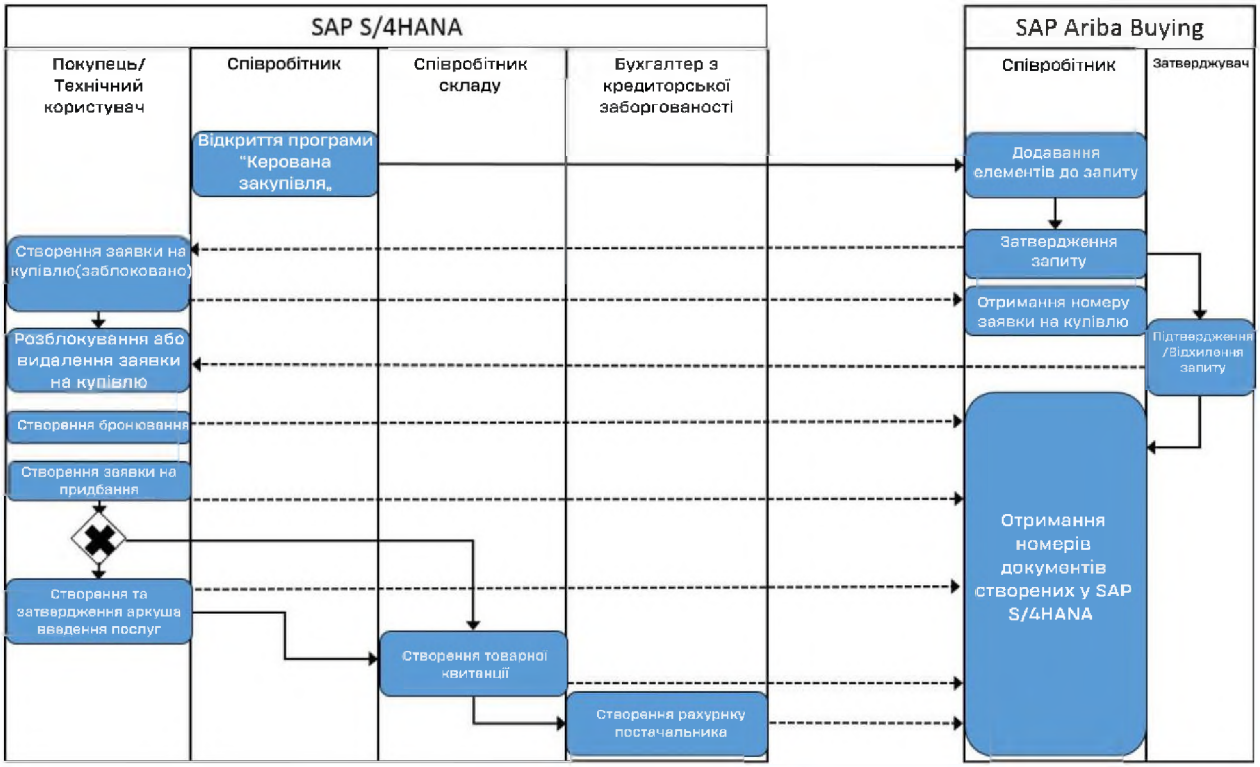

Рисунок 2.5 – Схема взаємодії систем SAP S/4HANA та Ariba для сценарію Можливість керованих закупівель

У наступній таблиці пояснюються етапи процесу та технічні служби, які використовуються для зв'язку між системами.

Таблиця 2.6 – Опис процесу взаємодії двох систем у рамках сценарію Можливість керованих закупівель

Крок процесу №	Деталі процесу
1. Відкритя програми Guided Buying у SAP Fiori Launchpad і створення запиту	Якщо створено відповідну плитку в SAP Fiori Launchpad, працівник може отримати доступ до можливості керованих покупок у SAP Ariba Buying із SAP Fiori Launchpad шукаючи елементи (матеріали або економні послуги) у каталогах і додавати їх до запиту.
2. Надсилання запиту на затвердження	Коли працівник перевіряє запит, є можливість переглянути його та подати на затвердження. Це ініціює створення заявки на купівлю в SAP S/4HANA. Якщо вкладення було додано для

Продовження таблиці 2.6

	запиту позицій під час керованої покупки, вони також переносяться до SAP S/4HANA. Заявка на купівлю блокується, доки її не буде схвалено у функції керованих закупівель.
3. Схвалення або відхилення запит	Щойно особа, що затверджує, випускає запит, у SAP S/4HANA надсилається повідомлення про оновлення, яке ініціює розблокування заявки на придбання. Після того, як особа, що затверджує, відхиляє запит, повідомлення про оновлення надсилається до SAP S/4HANA, яке ініціює видалення заявки на купівлю, і на цьому процес завершується.
4. Створення бронювання	Якщо елемент заявки на купівлю є релевантним для резервування, резервування створюється для запитуваного елемента. Номер резервування передається в SAP Ariba Buying і відображається в запиті.
5. Створення замовлення на купівлю	На основі заявки на купівлю створюється замовлення на закупівлю запитаної позиції. Якщо система налаштована відповідно, це буде зроблено автоматично. Номер замовлення на купівлю передається в SAP Ariba Buying і відображається в запиті.
6. Створення товарний чек або аркуш введення послуг для ощадливих послуг	У випадку матеріальних одиниць: коли товар доставлено, працівник складу створює товарну квитанцію в SAP S/4HANA. У випадку ощадливих елементів послуг: Коли послуги надаються, Покупець (наприклад) створює аркуш введення послуг у SAP S/4HANA. Після цього автоматично створюється товарний чек. Номер товарного чеку (і аркуша введення послуг, у разі послуг) передається в SAP Ariba Buying і відображається в запиті. У випадку матеріальних одиниць: коли товар отримано під час керованої закупівлі, працівник складу створює товарну квитанцію в керованій закупівлі, а деталі надсилаються до SAP S/4HANA за допомогою служби OData API.
7. Створення рахунку постачальника	Бухгалтер із кредиторської заборгованості створює рахунок–фактуру постачальника в SAP S/4HANA. Номер рахунка–фактури передається в SAP Ariba Buying і відображається в запиті.

Кожен зі сценаріїв, має свої відповідні ризики але як можна побачити на рисунку 2.5 такі ризики як створення фіктивного замовлення на купівлю і оприлюднення товарного чека призводить яке до відхилення та створення фіктивного матеріал у головному записі(master data), а після додавання основного запису маніпулювання загальною угодою купівлі–продажу, включивши цей матеріал до угоди купівлі, яку підтримує/створює користувач неможливі через численні перевірки з боку двох систем. Наприклад від співробітника до затверджувача заявка на купівлю блокується, доки її не буде схвалено у функції керованих закупівель затверджувачем який знаходиться у одній системі. І остаточне видалення або створення заявки на придбання технічним працівником у іншій системі. Таким чином обов'язки та права рівномірно розподіляються між декількома уповноваженими особами в двох системах та забезпечують більш надійну взаємодію у системах.

2.6 Висновки за другою частиною

У спеціальній частини було проаналізовіано та визначено ризики та їх сценарії пов’язанні з використанням гібридних систем на базі системи SAP Ariba(у зв'язці з S/4HANA).

Далі, запропоновано сценарій реалізації технології Єдиного входу за допомогою налаштування постачальнику ідентифікаційної інформації (IdP), налаштування постачальника послуг SAML 2.0 або альтернативного постачальника послуг OpenID.

За результатами реалізації Єдиного входу наведено та проаналізовано сценарії використання технології у гібридній системі S/4HANA та SAP Ariba.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ до економічної частини

Метою виконання розділу є визначення витрат на впровадження технології Єдиного входу в системі SAP Ariba, а також для підтримання системи.

Для розрахунку вище вказаного необхідно:

– розрахувати капітальні витрати на реалізацію запропонованих рекомендацій;

– розрахувати річні експлуатаційні витрати на виконання рекомендацій;

– сума річних амортизаційних відрахувань на апаратні засоби, необхідні для виконання рекомендацій;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.2 Розрахунок капітальних витрат

Капітальні інвестиції–це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта технології складають:

$$K = K_{\text{пр}} + K_{\text{зпз}} + K_{\text{навч}} + K_{\text{д}} \quad (3.1)$$

$$K = 130000 + 20000 + 30000 + 10000 = 190000 \text{ тис. грн}$$

де $K_{\text{пр}}$ – вартість впровадження проєкту та залучення для цього зовнішніх консультантів, тис. грн;

$$K_{\text{пр}} = 90000 + 40000 = 130000, \text{ тис грн}$$

На розробку та впровадження проєкту компанія витратить близько 90000 грн, а також на залучення зовнішніх консультантів 40000 грн.

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) дорівнює 20000 тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу дорівнює 30000 тис. грн;

$К_д$ – додаткові витрати витрати на налагодження системи дорівнює 10000 тис. грн.

Розрахувати альтернативні витрати $К_а$ неможливо так як вартість впровадження проєкту фіксована.

3.3 Експлуатаційні витрати

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за рік, що виражені у грошовій формі.

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$C = C_в + C_к + C_{ак} \quad (3.2)$$

$$C = 37000 + 11000 = 48000, \text{ тис.грн}$$

де $С_в$ – вартість Upgrade–відновлення й модернізації системи;

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$(активність користувача)– витрати, викликані активністю користувачів в системі SAP Ariba. Витрати на користувачів непотрібні бо це вже входить у вартість технології.

Витрати на керування технологією Єдиного входу в системі SAP Ariba ($С_к$) складають:

$$C = C_н + C_а + C_з + C_{єв} + C_{ел} + C_о + C_{тос}, \text{ тис грн} \quad (3.3)$$

$$C = 5000 + 2000 + 259200 + 12000 + 36067 + 15000 + 7800 = 337067$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$) =20000.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів.

$$C_a = Ф_{перв} * Н_а + К_{лиз} * Н_{апз}, \text{ грн} \quad (3.4)$$

$$С_а = 13636*0,33+37500*0,2=12000$$

де $Ф_{перв}$ – первісна вартість обладнання на початок року, грн.;

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

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

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

Річний фонд заробітної персоналу, що обслуговує систему ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.5)$$

$$C_з = 20000 * 12 + 1600 * 12 = 259200 \quad (2.9)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування $С_{єв}$= 12000.

Вартість електроенергії, що споживається апаратурою протягом року ($С_{ел}$), визначається за формулою:

$$C_{ел} = P * F_p * Ц_е, \text{ грн} \quad (3.6)$$

$$C_{ел} = 6 * 2080 * 2,89 = 36067$$

де Р – встановлена потужність апаратури для взаємодії з системою, кВт;

$F_р$ – річний фонд робочого часу використання системи з технологією;

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

Витрати на залучення сторонніх *організацій* для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації. В данному випадку стороньою організацією буде фірма зі встановлення технології. $С_о$= 64000

Витрати на технічне й організаційне адміністрування та сервіс системи $С_{тос}$=10800.

3.4 Оцінка величини збитка

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \text{ грн} \quad (3.7)$$

$$U = 14700 + 34970 + 7690 = 128360$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за годину простою внаслідок атаки:

$$П_{п} = \frac{\sum Зс}{F} * t_{п} \quad (3.8)$$

$$П_{п} = \frac{\sum 85000}{160} * 6 = 3187, \text{грн}$$

де F – місячний фонд робочої години (при 40–й годинній робочій неділі становить 160 год).

$t_{п}$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$З_{с}$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають декілька складових:

$$П_{в} = П_{ві} + П_{пв} + П_{зч} \quad (3.9)$$

$$П_{в} = 5000 + 25000 + 7000 = 37000$$

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

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

$П_{зч}$ – вартість заміни обладнання чи запасних частин, грн.

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_{в}$ і розміром середньогодинної заробітної плати обслуговуючого персоналу($З_{о}$):

$$П_{пв} = \frac{\sum З_{о}}{F} * t_{в} \quad (3.10)$$

$$П_{пв} = \frac{\sum 40000}{160} * 9 = 2250, \text{грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_{r}} * (t_{п} + t_{в} + t_{ви}) \quad (3.11)$$

$$V = \frac{12670000}{2080} * (6 + 9 + 5) = 121826$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5–ти денний робочий тиждень, 8–ми годинний робочий день) становить близько 2080 ч.

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

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

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

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

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum i \sum n\, U \tag{3.12}$$

$$B = 4 * 2 * 128360 = 1026880$$

Де I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

3.5. Загальний ефект від впровадження технології Єдиного входу

Загальний ефект від впровадження технології визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B * R - C \tag{3.13}$$

$$E = 1026880 * 0.5 - 48000 = 465440$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. Грн;

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

C – щорічні витрати на експлуатацію технології, тис. Грн.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} \tag{3.14}$$

$$ROSI = \frac{465440}{190000} = 2.45$$

де Е – загальний ефект від впровадження технології Єдиного входу, тис. грн;

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

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності $E_н$.

Проект визнається доцільним за умови

$$ROSI > E_н$$

При ROSI < $E_н$ варіант є збитковим і більш економічним визнається відмова від його реалізації.

Термін окупності капітальних інвестицій $T_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження технології Єдиного входу:

$$T_о = \frac{K}{E} = \frac{1}{ROSI} \tag{3.15}$$

$$T_о = \frac{1}{2.45} = 0.40 = 146 \text{ днів}$$

Якщо варіанти економічно рівноцінні, то приймається варіант, що забезпечує більш високу надійність, поліпшення умов праці.

3.6 Висновок за третьою частиною

Згідно з отриманими даними під час розрахунку економічної частини капітальні затрати становлять 190000 грн, експлуатаційні 48000 грн. Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 1026880 грн. Загальний ефект від впровадження технології Єдиного входу склав 465440 грн. Згідно с коефіцієнтом ROSI який становить 2,45 розроблений проєкт є цілком доцільними. Термін окупності проєкту становить 146 робочих днів.

ВИСНОВКИ

Для користувачів системи Сап Ариба, особливо для тих хто використовує її у складі гібридних систем, актуальність проблем авторизаціного концепту достатньо довго залишається основною проблемою використання цих систем. завдяки тому що система дозволів погано синхронізована, а технології об'єднання до цього моменту наведено не було, це призводило до появи великої кількості проблем. Доказом цього є виявлені та наведені ризики при використані систем які нашкодили не одному клієнту САП та призвели до витоку важливої інформації.

З огляду на поточну проблематику запропонована технологія здатна єфективно об'єднати системи та розподілити права користувачів в них корректно. Завдяки наведеній покроковій інструкції по впровадженю даної технології, будь–який адміністратор системи або співробітник безпеки з дозволу клієнта або керівника проєкту може з легкістю впровадити представлені зміни та покращити не тільки поточний стан безпеки компанії а також контроль розподілу та керування ролями та дозволами користувачів.

Слід пам'ятати, що проєктування ефективної системи авторизації та автентифікації, враховуючи типові вразливості зі створенням захисту від них, набагато дешевше та доцільніше, аніж ліквідовувати наслідки витоку інформації. Найняти спеціалістів з кібербезпеки буде правильним рішенням, для створення надійного захисту, та дешевше аніж зустрітися с наслідками незахищеної системою автентифікації.

В економічному розділі було розглянуто питання доцільності впровадження технології Єдиного входу, та за результатами розрахунків було визначено, що капітальні втрати на проєктування окупляться вже за 5 місяців функціонування систем захисту, через те, що вдасться уникнути несанкціонованого витоку інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. “What is SAP ERP?”
URL: https://www.ibm.com/topics/iaas–paas–saas (дата звернення: 29.05.2024).
2. “What is Ariba?”
URL: https://www.sap.com/sea/products/acquired–brands/what–is–ariba.html
3. “Access Control: Models and Methods»
URL:https://delinea.com/blog/access–control–models–methods#:~:text=Access%20Control%20Models%20allow%20organizations,RBAC%20or%20RB%2DRBAC).
4. “Concepts”
URL:https://help.sap.com/docs/cloud–identity–services/cloud–identity–services/concepts
5. “The Authorization Concept”
URL:https://help.sap.com/doc/saphelp_nw74/7.4.16/en–US/4c/e65fbf7e173ec6e10000000a42189b/content.htm?no_cache=true
6. “Benefits and Challenges of Implementing Cross System”
URL:https://help.sap.com/docs/cloud–identity–services/cloud–identity–services/concepts
7. “Considerations and Requirements for User Setup in SAP Cloud Identity Services – Identity Authentication”
URL: https://help.sap.com/docs/strategic–sourcing/configuration–guide–for–sap–ariba–supplier–management–applications–on–sap–business–technology–platform/considerations–and–requirements–for–user–setup–in–sap–cloud–identity–services–identity–authentication
8. “SAP Single Sign–On”
URL:https://help.sap.com/docs/SAP_SINGLE_SIGN–ON
9. “Top 5 Federated Single Sign–on (SSO) Scenarios”
URL:https://blog.empowerid.com/blog–1/bid/153386/Top–5–Federated–Single–Sign–on–SSO–Scenarios

10. “What is SAML 2.0”

URL: https://help.sap.com/docs/SAP_IDENTITY_MANAGEMENT/7c61245338d0434c91cb587217404b71/a634a802e03644d2a99ae96665229a7c.html

11. “Configure OpenID Connect Application for Authorization Code Flow”

URL: https://help.sap.com/docs/cloud–identity–services/cloud–identity–services/oidc–trust–configure–openid–connect–application–for–authorization–code–flow

12. “Integration with SAP Ariba Applications”

URL: https://help.sap.com/docs/SAP_S4HANA_ON–PREMISE/754a46a305c642559f21625ca2744170/705e158a91894e758565840b0e0100d8.html?version=2023.000

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	13	
6	А4	2 Розділ	28	
7	А4	3 Розділ	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна_записка_Гречук_125_20_3.docx

Пояснювальна_записка_Гречук_125_20_3.pdf

Презентація_Гречук_125_20_3.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85б. («добре»).

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ім'я, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
«Підсистема керування доступом системи управління закупівель SAP Ariba»
студентки групи 125–20–3
Гречук Діани Вадимівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 65 сторінках та містить 14 рисунків, 6 таблиць, 15 джерел та 4 додатка.

Метою кваліфікаційної роботи є забезпечення надійної авторизації в гібридних підсистемах на базі системи управління закупівель SAP Ariba.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз авторизаційних концептів систем, аналіз ризиків при взаємодії SAP Ariba з іншими системами, розробка проектних рішень.

Запропоновано впровадження технології Единого входу та сценарії реалізації взаємодії систем SAP Ariba та SAP S/4HANA з використанням технології Единого входу. Обґрунтовано ефективність запропонованих рішень.

Практичне значення результатів кваліфікаційної роботи полягає у можливості використанні запропонованих рішень в реальних системах управління закупівель.

До недоліків відноситься використання недостане обґрунтування окремих елементів запропонованих рішень.

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

За час дипломування Гречук Д.В. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо–професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки « відмінно ».

Керівник кваліфікаційної роботи, професор **Кагадій Т.С.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**