ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»
Факультет автоматизації виробництва та цифрових технологій
Кафедра цифрових технологій та проєктно-аналітичних рішень

«Допущено до захисту»
Гарант ОПП

Павло САГАЙДА

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістра

за підсумками виконання
освітньо-професійної програми
«Комп'ютерні науки та цифровий інтелект»
за спеціальністю 122 Комп`ютерні науки

на тему «Дослідження методів, моделей та інформаційних технологій автоматизації процесу інвентаризації конфіденційної інформації на підприємстві»

Керівник роботи Павло САГАЙДА

Консультант від бази практики Юрій РАТНЕР

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач Микита ІЛЬЧЕНКО

Підсумкова оцінка за атестацію			

Голова ЕК Олена ПАВЛЕНКО

КРИВИЙ РІГ 2024

metinvest polytechnic

ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»

Факультет	автоматизації виробництва та цифрових технологій
Кафедра	цифрових технологій та проектно-аналітичних рішень
Ступінь вищої освіти	магістр
Спеціальність	122 Комп'ютерні науки
ОПП	Комп'ютерні науки та цифровий інтелект

ЗАТВЕРДЖУЮ
Гарант ОПП

Павло САГАЙДА

«02» грудня 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Ільченку Микиті Володимировичу
(прізвище, ім'я, по батькові здобувача)

1. Тема роботи *Дослідження методів, моделей та інформаційних технологій автоматизації процесу інвентаризації конфіденційної інформації на підприємстві*
керівник роботи *Сагайда Павло Іванович, доцент, докт. техн. наук,*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом Університету від *14.10.2024 р. №238/14.10.2024*
2. Термін подання роботи *08.02.2025 р.*
3. Вихідні дані до роботи *Навчальна література, державні стандарти, методична література з спеціальних дисциплін та підготовки кваліфікаційної роботи, науково-дослідницькі роботи з тематики автоматизації обробки й аналізу даних та методів цифрового інтелекту, літературні джерела, результати власних експериментів та досліджень, технологічні інструкції тощо*
4. Зміст пояснювальної записки (перелік питань) *Реферат. Зміст. Вступ. 1. Аналіз стану питання, предметної області, концепцій з проблеми, що розглядається (літературний огляд, недоліки існуючих систем, сучасні тенденції). 2. Розробка математичної моделі об'єкта (предметної області) та методики дослідження. 3. Розробка програмно-методичного комплексу для інформаційної підтримки діяльності у процесу інвентаризації конфіденційної інформації на підприємстві. 4. Проведення та аналіз результатів теоретичних та експериментальних досліджень за індивідуальним завданням. 5. Економічне обґрунтування запропонованих технічних рішень. Висновки. Перелік використаних джерел. Додатки.*
5. Перелік графічного (демонстраційного) матеріалу (з точним зазначенням обов'язкових креслень): *Актуальність, мета, об'єкт, предмет та завдання дослідження; розроблені або удосконалені математичні моделі, методика дослідження; діаграми проекту програмно-методичного комплексу в нотації UML (діаграми прецедентів, класів, послідовностей, діяльності); результати розробки та експериментальних досліджень; результати економічних розрахунків; висновки до роботи; публікація результатів дослідження.*

6. Консультанти по роботі, із зазначенням розділів роботи, що стосуються їх.

Розділ	Прізвище, ініціали та посада консультанта
1	Сагайда П.І., проф. каф. ЦТПАР
2	Сагайда П.І., проф. каф. ЦТПАР
3	Сагайда П.І., проф. каф. ЦТПАР
4	Сагайда П.І., проф. каф. ЦТПАР
5	Гетьман І.А., доц. каф. ЦТПАР

7. Дата видачі завдання *02.12.2024*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи
1	Розділ 1. Аналіз стану питання, концепцій з проблеми, що розглядається	20.01.2025 - 22.01.2025
2	Розділ 2. Розробка математичної моделі об’єкта (предметної області) та методики дослідження	23.01.2025 - 25.01.2025
3	Розділ 3. Розробка програмно-методичного комплексу для інформаційної підтримки діяльності у процесі інвентаризації конфіденційної інформації на підприємстві	27.01.2025 – 30.01.2025
4	Розділ 4. Проведення та аналіз результатів теоретичних та експериментальних досліджень за індивідуальним завданням	31.01.2025 - 03.02.2025
5	Розділ 5. Економічні розрахунки	04.02.2025 - 05.02.2025
6	Висновки, перелік посилань, вступ, зміст, реферат	06.02.2025 – 07.02.2025
7	Подання завершеної роботи. Перевірка на академічний плагіат	08.02.2025 – 10.02.2025
8	Остаточне оформлення роботи, презентаційного матеріалу, автореферату	11.02.2025 – 13.02.2025
9	Рецензування завершеної роботи. Захист	14.02.2025 – 17.02.2025

Здобувач (Микита ІЛЬЧЕНКО)

Керівник роботи (Павло САГАЙДА)

РЕФЕРАТ

Мета дослідження.

Підвищення ефективності процесу інвентаризації критичної інформації та методи здобуття економії за рахунок даного процесу.

Об’єкт дослідження.

Автоматизація процесу інвентаризації критичної інформації.

Предмет дослідження.

Методи, моделі та інформаційні технології для автоматизації процесу інвентаризації критичної інформації.

Задачі дослідження.

Відповідно до зазначеної мети поставлено наступні задачі: огляд існуючих систем інвентаризації критичної інформації, аналітичний огляд парадигм по розробці ПЗ, логічне модулювання процесу, проєктування та розробка програмних компонентів для автоматизації інвентаризації критичної інформації, тестування та впровадження розроблених програмних компонентів, обґрунтування ефективності застосування запропонованих технічних рішень.

Структура та обсяг роботи.

Робота складається з визначень і термінології, вступу, 5 розділів, висновків, списку використаних джерел, 3 додатків. Загальний обсяг роботи становить 137 сторінок, робота містить 81 рисунок, 17 таблиць. Список використаних джерел складається з 40 джерел.

Ключові слова: інформаційна безпека, інвентаризація критичної інформації, конфіденційність, автоматизації процесів інформаційної безпеки, зниження ризиків ІБ.

ABSTRACT

Research goal.

Increasing the efficiency of the critical information inventory process and methods for obtaining savings through this process.

Research object.

Automation of the critical information inventory process.

Research subject.

Methods, models and information technologies for automating the critical information inventory process.

Research tasks.

In accordance with the stated goal, the following tasks were set: review of existing critical information inventory systems, analytical review of software development paradigms, logical process modulation, design and development of software components for automation of critical information inventory, testing and implementation of developed software components, justification of the effectiveness of the application of the proposed technical solutions.

Structure and scope of work.

The work consists of definitions and terminology, introduction, 5 sections, conclusions, list of sources used, 3 appendices. The total volume of the work is 137 pages, the work contains 81 figures, 17 tables. The list of sources used consists of 40 sources.

Keywords: information security, inventory of critical information, confidentiality, automation of information security processes, reduction of IS risks.

ЗМІСТ

ВИЗНАЧЕННЯ, ТЕРМІНОЛОГІЯ, СКОРОЧЕННЯ ТА АБРЕВІАТУРИ

Таблиця 1 - Визначення, термінологія, скорочення та абревіатури

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
ABAC	модель контролю доступу, заснована на атрибутах. Вона дозволяє визначати, чи надається доступ до ресурсів на основі атрибутів користувача, ресурсу та середовища, наприклад, місцезнаходження або часу доступу
Azure AD Conditional Access	функція в Azure Active Directory, яка дозволяє застосовувати правила доступу до ресурсів на основі різних умов, таких як стан пристрою, місцезнаходження користувача, тип підключення чи ризикова оцінка. Вона забезпечує гнучкий контроль доступу до корпоративних ресурсів
BPMN діаграма	стандарт для моделювання бізнес-процесів, який використовує графічні нотації для відображення процесів в організації. Це дозволяє спростити розуміння, аналіз та удосконалення процесів, а також покращити комунікацію між учасниками
DLP	набір технологій та політик, спрямованих на запобігання витоку або несанкціонованого доступу до чутливої інформації. DLP системи дозволяють відслідковувати, контролювати та обмежувати передачу конфіденційних даних у межах організації

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Gartner	міжнародна консалтингова компанія, яка надає дослідження, аналізи та поради для технологічних підприємств та організацій. Gartner відомий своїми звітами, рейтингами та прогнозами в області IT-ринку
ISMS	система управління інформаційною безпекою, яка включає набір політик, процедур та інструментів для управління ризиками та забезпечення захисту інформації в організації. ISMS базується на міжнародних стандартах, таких як ISO/IEC 27001, і допомагає підтримувати конфіденційність, цілісність та доступність даних
ISO	International Organization for Standardization (Міжнародна організація зі стандартизації), міжнародна неприбуткова організація, яка складається з національних органів зі стандартизації. Вона розробляє і публікує велику кількість міжнародних стандартів, які охоплюють майже всі аспекти технології і виробництва.
NIST	National Institute of Standards and Technology (Національний інститут стандартів і технологій), агентство Міністерства торгівлі США, чия місія полягає у сприянні американській інновації і промисловій конкурентоспроможності.

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
SaaS	модель надання програмного забезпечення, при якій програма розміщується на сервері постачальника і надається користувачам через Інтернет. Користувачі можуть користуватися програмою без необхідності її встановлення та обслуговування на власних пристроях
TLS	протокол шифрування, що використовується для забезпечення безпечної передачі даних між клієнтом і сервером через Інтернет. TLS забезпечує конфіденційність, цілісність та автентичність переданих даних
Автентифікація	процес перевірки ідентичності користувача або системи, щоб переконатися, що вони є тим, за кого себе видають, зазвичай через введення пароля або використання біометричних даних
Авторизація користувача	процес надання користувачеві доступу до ресурсів після автентифікації. Авторизація визначає, які дії користувач може виконувати на певних ресурсах або в системах
Архітектура	структурне планування або організація системи, що визначає її основні компоненти, їх взаємодію і принципи роботи. В IT-архітектурі це може стосуватися як апаратних, так і програмних компонентів

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Багатофакторна автентифікація	метод безпеки, що вимагає від користувача підтвердження його особи за допомогою двох або більше факторів: щось, що він знає (пароль), щось, що він має (смартфон або токен), або щось, що є частиною його біометрії (відбиток пальця)
База даних	організована колекція даних, яка зберігається та керується через систему управління базами даних (СУБД). База даних дозволяє ефективно зберігати, знаходити та обробляти великі обсяги інформації
Бізнес-вимога	необхідність або вимога, яка виникає в рамках бізнес-процесу або проекту і вимагає досягнення певного результату або функціональності. Бізнес-вимоги визначають, що має бути досягнуто для досягнення цілей організації
Бізнес-власник інформації	особа або група осіб, відповідальна за управління і захист інформації в організації. Бізнес-власник визначає, які дані є критичними для бізнесу і як вони повинні використовуватись, зберігатись та захищатись
Бізнес-процес	набір взаємопов'язаних дій або завдань, що виконуються для досягнення певної бізнес-мети або результату. Бізнес-процеси часто описуються за допомогою моделей, таких як BPMN діаграми

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Блокчейн	технологія дистрибутивного реєстру, яка забезпечує збереження даних у вигляді ланцюга блоків, що взаємопов’язані та захищені за допомогою криптографії. Блокчейн є основою для таких технологій, як криптовалюти, і може використовуватися для забезпечення прозорості та безпеки в різних сферах
Домен	сукупність комп'ютерних ресурсів (серверів, пристроїв, користувачів), що знаходяться під управлінням певної організації чи адміністратора. В IT-домені зазвичай встановлюються правила доступу і управління ресурсами, що дозволяють централізовано керувати системами
Доступ	можливість користувача або програми отримати доступ до ресурсів, функцій та даних інформаційно-телекомунікаційної системи за певними правилами та обмеженнями
Закон	нормативно-правовий акт, який приймається представницьким органом державної влади в особливому порядку, регулює певні суспільні відносини і забезпечується можливістю застосування заходів державного примусу

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Зловмисник	суб’єкт, який намагається отримати несанкціонований доступ до інформаційних ресурсів
Інвентаризація інформації	процес виявлення, опису, класифікації та обліку інформації, доступ до якої обмежено фізичною або юридичною особою
Інтелектуальна власність	права на результати інтелектуальної діяльності та на засоби індивідуалізації юридичних осіб, товарів, робіт, послуг та підприємств, які охороняються законом
Інтерфейс	набір засобів та методів для взаємодії користувача з програмним забезпеченням або апаратними засобами. В інформатиці це може бути як графічний інтерфейс (GUI), так і командний рядок (CLI), через які користувач взаємодіє з комп'ютерними системами
Інформаційна безпека	сукупність заходів і методів, спрямованих на захист інформації від несанкціонованого доступу, змін, знищення або втрати. Інформаційна безпека включає в себе забезпечення конфіденційності, цілісності та доступності інформації
Інформаційна система	сукупність інформації, інформаційних процесів, ресурсів, учасників та засобів збору, обробки, зберігання, передавання та використання інформації для досягнення певних цілей

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Інформаційний актив	будь-яка інформація, яка має цінність для організації або особи і потребує захисту від загроз
Інформація	відображення об’єктів, процесів, явищ та їх взаємозв’язків у формі, придатній для сприйняття, передавання, зберігання та обробки людиною або технічними засобами
Кібератака	навмисна спроба порушити роботу комп'ютерної системи, мережі або сервісу за допомогою шкідливих дій, таких як віруси, трояни, атаки типу "відмова в обслуговуванні" (DoS), фішинг та інші методи
Класифікатор інформації	система кодів, які відповідають певним категоріям інформації за її змістом, призначенням, формою подання та іншими ознаками
Комерційна таємниця	інформація, яка має комерційну цінність, є невідомою та не легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, і щодо якої вжито заходів щодо збереження її секретності
Консистентність	властивість даних або системи залишатися у коректному і логічному правильному стані після виконання операцій. В IT-контексті це стосується правильності і точності даних під час їх обробки та збереження

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Конфіденційна інформація	інформація, яка не є комерційною таємницею, але має обмежений доступ і не підлягає розголошенню без згоди її власника або інших підстав, передбачених законом
Ліцензія	правовий документ, який надає користувачу право використовувати програмне забезпечення або інші інтелектуальні ресурси за певних умов. Ліцензія визначає обмеження та права користувача на використання продукту
Методологія MoSCoW	підхід до виявлення пріоритетів вимог, який використовується в управлінні проектами. Вона дозволяє визначити, які завдання є найважливішими, і групує вимоги за категоріями: Must have (необхідно мати), Should have (повинно бути), Could have (можна мати), Won't have (не буде)
Персональні дані	будь-яка інформація, що стосується конкретної особи, яку можна ідентифікувати, як-от ім’я, адреса, номер телефону, електронна пошта, дані про місцезнаходження, біометричні дані тощо
Ризик інформації	ймовірність втрати, пошкодження, крадіжки, зловживання або несанкціонованого доступу до інформації, що може призвести до негативних наслідків для організації або особи.

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Роль користувача	набір прав і дозволів, які визначають, які дії може виконувати користувач в системі. Ролі дозволяють керувати доступом і встановлюють рівні привілеїв для різних типів користувачів
Сесія користувача	період часу, протягом якого користувач взаємодіє з комп'ютерною системою або веб-сайтом після автентифікації, до моменту виходу з системи або завершення сеансу. Сесія може включати в себе збереження даних користувача, налаштувань або історії взаємодії
Сценарій використання	опис конкретної ситуації, в якій система чи програмне забезпечення буде використовуватись, з акцентом на завдання та дії користувача. Сценарії використання зазвичай використовуються для визначення функціональності системи або для тестування
Хешування	процес перетворення вхідних даних (наприклад, пароля) у фіксовану рядок символів через математичний алгоритм. Хешування забезпечує незворотність цього процесу, тобто не можна відновити початкові дані з хешу

Продовження таблиці 1

Визначення, термінологія, скорочення та абревіатури	Визначення/Опис
Хмара, хмарна архітектура	технологія, що дозволяє зберігати та обробляти дані на віддалених серверах (в "хмарі") через Інтернет, замість локальних серверів чи пристроїв. Хмарна архітектура передбачає використання ресурсів за запитом і є основою для різних моделей хмарних сервісів, таких як IaaS, PaaS, SaaS
Шифрування	процес перетворення інформації в код, який може бути прочитаний лише тими, хто має спеціальний ключ для її дешифрування. Шифрування використовується для захисту конфіденційної інформації під час її передачі або зберігання
Юридична особа	організація, яка має права та обов’язки, визнані законом, та здатна брати участь у цивільно-правових відносинах від свого імені
BA	бізнес-аналітик
QA Tester	тестер програмного забезпечення
ЦОД	центр обробки даних
ПЗ	програмне забезпечення

ВСТУП

В умовах швидкого розвитку технологій та зростання кількості кібератак сучасні підприємства стикаються з необхідністю забезпечення кіберстійкості. Одним з важливих елементів цього процесу є інвентаризація критичної інформації. Процес інвентаризації дозволяє виявити та класифікувати інформаційні активи (форму в якій обробляється інформація), що є критично важливими для підприємства, а також ідентифікувати потенційні ризики та загрози для їх безпеки. Процес необхідний для ефективного управління інформаційною безпекою, збереженням даних та їх плануванням їх захисту, зменшенням ризиків впливу на репутацію компанії, довіри клієнтів та партнерів, а також її фінансової стабільності.

Одним з ключових аспектів інвентаризації критичної інформації є її відповідність міжнародним стандартам, таким як ISO/IEC 27001:2022. Цей стандарт надає керівництво щодо встановлення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Відповідність стандартам ISO [1-2] дозволяє підприємствам організувати процеси інвентаризації та управління ризиками більш структуровано, що сприяє підвищенню загальної ефективності системи безпеки. Крім того, наявність сертифікації ISO27001 може бути додатковою перевагою при співпраці з партнерами та клієнтами, оскільки це підтверджує високу якість управління інформаційною безпекою на підприємстві.

Процес інвентаризації критичної інформації допомагає підприємствам зосередити ресурси на найбільш важливих активах, знижуючи при цьому витрати та підвищуючи ефективність захисту. В умовах обмежених ресурсів та високої конкуренції важливо забезпечити, щоб вкладені в безпеки інвестиції мали максимальний ефект. Автоматизація процесів інвентаризації [12, 26, 31], впровадження

інтелектуальних систем для аналізу та оцінки ризиків, а також інтеграція з іншими системами управління інформаційною безпекою дозволяють підприємствам оптимізувати використання ресурсів та підвищити загальну ефективність роботи.

Інвентаризація критичної інформації включає в себе кілька етапів: виявлення інформаційних активів, їх класифікація, оцінка ризиків та загроз, а також розробка заходів для їх мінімізації (може існувати окремо). Виявлення інформаційних активів передбачає створення повного переліку всіх даних, що є критичними для роботи підприємства. Класифікація інформаційних активів дозволяє визначити їх важливість та пріоритетність, що допомагає у подальшому розподілі ресурсів для їх захисту. Оцінка ризиків та загроз включає в себе аналіз потенційних вразливостей та ймовірності їх реалізації, а також визначення можливих наслідків для підприємства. На основі цього аналізу розробляються заходи для мінімізації ризиків, включаючи впровадження технічних, організаційних та процедурних заходів безпеки.

Розвиток процесу інвентаризації критичної інформації включає кілька ключових напрямків:

– автоматизація збору та обробки даних;

– використання сучасних технологій, таких як машинне навчання та штучний інтелект, для підвищення точності та швидкості процесів інвентаризації;

– впровадження інтелектуальних систем для аналізу та оцінки ризиків, що дозволяють прогнозувати можливі загрози та розробляти заходи для їх запобігання.

Великі підприємства для ефективної обробки цього процесу повинні мати систему, яка буде мати можливість електронно обслуговувати процеси збору та актуалізації інформаційних активів за допомогою розроблених стандартизованих даних з урахуванням

сучасних можливостей інтеграцій зі штучним інтелектом. Зв’язок зі штучним інтелектом дасть можливість аналітикам, інформаційній безпеці та бізнес-власникам інформації економити свій час для заповнення і скорочувати загальні терміни процесу.

Область застосування процесів інвентаризації критичної інформації є важливою для великих підприємства. Ось декілька основних галузей, де цей процес важливий:

– Банки, інвестиційні компанії та інші фінансові установи використовують інвентаризацію для захисту конфіденційної інформації клієнтів, регуляторних даних та фінансової звітності.

– Лікарні, клініки та фармацевтичні компанії інвентаризують медичні записи пацієнтів, результати досліджень та інші чутливі дані для забезпечення їх конфіденційності та безпеки.

– Державні установи використовують інвентаризацію для захисту персональних даних громадян, інформації національної безпеки та інших критично важливих даних.

– Енергетичні компанії інвентаризують дані про виробництво, передачу та розподіл енергії для забезпечення стабільності енергосистеми та захисту від кібератак.

– Виробничі підприємства інвентаризують дані про проекти, процеси, обладнання та інтелектуальну власність для підвищення ефективності виробництва та захисту ноу-хау.

– Роздрібні компанії інвентаризують дані про клієнтів, продажі, інвентар та логістику для оптимізації бізнес-процесів та персоналізації маркетингових кампаній.

– ІТ-компанії та оператори зв'язку інвентаризують дані про клієнтів, мережі, програмне забезпечення та інфраструктуру для забезпечення безперебійної роботи систем та захисту від кібератак.

– Ключові аспекти інвентаризації критичної інформації:

– Визначення типів даних, їхнього значення для бізнесу та рівня конфіденційності.

– Визначення місцезнаходження даних (на серверах, у хмарі, на локальних пристроях).

– Аналіз потенційних ризиків, пов'язаних із даними.

Методи дослідження.

Дослідження базується на комбінації програмних та інженерних методів, спрямованих на досягнення поставлених завдань. В роботі використовуються методи оптимізації процесу. Сервісно-орієнтований підхід використовується для розробки інструментальних засобів вирішення поставлених задач.

Наукова новизна.

Розроблено модель та вдосконалені алгоритми реалізації процесу для програмного забезпечення, яке дозволить централізувати обробку даних, автоматизувати процес та ефективніше використовувати ресурси компанії з урахуванням вимог інформаційної безпеки.

Практичне значення отриманих результатів.

Полягає в розробці програмного додатку у якому будуть працювати користувачі, власники інформації та інформаційна безпека. Система дозволить вирішити проблеми, виявлені при аналізі процесу.

Апробація отриманих результатів: Основні положення та результати доповідалися і обговорювалися на міжнародній науково-технічній конференції «MININGMETALTECH 2024 – The mining and metals sector: integration of business, technology and education» та Міжнародної науково-практичної інтернет-конференції «Development of Education, Science and Business: Results 2024», 28 - 29 листопада 2024 року в ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА».

РОЗДІЛ 1. АНАЛІЗ СТАНУ ПИТАННЯ ТА КОНЦЕПЦІЙ, ПОВ'ЯЗАНИХ З ПРОЦЕСОМ ІНВЕНТАРИЗАЦІЇ КРИТИЧНИХ ДАНИХ НА ПІДПРИЄМСТВАХ

1.1 Аналіз предметної області, сучасних принципів моделювання.

Конфіденційна інформація - це інформація, яка має високу цінність для організації або особи та потребує захисту від несанкціонованого доступу, порушення або втрати. Конфіденційна інформація може включати особисті дані, фінансові дані, таємниці, інтелектуальну власність тощо.

Захист конфіденційної інформації описується різними законами України, залежно від типу, джерела та сфери застосування такої інформації. Ось деякі з них:

– Закон України “Про інформацію” [9] - це загальний закон, який визначає правові, організаційні та економічні засади діяльності у сфері інформації, а також права, обов’язки та відповідальність суб’єктів інформаційних відносин. Цей закон також встановлює поняття та види конфіденційної інформації, її режими доступу та захисту.

– Закон України “Про захист персональних даних” [11] - це спеціальний закон, який регулює відносини, що виникають у зв’язку з обробкою персональних даних фізичних осіб, а також визначає права, обов’язки та відповідальність суб’єктів відносин у сфері захисту персональних даних. Цей закон також встановлює поняття та принципи обробки персональних даних, їхні категорії та рівні захисту.

– Закон України “Про доступ до публічної інформації” [10] - це інший спеціальний закон, який регулює відносини, що виникають у зв’язку з реалізацією права на доступ до публічної інформації, яка знаходиться у володінні суб’єктів владних повноважень, а також інших

розпорядників публічної інформації. Цей закон також встановлює поняття та види публічної інформації, її режими доступу та обмеження.

Конфіденційна інформація поряд з службовою та таємною належить до інформації з обмеженим доступом.

Відповідно до п.2 ст. 21 Закону України «Про інформацію» «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом».

Відповідно до ст. 505 Цивільного Кодексу України «Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію».

Відповідно до ст. 506 Цивільного Кодексу України:

– Майновими правами інтелектуальної власності на комерційну таємницю є:

a) право на використання комерційної таємниці;

b) виключне право дозволяти використання комерційної таємниці;

c) виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;

d) інші майнові права інтелектуальної власності, встановлені законом.

– Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка законно визначила інформацію комерційною таємницею, якщо інше не встановлено договором».

Відповідно до ст. 36 господарського Кодексу України «відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону».

Також є стандарти ISO та NIST [4-5] надають рекомендації та вимоги для управління ризиками, пов’язаними з конфіденційною інформацією, та встановлення ефективних контролів для її захисту. Ось деякі приклади таких стандартів:

– ISO/IEC 27001:2022 - це міжнародний стандарт для систем управління інформаційною безпекою (ISMS). Він визначає вимоги, яким повинна відповідати ISMS. Стандарт ISO/IEC 27001 надає організаціям будь-якого розміру та з усіх сфер діяльності керівництво щодо встановлення, впровадження, підтримки та постійного вдосконалення ISMS.

– NIST Cybersecurity Framework - це гнучкий і добровільний фреймворк для управління кібербезпекою, розроблений Національним інститутом стандартів і технологій (NIST). Він допомагає організаціям краще розуміти свої кібер-ризики, визначати свої цілі та пріоритети, вибирати відповідні заходи безпеки та вимірювати свій прогрес.

Процес інвентаризації конфіденційної інформації описує стандарт ISO/IEC 27001:2022, який вимагає від організацій визначати та класифікувати свої активи інформаційної безпеки, включаючи

конфіденційну інформацію. Цей стандарт також надає рекомендації щодо встановлення відповідальності за активи, розробки політики захисту інформації та проведення регулярних оцінок ризиків.

Інвентаризація конфіденційної інформації допомагає організаціям ідентифікувати та захистити свої цінні дані, запобігти втраті, порушенню або крадіжці інформації, а також дотримуватися вимог законодавства та нормативів.

Інвентаризація конфіденційної інформації може включати такі етапи:

– Визначення мети, обсягу та критеріїв інвентаризації.

– Збір інформації про існуючі активи, їхнє розташування, власників, користувачів, характеристики, стан та вартість.

– Аналіз інформації за допомогою методів класифікації, категоризації, оцінки та пріоритетів.

– Документування результатів інвентаризації у вигляді звітів, таблиць, діаграм, баз даних тощо.

– Оновлення інформації про активи в разі зміни їхнього стану, власності, розташування або інших параметрів.

Інвентаризація конфіденційної інформації є важливим та необхідним процесом для підприємства, тому що:

– Вона допомагає ідентифікувати та захистити цінні дані, які можуть бути використані конкурентами, зловмисниками або шахраями для завдання шкоди підприємству;

– Вона допомагає запобігати втраті, порушенню або крадіжці інформації, яка може призвести до репутаційних, фінансових, правових або інших наслідків;

– Вона допомагає дотримуватися вимог законодавства та нормативів, які регулюють захист конфіденційної інформації, а також уникати штрафів, санкцій або позовів;

– Вона допомагає встановити відповідальність за активи, розробити політику захисту інформації та проводити регулярні оцінки ризиків.

Інвентаризація конфіденційної інформації є одним з елементів системи управління інформаційною безпекою (ISMS), яка рекомендується міжнародним стандартом ISO/IEC 27001:2022. Цей стандарт також надає керівництво щодо встановлення, впровадження, підтримки та постійного вдосконалення ISMS.

Моделювання інвентаризації конфіденційної інформації - це процес створення та використання математичних, логічних або комп'ютерних моделей для аналізу, планування, управління та оптимізації процесу інвентаризації конфіденційної інформації. Сучасні принципи моделювання інвентаризації конфіденційної інформації можуть включати такі:

– Використання інтегрованих інформаційних систем, які дозволяють автоматизувати та координувати процеси збору, обробки, зберігання, передачі та використання конфіденційної інформації між різними суб'єктами інформаційних відносин;

– Використання сучасних методів та засобів захисту конфіденційної інформації від несанкціонованого доступу [15], порушення, втрати або знищення, таких як криптографія, біометрія, стеганографія, цифровий підпис, блокчейн тощо;

– Використання сучасних методів та засобів аналізу та оцінки ризиків, пов'язаних з конфіденційною інформацією, таких як експертні системи, нейронні мережі, нечітка логіка, аналітична ієрархія, дерева рішень тощо

– Використання сучасних методів та засобів планування та оптимізації процесу інвентаризації конфіденційної інформації, таких як

лінійне програмування, динамічне програмування, генетичні алгоритми, штучні мурашники, методи імітаційного моделювання тощо.

1.2 Проблематика в процесі інвентаризації на підприємстві

Процес у середовищі підприємства, яке ми аналізували, функціонує та ілюстровано на рисунку 1.1.

Даний процес формуються та обслуговуються у окремих excel файлах та узгоджуються через електронну пошту.

Виявлені проблеми в процесі:

– Відсутність актуального єдиного переліку інформації інформаційних активів та переліку ризиків, які є у наявності у великій кількості окремих файлів. При формування у ручному режимі спільного файлу, є необхідність і його підтримувати в актуальному стані після зміни будь-якого окремого;

– Несистемність частини записів, які ведуться у формах процесу, що породжує складність роботи з масивами даних;

– Формування запитів на періодичну актуалізацію у ручному режимі;

– Необхідність порівняння даних в пошті та окремих файлах при питаннях перевірки цілісності даних.

Якщо підсумувати проблеми: процеси обслуговуються повністю у ручному режимі із не системним підходом до збору та затвердження даних

Об’єктом дослідження є способи та технологічні рішення, які допоможуть підвищити ефективність розглянутих процесів при зниженні ресурсів на обслуговування.

Рисунок 1.1 – Схема процесу інвентаризації конфіденційної інформації

1.3 Аналіз сучасних інформаційних технологій, технологій та засобів розробки програмного забезпечення, методів оптимізації, систем цифрового інтелекту і т. п. стосовно завдання роботи

Проведено пошук та аналіз наявних готових систем, які мають відношення до процесу інвентаризації конфіденційної інформації, результати у таблиці 1.1 та 1.2.

Таблиця 1.1 – Результати аналізу українських систем інвентаризації інформації

Назва	Опис
Система інвентаризації та обліку документів (СІОД)	Програмний продукт, який дозволяє автоматизувати процеси створення, обліку, зберігання, пошуку, видачі та знищення документів, що містять конфіденційну інформацію, що є власністю держави. Дана система розроблена компанією Баланс-Сервіс, яка займається розробкою та впровадженням програмних продуктів для автоматизації діяльності державних органів, банків, підприємств та організацій.
Система управління конфіденційною інформацією (СУКІ)	Комплексне рішення, яке допомагає організувати ефективне управління конфіденційною інформацією в установі. СУКІ включає модулі для класифікації, інвентаризації, обліку, зберігання, передачі, використання та знищення конфіденційної інформації, а також модулі для аудиту, моніторингу, аналізу та звітності. Дана система розроблена компанією Інформаційні технології, яка спеціалізується на розробці та впровадженні комплексних рішень для захисту інформації, документообігу, архівування, електронного підпису та інших сфер.

Продовження таблиці 1.1

Назва	Опис
Система інвентаризації та захисту конфіденційної інформації (СІЗКІ)	Інтегроване рішення, яке поєднує функції інвентаризації та захисту конфіденційної інформації в одній системі. СІЗКІ дозволяє автоматично виявляти, класифікувати, інвентаризувати, захищати, контролювати та знищувати конфіденційну інформацію на різних носіях, включаючи паперові документи, електронні файли, електронну пошту, бази даних, веб-сайти тощо. Система розроблена компанією Софтлайн.

Варто відмітити, що точної інформації щодо можливостей та архітектури даних систем на сайтах розробників не багато, що свідчить про можливу адаптацію процесів і розробку «під ключ» для кожного підприємства індивідуально.

Таблиця 1.2 – Результати аналізу іноземних систем інвентаризації інформації

Назва	Опис
Microsoft Information Protection (MIP)	Рішення, яке дозволяє класифікувати, маркувати, захищати, виявляти та контролювати конфіденційну інформацію на різних платформах, пристроях і сервісах
Amazon Macie	Рішення, яке використовує машинне навчання та штучний інтелект для виявлення, інвентаризації, класифікації та захисту конфіденційної інформації, яка зберігається в хмарному сховищі Amazon S32

Продовження таблиці 1.2

Назва	Опис
Forcepoint Data Loss Prevention (DLP)	Рішення, яке допомагає запобігати витоку конфіденційної інформації з підприємства шляхом виявлення, ідентифікації, класифікації, блокування та шифрування даних на різних каналах передачі
Symantec Data Loss Prevention (DLP)	Рішення, яке також дозволяє захищати конфіденційну інформацію від несанкціонованого доступу, копіювання, передачі або видалення, шляхом використання різних технологій, таких як аналіз змісту, шифрування, карантин, аудит та звітність
IBM Data Risk Manager	Рішення, яке допомагає оцінювати, мінімізувати та управляти ризиками, пов’язаними з конфіденційною інформацією. IBM Data Risk Manager використовує аналітику, штучний інтелект та автоматизацію для виявлення, класифікації, інвентаризації та захисту конфіденційної інформації в різних джерелах даних
Google Cloud Data Loss Prevention (DLP)	Рішення, яке дозволяє виявляти, ідентифікувати, маскувати та захищати конфіденційну інформацію, яка зберігається, обробляється або передається в хмарному середовищі Google Cloud. Google Cloud DLP використовує передбачувані та налаштовані детектори, щоб розпізнавати та класифікувати конфіденційну інформацію, таку як особисті дані, фінансова інформація, медичні записи тощо

Продовження таблиці 1.2

Назва	Опис
McAfee Total Protection for Data Loss Prevention (DLP)	Рішення, яке допомагає запобігати втраті, крадіжці або витоку конфіденційної інформації з підприємства. McAfee Total Protection for DLP включає модулі для захисту даних на робочих станціях, мережах, хмарних сервісах та зовнішніх носіях. McAfee Total Protection for DLP використовує різні методи для виявлення, класифікації, шифрування, блокування та звітності про конфіденційну інформацію

Усі запропоновані рішення є постійними членами Gartner у своїх нішах та мають відповідне призначення та ефективність але і високу вартість та необхідність знань у інтеграції, яка залежить від обраної архітектури.

Архітектура, яка наявна у середовищі, де проводився аналіз, має велику кількість інформаційних систем для збереження і обробки даних, а саме:

– Microsoft Office365 Enterprise із сервісами Exchange, Azure (blob storage та інші), OneDrive, Sharepoint Online, Dynamics, тощо.

– Програмний комплекс SAP ERP із рядом хмарних рішень по типу SAP ARIBA, SAP CPQ\C4C, SAP Success Factors;

– Середовища баз даних Microsoft SQL та Oracle із інформаційними системами;

– ПК та сервери із сховищами даних (мережеві папки).

Великий перелік систем практично унеможливлює вибір одного комплексного рішення щодо автоматичного збору даних у кожному з місць зберігання. Можливо розділити та структурувати дані у дві великі групи:

– Бази даних;

– Документи, які формуються з інформаційних систем на кінцеву робочу станцію користувача.

Базуючись на цих двох групах та наявній архітектурі, найбільш ефективно використовувати клас рішення Microsoft Information Protection (MIP), яки допоможе виявляти, класифікувати та автоматично інвентаризувати інформацію у місцях зберігання.

Модель MIP [3] базується на підходах, які ілюстровано на рисунку 1.2.

Модель інвентаризації інформації, що розглядається, знаходиться на етапі «Know your data», який залежить від наступних понять:

– Типи конфіденційної інформації - визначення конфіденційних даних за допомогою вбудованих або користувальницьких регулярних виразів, формул або функцій. Дане поняття має два розгалуження:

a) Стандартні типи, які надаються розробником. Даний тип має недоліки, так як західні розробники не дуже знайомі з конфіденційними поняттями та типами України або цього регіону і погано працюють із кирилицею;

b) Створювані типи, ті, які створюються аналітиком на базі даних процесу конфіденційної інформації. Власник каже те, що для нього є критичним і саме це є основою для створюваних типів.

– Класифікатори, що можуть навчатися - визначення конфіденційних даних за допомогою використання прикладів даних і машинного навчання. Дане поняття залежні від ідентифікації місця зберігання та бажання власників інформації постійно розміщувати там свіжі прикладі інформації. Машинне навчання оброблює дані та створює свої класифікатори. Варто відмітити, що є певні проблеми із обробкою даних з кирилицею та неможливість робити ручні покращення класифікаторів якщо виявляється їх неефективність (хибно-позитивні спрацьовування).

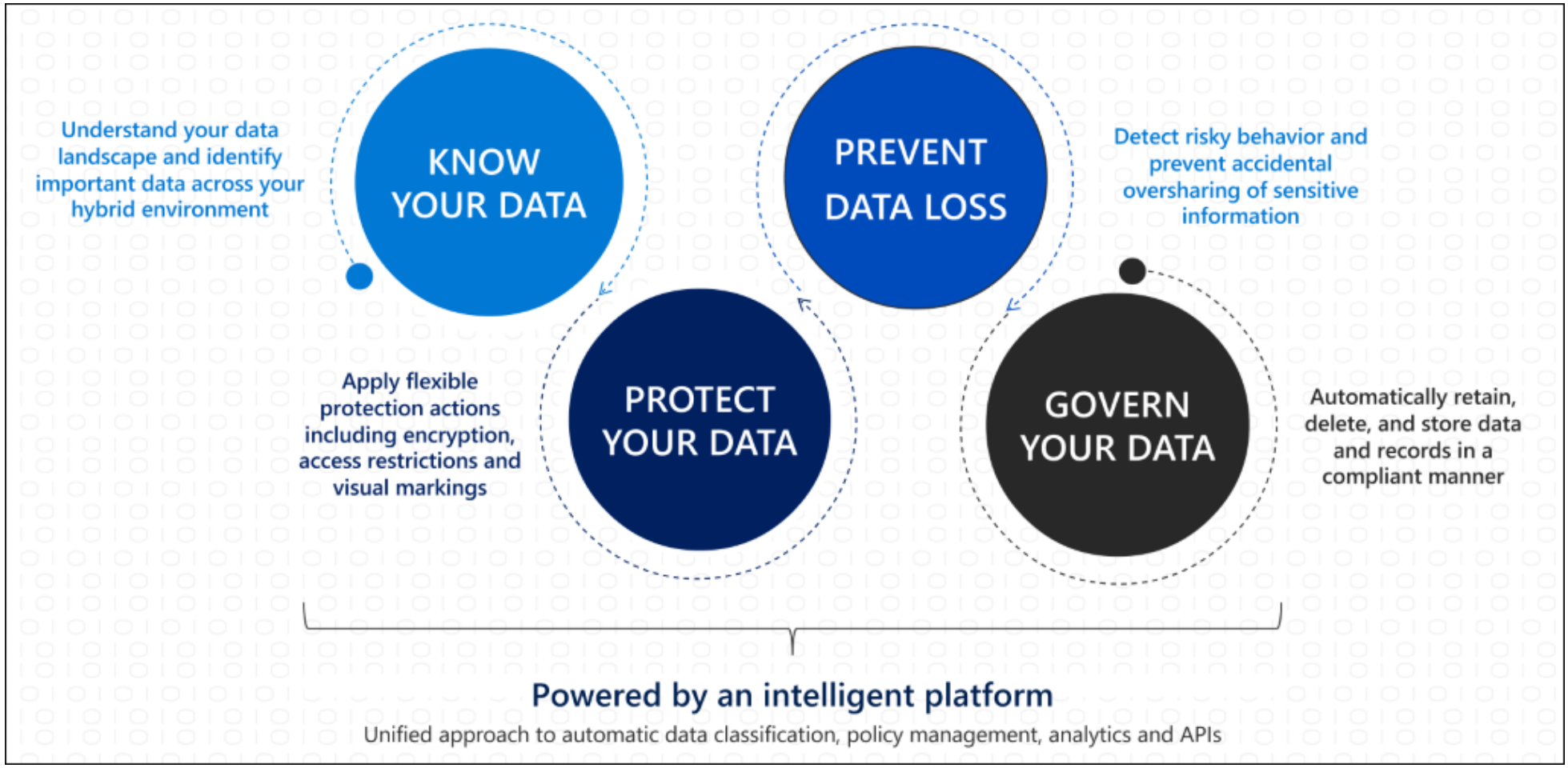


Рисунок 1.2 – Модель захисту даних

– Класифікація даних - графічна ідентифікація елементів в організації, помічених міткою конфіденційності. Дане поняття залежить тільки від власників даних та користувачів, які зможуть маркувати самостійно свої конфіденційні дані. Є негативні сторони такого поняття, яке:

a) Помилки користувачів, які не знають або переоцінюють\недооцінюють свої дані;

b) Небажання користувачів виконувати свої обов’язки.

Усе це стосується до організаційних підходів обробки даних та має неперервне та постійне покращення, потребує періодичного навчання та аналізу помилок.

Як висновок, дана система MIP допоможе автоматизувати інвентаризацію інформації у кінцевих системах але потребує знань по джерелу класифікаторів. Таке джерело можливо мати із процесу інвентаризації конфіденційної інформації, яка виконується у ручному режимі у середовищі, яке аналізувалося. Дослідження буде стосуватися технологій і методів, які зможуть покращити ефективність процесу, знизити трудовитрати на обслуговування та вивільнити час аналітиків та власників даних на більш важливі процеси.

1.4 Розробка пропозицій для автоматизації процесу інвентаризації конфіденційної інформації на підприємстві

Пропонується розробити систему, яка буде автоматизувати більшість процесів, які зараз виконуються у ручному режимі не уніфіковано. Система повинна враховувати процеси, які ілюстровані на BPMN діаграмі на рисунку 1.3 та рисунку 1.4.

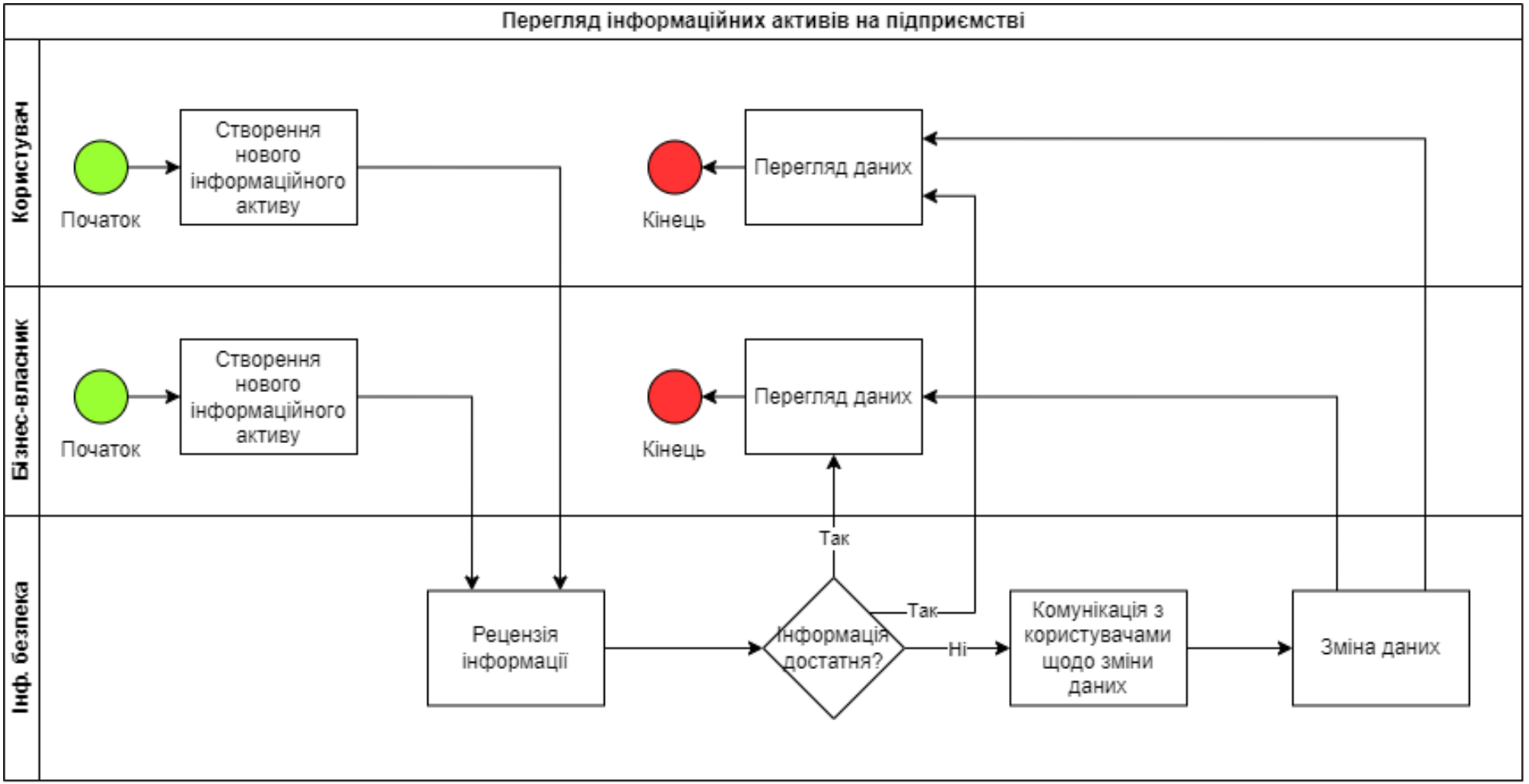


Рисунок 1.3 – BPMN діаграма по процесу ознайомлення за критичними даними

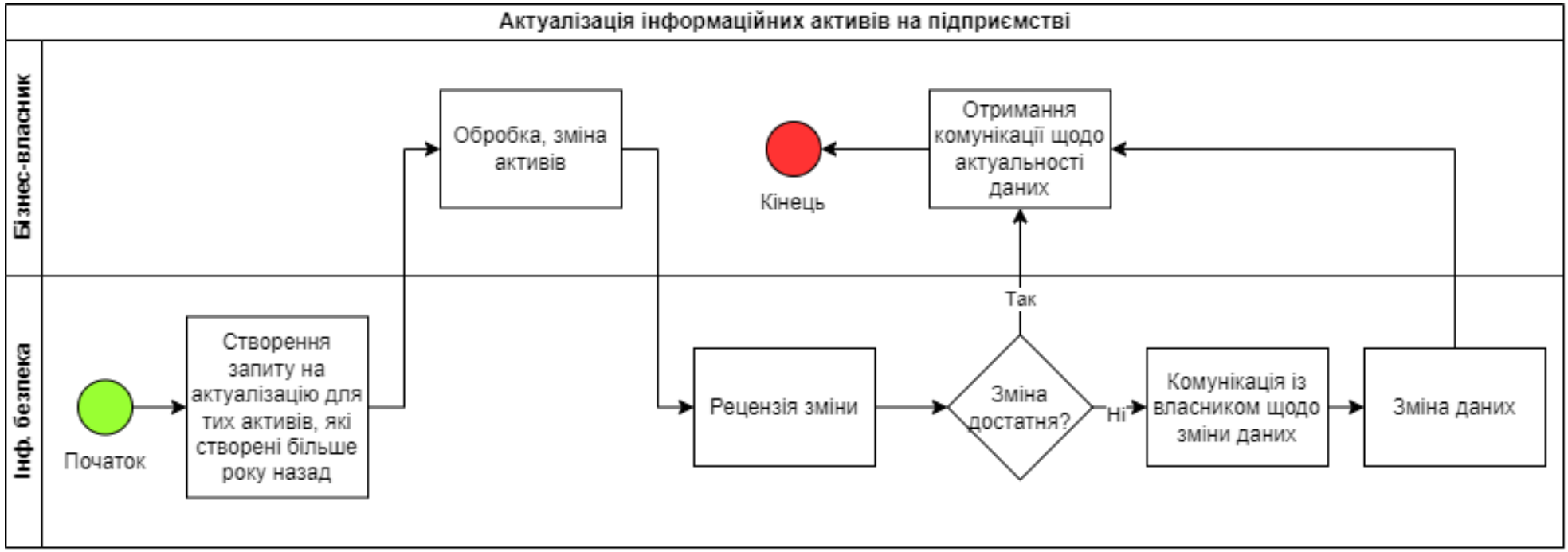


Рисунок 1.4 – BPMN діаграма по процесу актуалізації критичних даних

РОЗДІЛ 2. АНАЛІЗ СТАНУ БІЗНЕС-ПРОЦЕСІВ, ПРОЦЕСІВ ОБРОБКИ ДАНИХ ТА БІЗНЕС-ВИМОГИ

2.1 Наявний процес

Провівши діалог із представниками бізнес-користувачів на підприємстві, було сформовані бізнес вимоги для розробки можливої системи, яка покращить процес інвентаризації. Є процес інвентаризації конфіденційної інформації, який на зараз оброблюється наступним чином:

2.1.1 Виконання ініціації та узгодження процесу;

2.1.2 Формується відомість в Excel;

2.1.3 Вноситься пропозиція щодо назв інформаційних активів у відомість згідно бізнес-направлення;

2.1.4 Бізнес доповнює пропозицію, коригує;

2.1.5 Вносить назви бізнес-процесів до інф. активів;

2.1.6 Вносить наявність персональних даних;

2.1.7 Вносить легітимних користувачів;

2.1.8 Вносить системи в яких є такі інформаційні активи;

2.1.9 Надає приклади таких активів;

2.1.10 Узгоджує відомість.

2.2 Проблеми в процесі

2.2.1 Відсутність актуального єдиного переліку інформації інформаційних активів, які є у наявності у великій кількості окремих файлів. При формування у ручному режимі спільного файлу, є необхідність і його підтримувати в актуальному стані після зміни будь-якого окремого;

2.2.2 Не системність частини записів, які ведуться у формах процесу, що породжує складність роботи з масивами даних;

2.2.3 Формування запитів на періодичну актуалізацію у ручному режимі;

2.2.4 Необхідність порівняння даних в пошті та окремих файлах при питаннях перевірки цілісності даних.

2.3 Припущення щодо системи

2.3.1 Система забезпечить централізоване зберігання всіх інформаційних активів, що дозволить уникнути розпорошеності даних по різних файлах;

2.3.2 Процеси інвентаризації будуть автоматизовані, зокрема актуалізація даних.

2.3.3 Система впровадить стандартизовані форми для записів, щоб забезпечити консистентність та полегшити роботу з масивами даних.

2.3.4 Система буде регулярно оновлювати дані, використовуючи заплановані процедури, щоб забезпечити їх актуальність.

2.3.5 Система буде розроблена з урахуванням вимог безпеки, щоб забезпечити конфіденційність та захист інформаційних активів.

2.3.6 Система буде доступна для всіх легітимних користувачів з різних бізнес-підрозділів, забезпечуючи їм необхідні інструменти для роботи з інформаційними активами.

2.3.7 Система буде спроектована таким чином, щоб бути гнучкою та скальованою для майбутнього розширення та інтеграції з іншими системами.

2.4 Залежності для системи

2.4.1 Система повинна бути сумісною з існуючим IT-інфраструктурою компанії для забезпечення безперебійної інтеграції.

2.4.2 Успішне впровадження системи залежить від залучення та підтримки ключових користувачів бізнес-процесів.

2.4.3 Система має відповідати всім законодавчим та нормативним вимогам щодо обробки та зберігання конфіденційної інформації.

2.4.4 Розробка та впровадження системи залежать від встановлення ефективних заходів безпеки для захисту інформаційних активів.

2.4.5 Потрібно врахувати можливість інтеграції з іншими системами, які вже використовуються в компанії.

2.4.6 Реалізація системи залежить від забезпечення необхідного бюджету та ресурсів для розробки та підтримки.

2.5 Обмеження для системи:

2.5.1 Система повинна бути розроблена з урахуванням існуючих технічних можливостей компанії та не повинна вимагати значних змін в IT-інфраструктурі.

2.5.2 Розробка системи має відбуватися в межах затвердженого бюджету, без додаткових витрат.

2.5.3 Система має бути розроблена та впроваджена в строго визначені терміни.

2.5.4 Система має відповідати всім відповідним законодавчим та нормативним актам, особливо в частині захисту персональних даних.

2.5.5 Доступ до системи має бути строго регульованим та обмеженим для неавторизованих користувачів.

2.5.6 Система має бути сумісною з іншими програмними продуктами, які вже використовуються в компанії.

2.5.7 Система має бути готова до масштабування в майбутньому, але на початковому етапі не повинна мати надмірних можливостей, які не будуть використовуватися.

2.5.8 Інтерфейс користувача має бути інтуїтивно зрозумілим та не вимагати додаткового навчання для основних операцій.

2.6 В межах проєкту

2.6.1 Створення єдиної бази даних для зберігання всіх інформаційних активів та пов'язаних з ними даних.

2.6.2 Розробка функціоналу для автоматизації процесу перегляду даних відомостей.

2.6.3 Розробка зручного та інтуїтивно зрозумілого користувацького інтерфейсу для взаємодії з системою.

2.6.4 Створення інструментів для генерації звітів за різними параметрами, що дозволить легко аналізувати дані.

2.6.5 Забезпечення можливості інтеграції нової системи з вже використовуваними програмними рішеннями в компанії.

2.6.6 Організація семінарів та тренінгів для користувачів для забезпечення ефективного використання системи.

2.7 За межами проєкту по розробці системи

2.7.1 Система не буде інтегрована з програмним забезпеченням або платформами, які не були визначені як частина проекту.

2.7.2 Система не забезпечує підтримку або сумісність зі сторонніми додатками, якщо це не було зазначено у вимогах.

2.7.3 Обробка та аналіз даних, які виконуються поза межами системи, не входять до обсягу цього проекту.

2.7.4 Проект не передбачає створення або управління фізичними носіями інформації.

2.7.5 Система не буде оптимізована для використання на особистих пристроях користувачів, якщо це не вказано у вимогах.

2.7.6 Система не буде автоматично оновлювати дані з зовнішніх джерел, якщо це не було включено до проектних вимог.

2.8 Вимоги бізнесу

Вимоги будуть розміщені згідно пріоритетам, що базуються на техніці MoSCoW, котра розділяє вимоги на наступні категорії, які наведено у таблиці 2.1 та 2.2.

Таблиця 2.1 – Опис методології оцінки MoSCoW

Рейтинг пріоритетів	Опис
Повинен мати (M – Must Have)	Описуються вимоги, що повинні бути задоволені у фінальному представлені рішення для досягнення успіху.
Варто було б мати (S – Should Have)	Представляє високо-пріоритетні деталі (пункти), що повинні бути добавлені у рішення, якщо це можливо. Дуже часто це вирішальні вимоги, проте кожен з них може бути задоволений інших шляхом, якщо суворо необхідно.
Можливо мати (C – Could Have)	Описуються вимоги, які вважаються бажаними, але не обов'язковими. Вони будуть включені, якщо дозволять час і ресурси.

Продовження таблиці 2.1

Рейтинг пріоритетів	Опис
Хотілося б мати (W – Won’t Have)	Представляє вимоги, які були погоджені зацікавленими сторонами , що не будуть додаватися до анонсування, проте можуть бути розглянуті у майбутньому.

Таблиця 2.2 – Вимоги

Посилання	Вимоги	Пріоритет
BR01	Централізована база даних для всіх інформаційних активів.	M
BR02	Інтуїтивно зрозумілий користувацький інтерфейс.	S
BR03	Підтримка та навчання користувачів системи.	S
BR04	Автоматизація актуалізації даних.	M
BR05	Автоматичне оновлення даних з зовнішніх джерел.	M
BR06	Використання технологій, які зможуть використовувати або інтегрувати Office365 з рішенням	M
BR07	Мінімально достатня ціна використання рішення (політика ліцензування), яке доступне без бюджетуванню окремих ліцензій.	M
BR08	Система повинна бути розробленою згідно вимог інформаційної безпеки замовника, які наведені у Додатку Б.	M

2.9 Моделювання бізнес-процесів

Проаналізувавши доступні бізнес-вимоги, розробимо наступні процеси та діаграми використання для них:

2.9.1 Процес створення нових інформаційних активів на підприємстві – процес, при якому користувач або бізнес-власник зможе створити новий критичний інформаційний актив, що обслуговується, для подальшої його інвентаризації та захисту. Діаграма використання процесу зображена на рисунку 2.1.

2.9.2 Процес актуалізації наявних інформаційних активів на підприємстві – процес, при якому бізнес-власник або відповідальна особа, якій делегували право актуалізації, зможе актуалізувати свої наявні інформаційні активи. Діаграма використання процесу зображена на рисунку 2.2.

2.9.3 Процес перегляду інформації про наявні критичні інформаційні активи на підприємстві – процес, при якому користувач зможе ознайомитись з тими даними, які є важливими для підприємства і прийняти рішення про обробку або передачу створеної або інформації, що оброблюється, запросити необхідне узгодження по необхідності у бізнес-власника даних. Діаграма використання процесу зображена на рисунку 2.3.

2.9.4 Процес консалтингу щодо наявного процесу інвентаризації – процес, при якому користувач або бізнес-власник може задати питання щодо наявного процесу інвентаризації критичної інформації та отримати на нього відповідь від відповідальної служби підтримки для підвищення обізнаності або коректного обслуговування процесів. Діаграма використання процесу зображена на рисунку 2.4;

2.9.5 Процес навчання щодо наявного процесу інвентаризації – процес, при якому користувач або бізнес-власник може отримати базове навчання щодо обслуговування наявного процесу інвентаризації

критичної інформації. Діаграма використання процесу зображена на рисунку 2.5.

Для більш детального моделювання процесів, розробимо діаграми активності, які зможуть розкрити деталі процесів та їх послідовності. Розроблені діаграми наведені на рисунках 2.6 – 2.10.

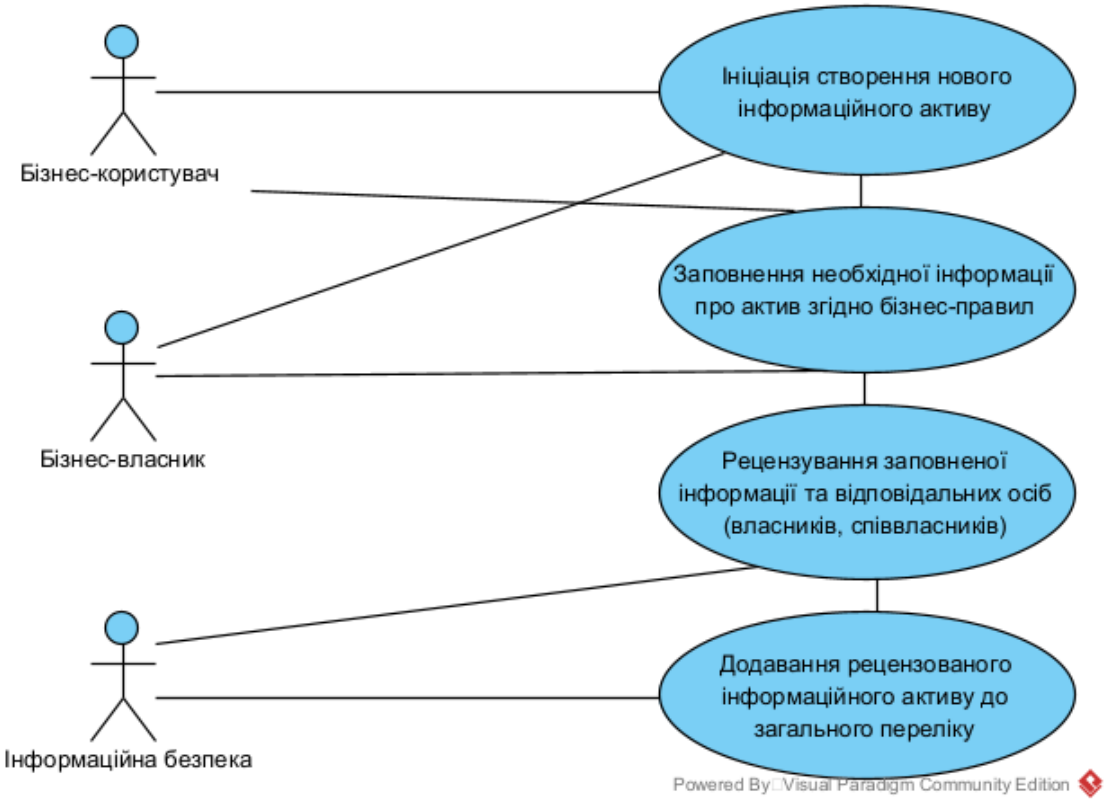


Рисунок 2.1 – Діаграма користування для процесу створення нових інформаційних активів на підприємстві

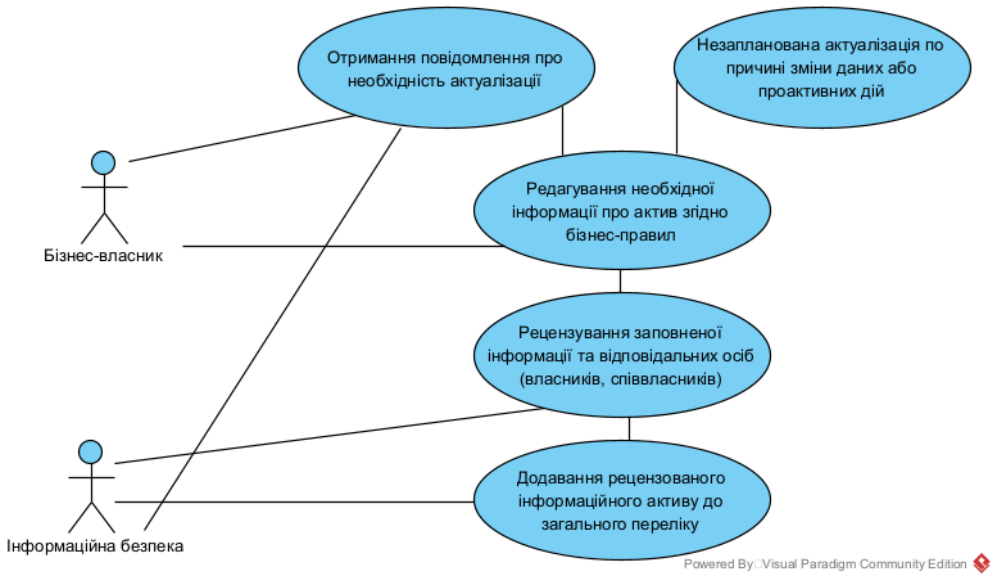


Рисунок 2.2 - Діаграма користування для процесу актуалізації наявних інформаційних активів на підприємстві

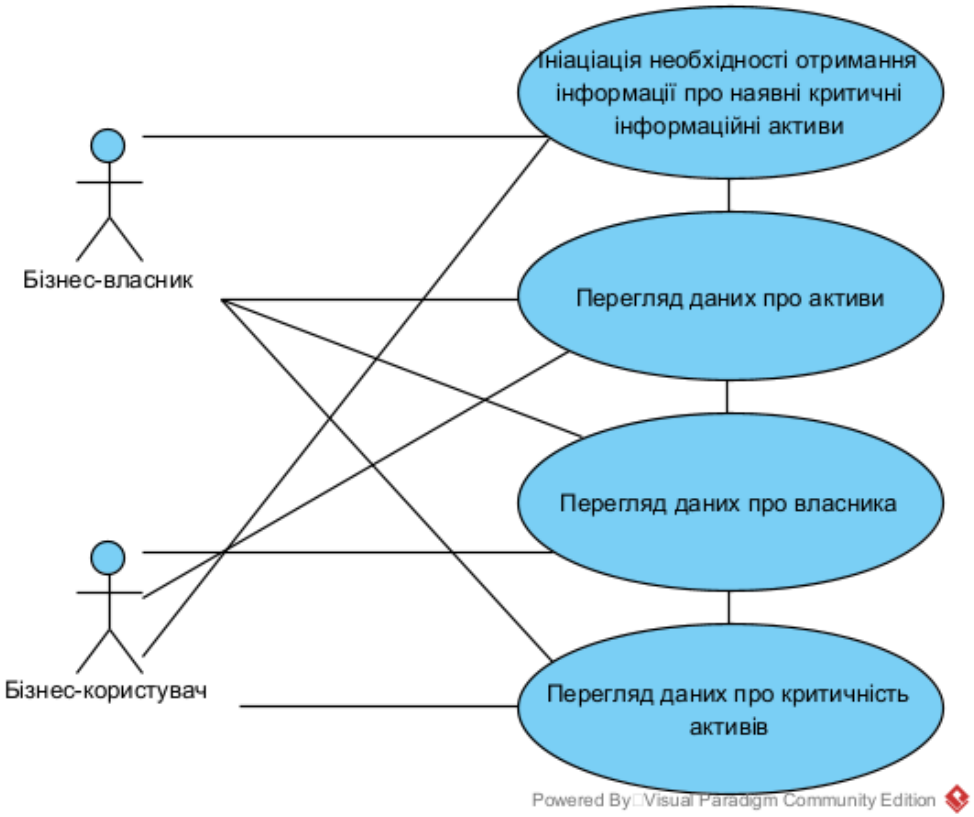


Рисунок 2.3 - Діаграма користування для процесу перегляду інформації про наявні критичні інформаційні активи на підприємстві

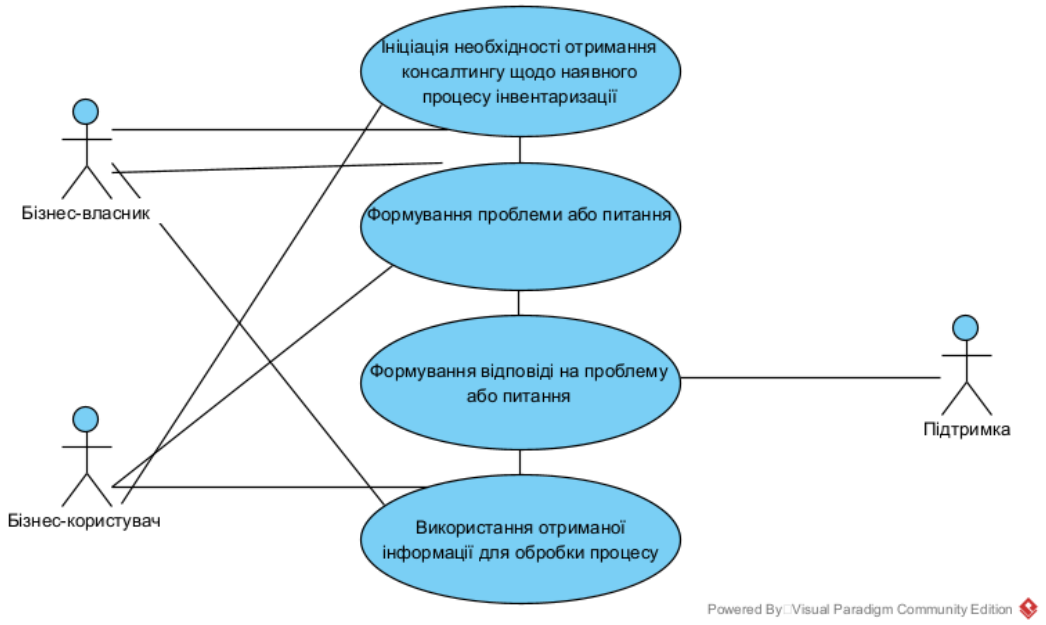


Рисунок 2.4 - Діаграма користування для процесу консалтингу щодо наявного процесу інвентаризації

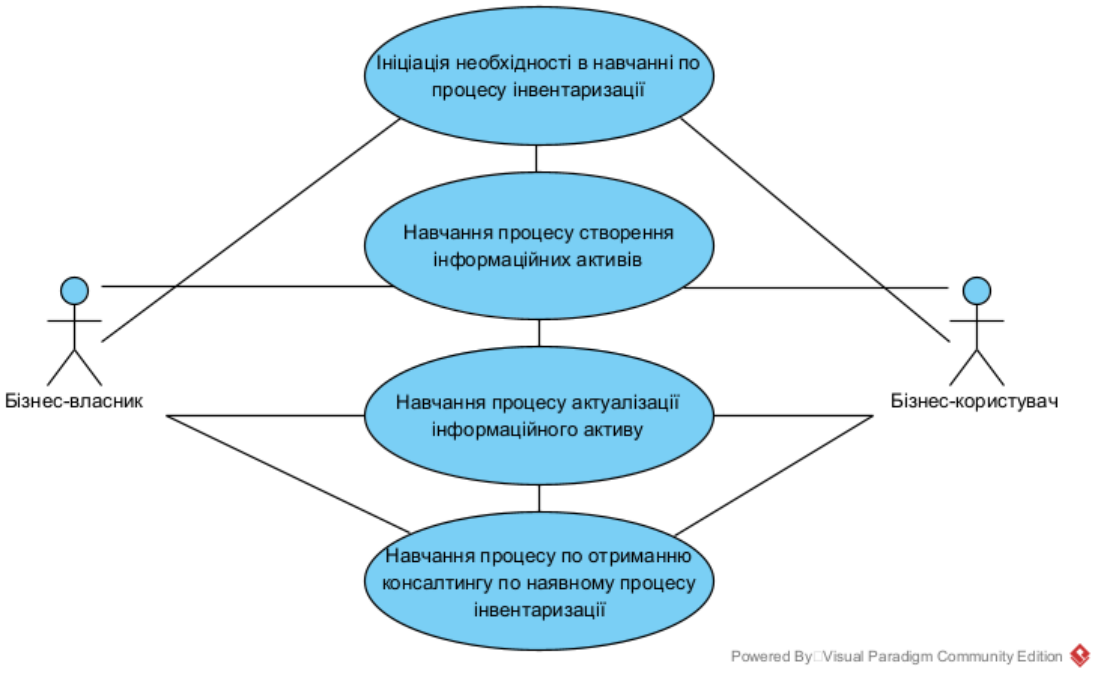


Рисунок 2.5 - Діаграма користування для процесу навчання щодо наявного процесу інвентаризації

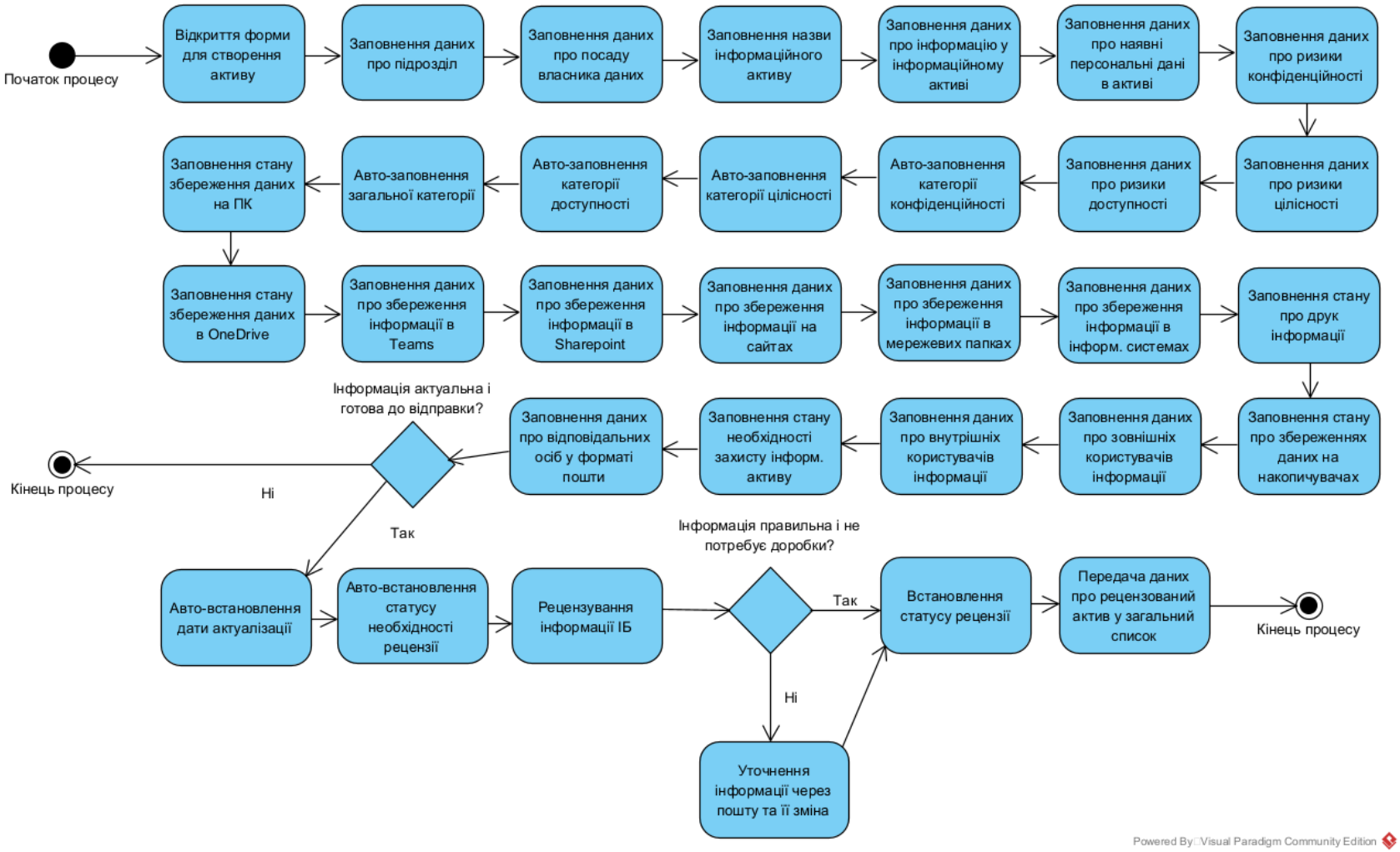


Рисунок 2.6 – Діаграма активності для процесу створення нових інформаційних активів на підприємстві

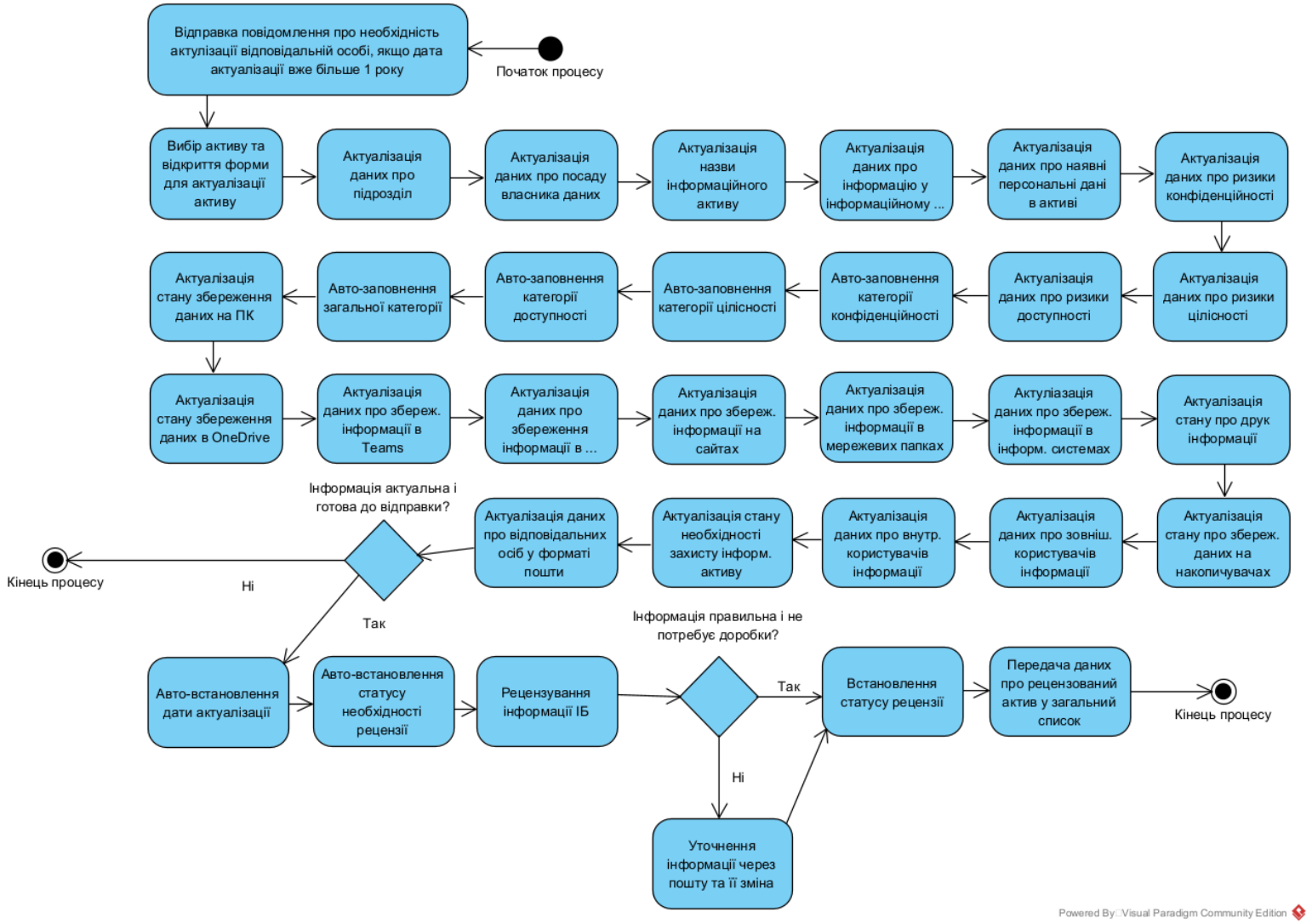


Рисунок 2.7 – Діаграма активності для процесу актуалізації наявних інформаційних активів на підприємстві

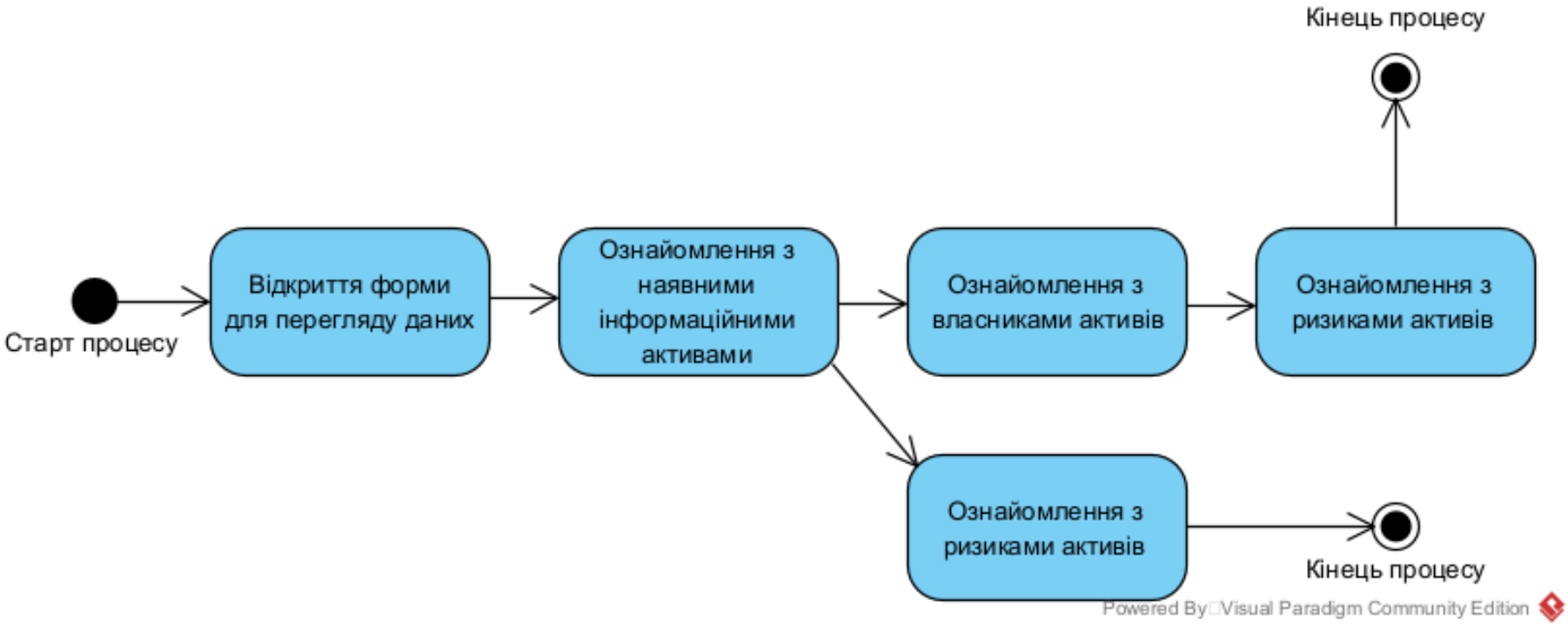


Рисунок 2.8 – Діаграма активності для процесу перегляду інформації про наявні критичні інформаційні активи на підприємстві

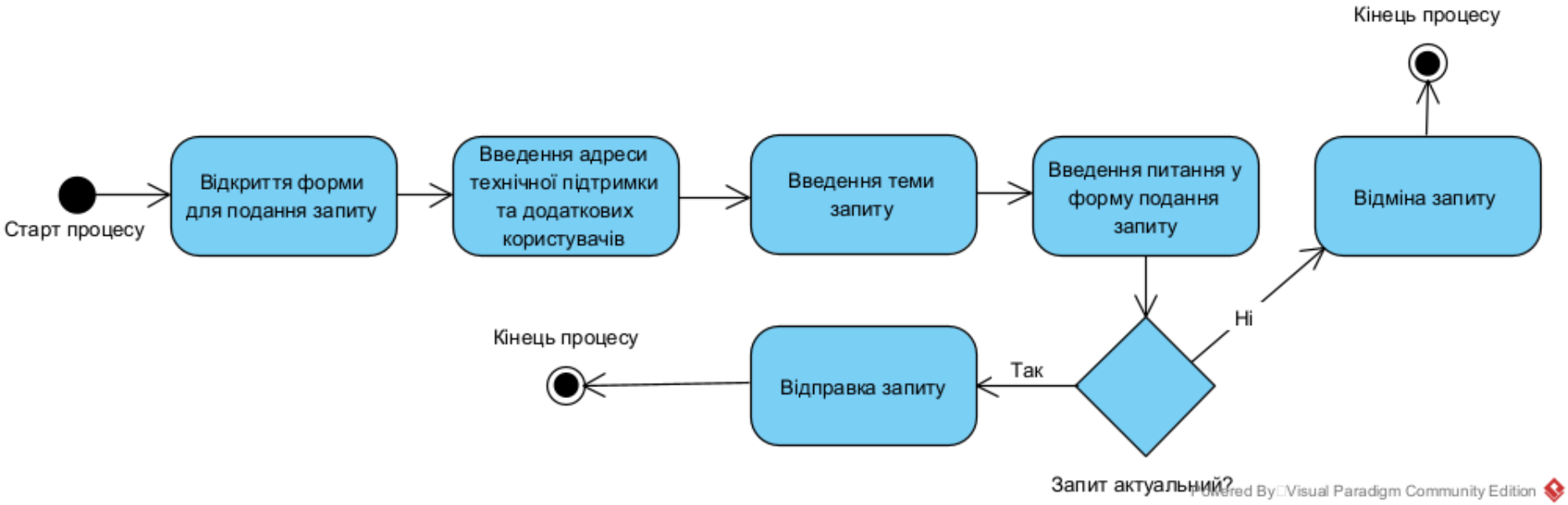


Рисунок 2.9 – Діаграма активності для процесу консалтингу щодо наявного процесу інвентаризації

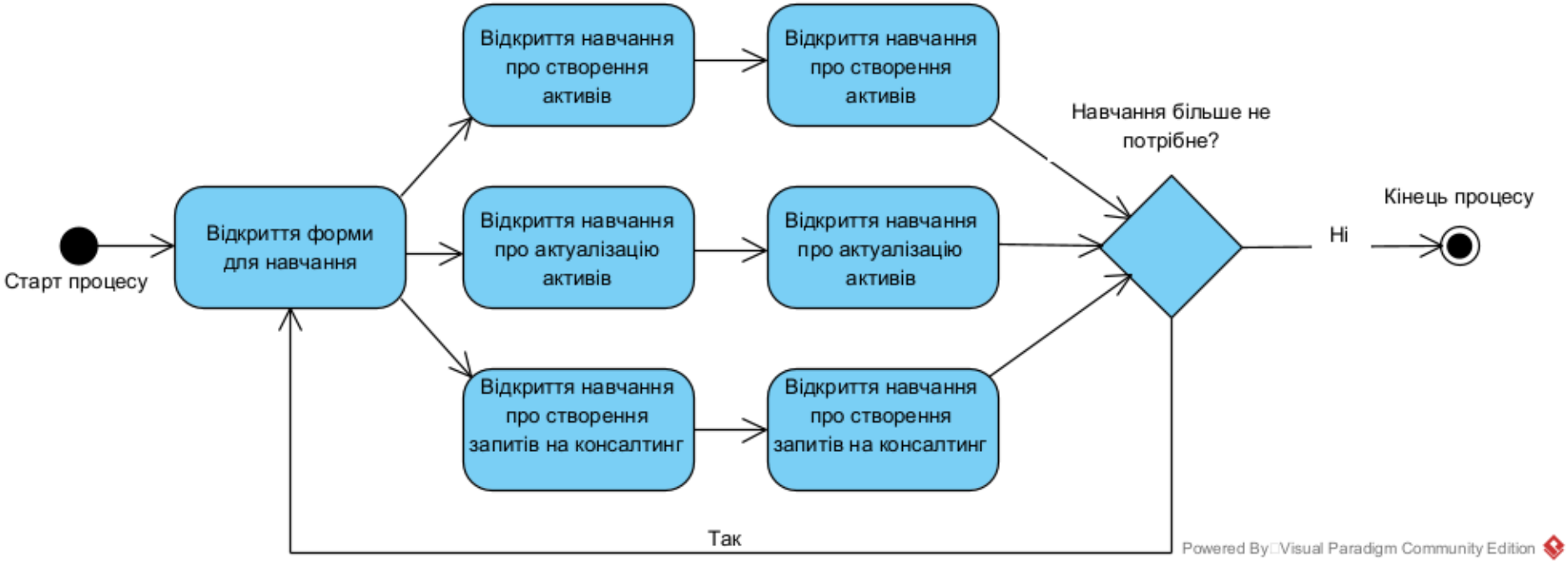


Рисунок 2.10 – Діаграма активності для процесу навчання щодо наявного процесу інвентаризації

На базі даних діаграм розроблений програмний додаток, який описаний у наступному розділі.

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Архітектура програмного забезпечення

Виконуючи вимогу BR06, BR07, розроблена наступна архітектура у наявному середовищі (рисунок 3.1).

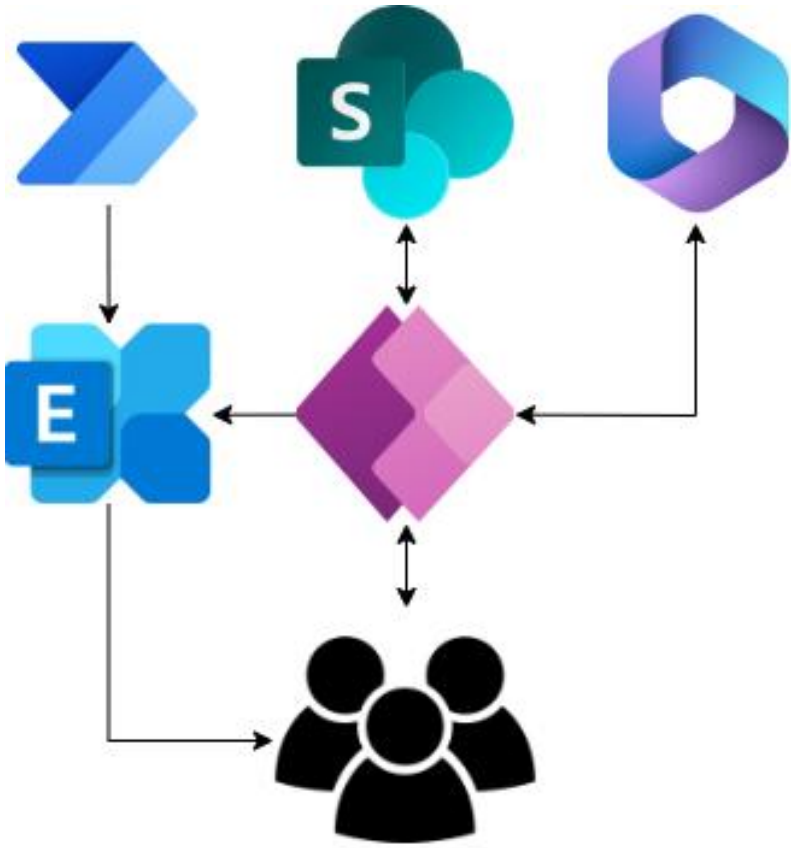


Рисунок 3.1 – Архітектура розроблюваного програмного забезпечення

Дана архітектура побудована на базі компонентів системи Office365, враховує наявні ліцензії клієнтів і за рахунок компонентів, які входять у наявні ліцензії [30], не додає додаткового бюджету для замовника. У таблиці 3.1 наданий опис використаних компонентів.

Таблиця 3.1 – Компоненти архітектури

Компонент	Опис
	Power Apps [18] — це набір програм, послуг і з'єднувачів, а також платформа даних, яка дозволяє швидко створювати користувацькі програми для ваших бізнес-потреб. Програми, створені за допомогою Power Apps, дозволяють використовувати широкі можливості бізнес-логіки для перетворення ручних бізнес-операцій на цифрові автоматизовані процеси. Power Apps «демократизує» процес створення бізнес-програм, тому для створення багатофункціональних налаштованих бізнес-програм користувачам не потрібно писати код. Power Apps також надає розширювану платформу, яка дозволяє професійним розробникам програмно взаємодіяти з даними та метаданими, застосовувати бізнес-логіку, створювати наштовані з'єднувачі та інтегруватись із зовнішніми даними.
	SharePoint Online - це хмарна служба, яка дозволяє організаціям створювати, керувати та обмінюватися вмістом, програмами та ресурсами між командами. SPO використовується як база даних для інформації, там створений Список Sharepoint [16] у якому зберігається інформація у табличному виді. Виконує вимогу BR01

Продовження таблиці 3.1

Компонент	Опис
	Office365 – хмарна платформа, в контексті програмного забезпечення використовується для вивантаження інформації про користувача, його посади, підрозділу, облікового запису і підприємства. Використовується в ПЗ для фільтрації даних по підприємству користувача або його облікового запису.
	Хмарний поштовий сервіс Office365 Exchange, який використовується для відправки поштових повідомлень від ПЗ або потоку автоматизації, який використовується для процесу актуалізації.
	Power Automate – це платформа від Microsoft, яка дозволяє автоматизувати робочі процеси та обмінюватися даними між різними додатками та службами. Використовується для автоматизації повідомлень про необхідність актуалізації інформації у ПЗ.
	Користувач ПЗ в Power Apps.

Дана архітектура визначена для розробки ПЗ в Power Apps, як дешевому аналогу розробки програмного забезпечення для економії часу та бюджету, оптимізації часу розробки та відсутності необхідності мати у штаті окрему позицію розробника.

3.2 Розробка бази даних для зберігання і обробки даних програмного забезпечення

Згідно бізнес-аналізу, бізнес-процес інвентаризації критичної інформації має велику кількість обов'язкових або необов'язкових атрибутів, також додані ті, які необхідні для функціонування ПЗ [19, 25]. Дані представлені у таблиці 3.2.

Таблиця 3.2 – Опис створеної бази даних в Sharepoint List

№	Атрибут	Бізнес-процес	Опис
1	Інформаційний актив актуальний? / Is the information asset relevant?	Наявний	Уточнення актуальності доданого інформаційного активу
2	Рецензія	Додано в ПЗ	Встановлення статусу необхідності рецензії інформаційної безпеки для доданого або зміненого інформаційного активу
3	Номер інформаційного активу / Information asset id	Наявний	Ідентифікаційний номер інформаційного активу
4	Дата актуалізації / Actualization date	Додано в ПЗ	Дата останньої актуалізації інформаційного активу
5	Підприємство / Company	Наявний	Підприємство-власник інформаційного активу
6	Підрозділ / Department	Наявний	Підрозділ-власник інформаційного активу
7	Власник активу / Owner of the asset	Наявний	Посада особи власника інформаційного активу

Продовження таблиці 3.2

№	Атрибут	Бізнес-процес	Опис
8	Назва інформ. активу / Name of the inf. asset	Наявний	Найменування інформаційного активу
9	Інформація / Information	Наявний	Інформація, яка оброблюється в інформаційному активі
10	Наявність персональних даних / Presence of PII	Наявний	Вказання наявності персональних даних в інформаційному активі
11	Вплив (конфіденційність) / Impact (privacy)	Наявний	Вибір ризику конфіденційності для інформаційного активу
12	Вплив (цілісність) \ Impact (integrity)	Наявний	Вибір ризику цілісності для інформаційного активу
13	Вплив (доступність) \ Impact (accessibility)	Наявний	Вибір ризику доступності для інформаційного активу
14	Категорія конфіденційності \ Category of privacy	Наявний	Ідентифікована категорія конфіденційності згідно обраних ризиків
15	Категорія цілісності \ Category of integrity	Наявний	Ідентифікована категорія цілісності згідно обраних ризиків
16	Категорія доступності \ Category of accessibility	Наявний	Ідентифікована категорія доступності згідно обраних ризиків

Продовження таблиці 3.2

№	Атрибут	Бізнес-процес	Опис
17	Загальна категорія \ Main category	Наявний	Ідентифікована категорія ризику інформаційного активу (максимальна серед конфіденційності, цілісності, доступності)
18	Зберігання на ПК / Storage on PC	Наявний	Вказання наявності обробки або зберігання даних на ПК
19	Зберігання в OneDrive / Storage on OneDrive	Наявний	Вказання наявності обробки або зберігання даних в OneDrive
20	Відправка по пошті / Sending by mail	Наявний	Вказання наявності обробки або зберігання даних у пошті
21	Зберігання в Teams / Storage on Teams	Наявний	Вказання наявності обробки або зберігання даних в Teams
22	Зберігання в Sharepoint / Storage on Sharepoint	Наявний	Вказання наявності обробки або зберігання даних в Sharepoint Online
23	Зберігання на сайтах \ Storage on sites	Наявний	Вказання наявності обробки або зберігання даних на сайтах або порталах

Продовження таблиці 3.2

№	Атрибут	Бізнес-процес	Опис
24	Зберіг. в мереж. папках / Storage on netw. folders	Наявний	Вказання наявності обробки або зберігання даних в мережевих папках
25	Зберігання в системах \ Storage on systems	Наявний	Вказання наявності обробки або зберігання даних в стандартизованих інформаційних системах
26	Зберігання в інш. системах / Storage in oth. syst.	Наявний	Вказання наявності обробки або зберігання даних в нестандартизованих інформаційних системах
27	Інформація друкується? / Information printing?	Наявний	Вказання наявності друку інформаційного активу
28	Зберігання на флешках / Storage on flashdrives	Наявний	Вказання наявності обробки або зберігання даних на зовнішніх накопичувачах
29	Зовнішні користувачі / External users	Наявний	Вказання наявності обробки інформаційного активу стандартизованих зовнішніми користувачами не з підприємства

Продовження таблиці 3.2

№	Атрибут	Бізнес-процес	Опис
30	Інші зовн. користувачі / Other ext. users	Наявний	Вказання наявності обробки інформаційного активу нестандартизованих зовнішніми користувачами не з підприємства
31	Внутрішні користувачі \ Internal users	Наявний	Вказання наявності обробки інформаційного активу внутрішніми користувачами для критичних інформаційних активів
32	Захист потрібен? / Need protection?	Додано в ПЗ	Вказання необхідності захисту інформаційного активу
33	Відповідальний 1-5	Додано в ПЗ	Вказання пошти першої відповідальної особи, яка є власником або особою, якій делегували право створювати або актуалізувати інформаційний актив

3.3 Розробка інтерфейсу та логіки програмного забезпечення

ПЗ [22-24, 27-29] складається з наступних інтерфейсів:

3.3.1 Main page – інтерфейс головного меню у якому користувач зможе обрати необхідну для себе функціональність. Компоненти інтерфейсу наведені у таблиці 3.3.

Таблиця 3.3 – Компоненти інтерфейсу Main page

Компонент	Опис
HeaderContainer	Зона для розміщення заголовку
Header	Заголовок
MainContainer	Головний контейнер для розміщення внутрішніх зон
Container 1-4	Чотири контейнера для розміщення контенту
Image 1-4	Зображення в контейнерах контенту
FeatureItemButton 1-4	Текстова кнопка, яка має посилання на інші інтерфейси згідно коду: *Navigate('Створення або актуалізація інформаційних активів / Creation or actualization of information assets'; ScreenTransition.Fade)* *Navigate(Support; ScreenTransition.Fade)* *Navigate(Learning; ScreenTransition.Fade)* *Navigate('Main Page'; ScreenTransition.Fade)*
DescriptionText 1-4	Підпис для контейнеру

Розроблений інтерфейс наведений на рисунку 3.2.

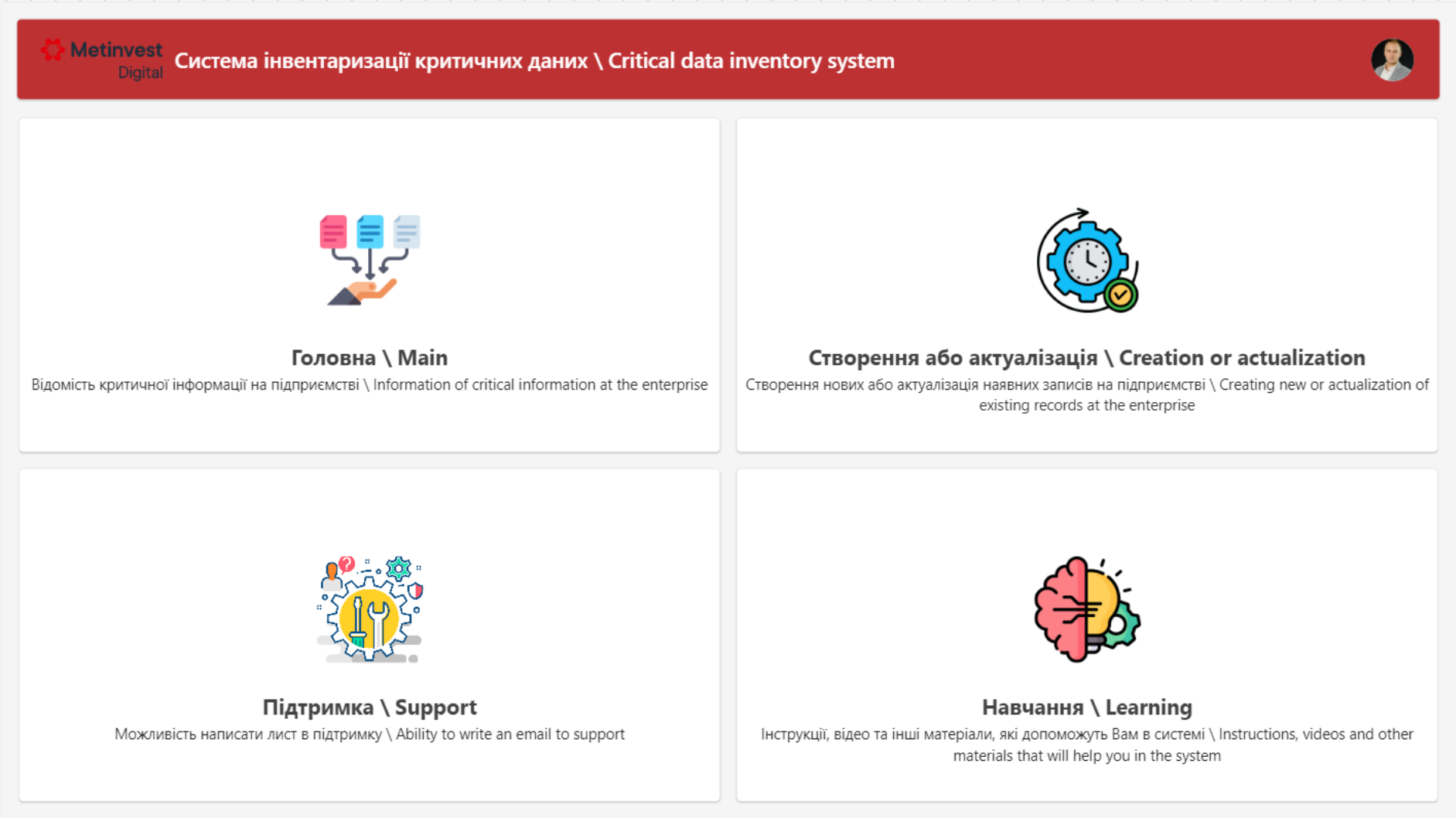


Рисунок 3.2 – Дизайн і функціональність інтерфейсу Main Page

3.3.2 Inventory assets – інтерфейс додатку у якому користувач зможе ознайомитися з інформаційними активами, які відносять до його підприємства. Кількість даних скорочена відносно бази даних, відсутня інформація по збереженню даних і користувачам (конфіденційні дані). Компоненти інтерфейсу наведені у таблиці 3.4. Розроблений інтерфейс наведений на рисунку 3.3 та 3.4.

Таблиця 3.4 – Компоненти інтерфейсу Inventory assets

Компонент	Опис
ButtonCanvas	Кнопка для повернення до інтерфейсу Main page, має код для переходу: Navigate('Inventory Assets'; ScreenTransition.Fade)
HeaderContainer	Зона для розміщення заголовку
Header	Заголовок
MainContainer	Головний контейнер для розміщення компонентів
Table	Елемент таблиці у якій є зв'язок з відображенням даних. Дані фільтрується для користувача по його підприємству вбудованим фільтром згідно формули *Filter('Inventory System'; 'Підприємство / Company' = ПользователиOffice365.MyProfile().CompanyName; Рецензія = true)*, який пов'язаний з інтегрованим компонентом Office365 [21] для зчитування даних підприємства користувача, яке заповнене в атрибуті CompanyName. Користувач нічого не побаче, якщо його підприємство не співпадає з даними у стовпці [20] 'Підприємство / Company'

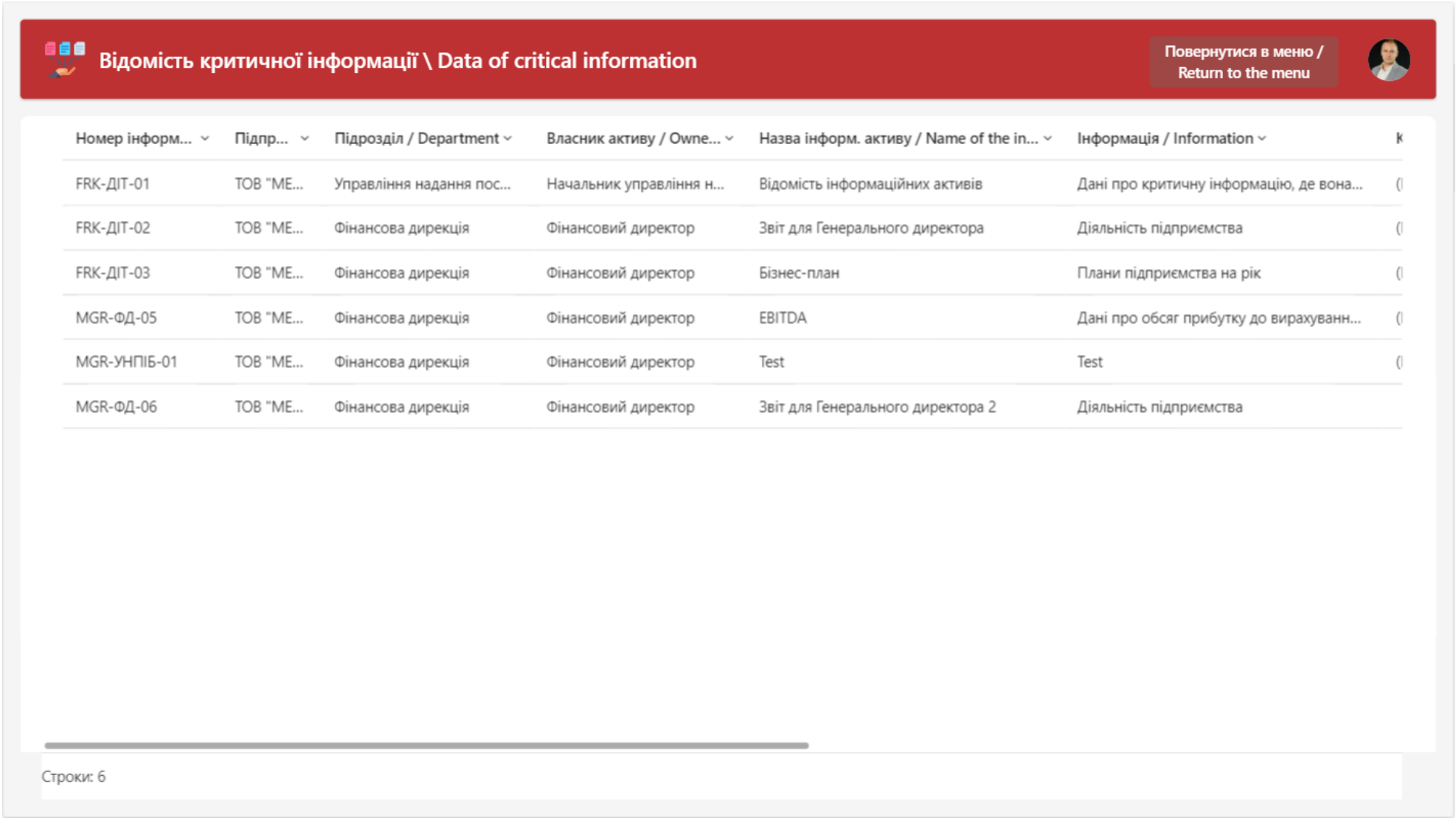


Рисунок 3.3 – Дизайн і функціональність інтерфейсу Inventory Assets (1 з 2)

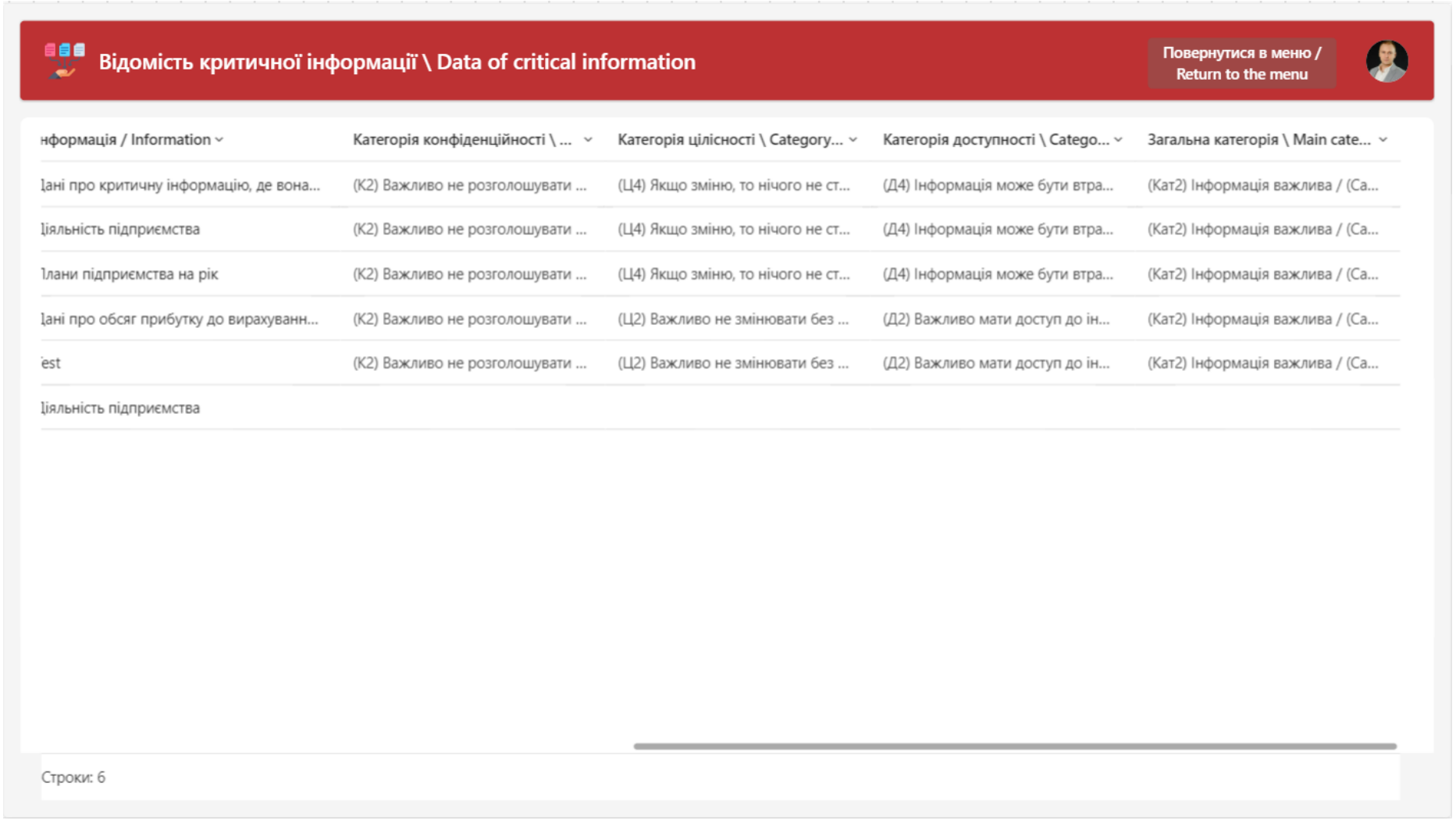


Рисунок 3.4 – Дизайн і функціональність інтерфейсу Inventory Assets (2 з 2)

3.3.3 Створення або актуалізація інформаційних активів – інтерфейс додатку у якому користувач зможе створити нові інформаційні активи або якщо користувач є відповідальною особою – додати зміни до інформаційних активів. Все створені або змінені активи одразу не з’являються в інтерфейсі поки інформаційна безпека не встановить ознаку успішною рецензії, яка при створенні або зміні автоматично встановлює значення False. Компоненти інтерфейсу наведені у таблиці 3.5. Розроблений інтерфейс наведений на рисунках 3.5 – 3.13.

Таблиця 3.5 – Компоненти інтерфейсу Створення або актуалізація інформаційних активів

Компонент	Опис
ButtonCanvas	Кнопка для повернення до інтерфейсу Main page, має код для переходу: Navigate('Inventory Assets'; ScreenTransition.Fade)
HeaderContainer	Зона для розміщення заголовку
Header	Заголовок
BodyContainer	Головний контейнер для розміщення компонентів
SideBarContainer	Контейнер для розміщення меню вибору, пошуку та фільтрації інформаційних активів
CheckboxCanvas	Елемент переключення стану активів, які потребують і не потребують актуалізації
TextInput	Елемент для вводу тексту для пошуку і фільтрації

Продовження таблиці 3.5

Компонент	Опис
Table	Таблиця, яка формує елементи для відображення тих активів, які відповідальна особа може побачити. Є вбудований складний фільтр, який виводить дані в залежності від вводу тексту у пошук, вибору переключення актуальності активів та перевірки хто ти є (відповідальна особа). Формується за формулою, яка наведена у Додатку В
RightContainer	Контейнер для розміщення кнопок створення активів або їх редагування
CreateButton	Кнопка для активації форми по створенню активів
EditButton	Кнопка для активації форми по редагуванню активів
MainContainer	Контейнер, де розміщується функціональність з формою створення або зміни інформаційних активів
Form	Форма, яка виводить у картці інформацію про формат створення активів або їх зміну, якщо вибраний актив із наявного списку
CancelButton	Кнопка відміни створення або редагування активів. Має формулу: ResetForm(Form2);; UpdateContext({ newMode: false; editMode: false; CurrentItem: First(Table2.SelectedItems); isItemSelected:false });;

Продовження таблиці 3.5:

Компонент	Опис
SubmitButton	Кнопка відправки змін по створенню або редагуванню активів. Додатково має функціонал виводу повідомлення про успішну зміну та відправку листа на інформаційну безпеку для повідомлення про зміну. Код: SubmitForm(Form2);; Office365Outlook.SendEmail("nikita"; "Змінено інформаційні активи"; "Потребує рецензії"; {Importance:"Normal"});; Notify("Запис оновлено. Після рецензії ІБ він з'явиться у загальному реєстрі / The record has been updated. After the IS review, it will appear in the general register"; NotificationType.Success);;
PromptDescription	Підказки, які додаються у вигляді іконки «Інформації» у формі з інформацією для користувача

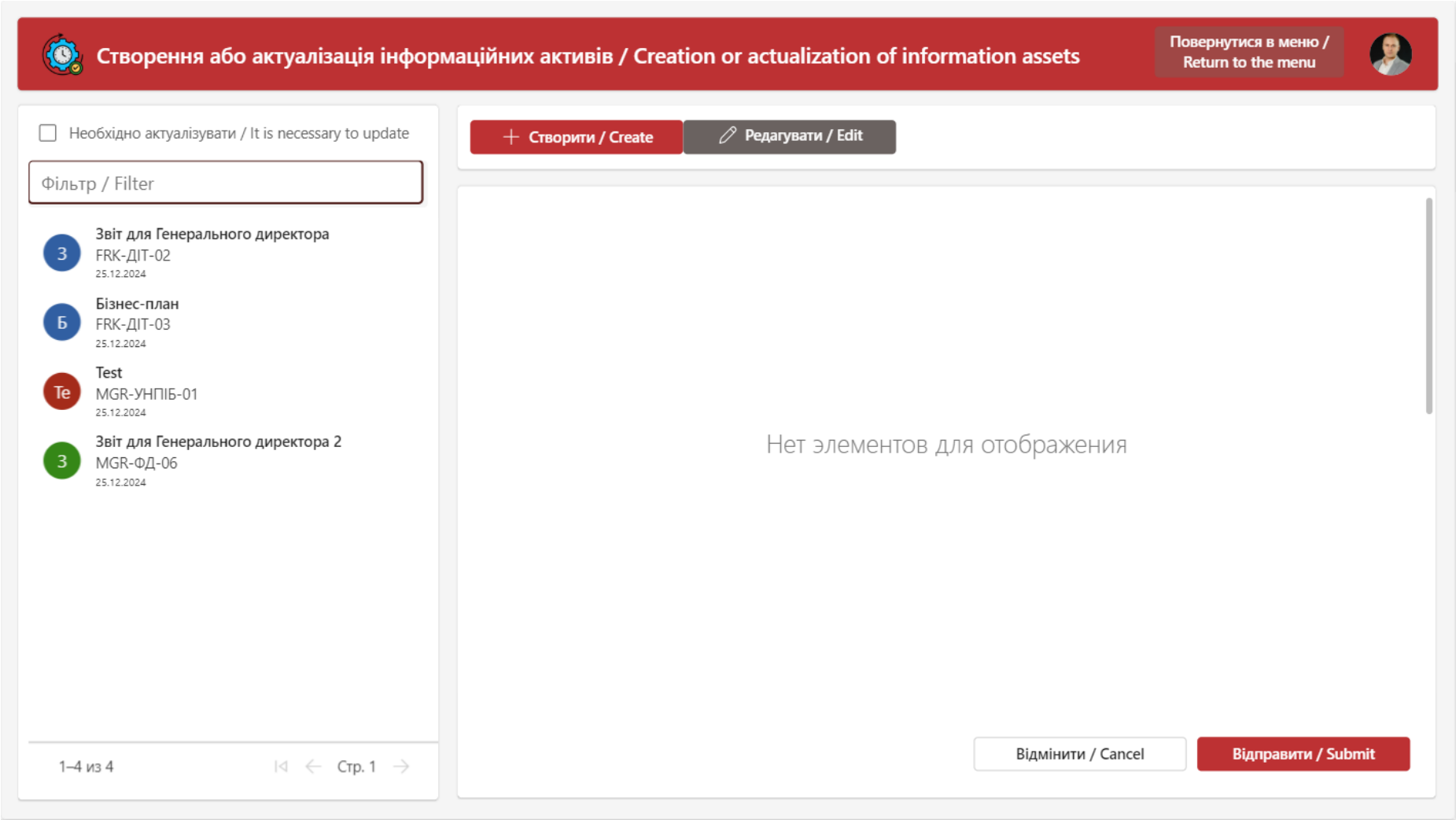


Рисунок 3.5 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (1 з 9) – Основний інтерфейс без обраних дій

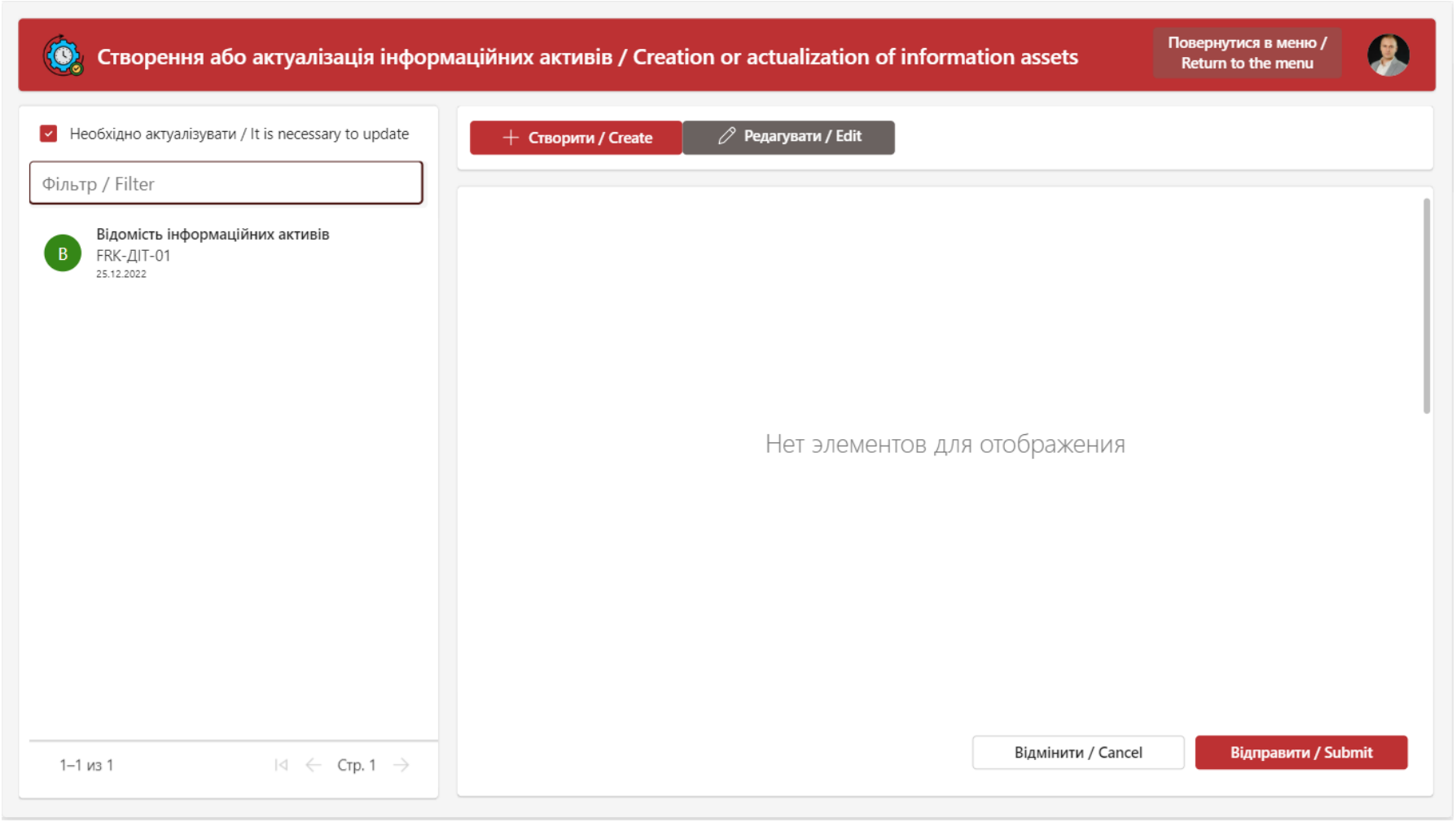


Рисунок 3.6 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (2 з 9) – Функціональність фільтрації через обраний стан неактуальності

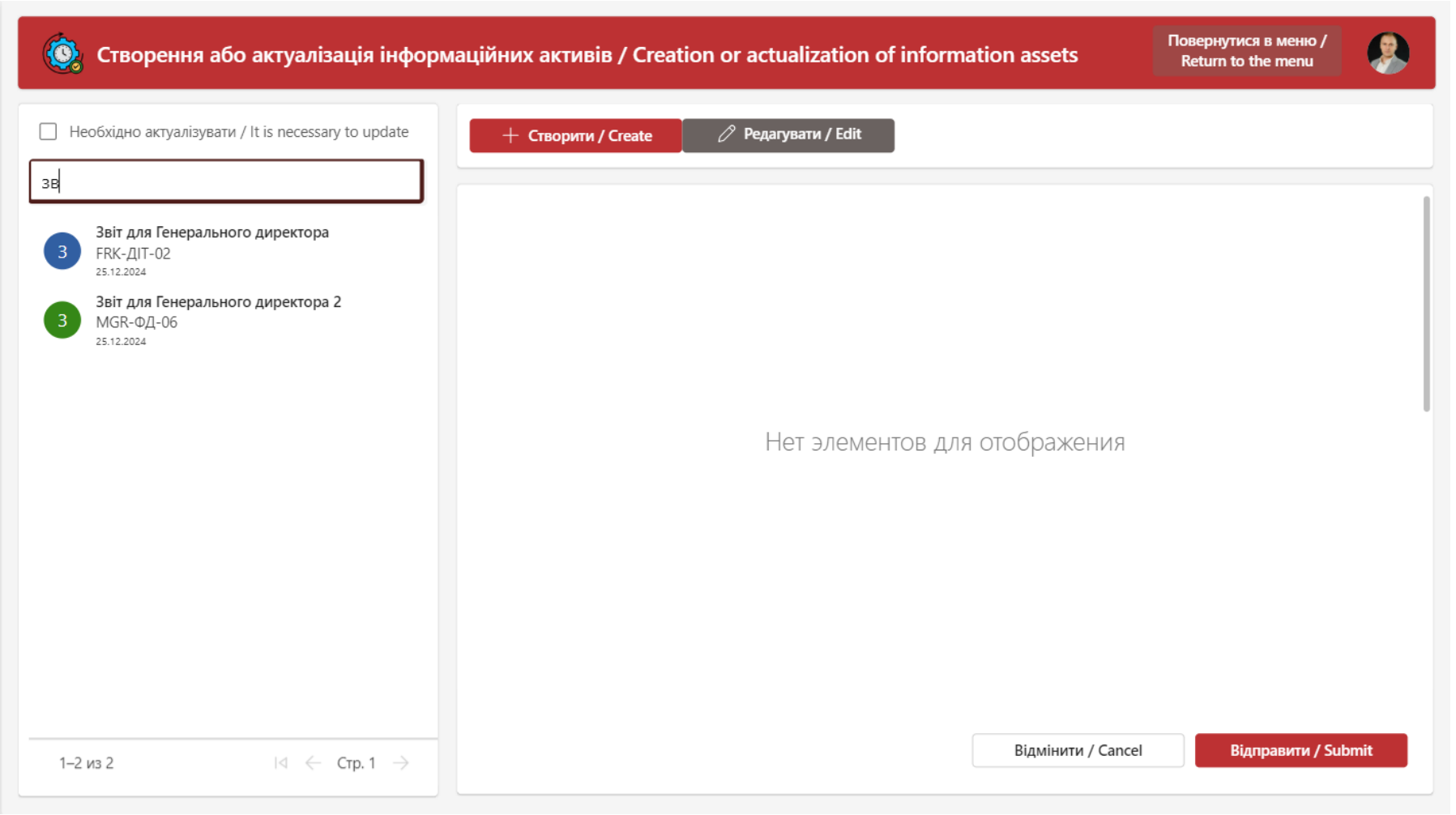


Рисунок 3.7 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (3 з 9) – Функціональність фільтрації через пошук даних у списку активів

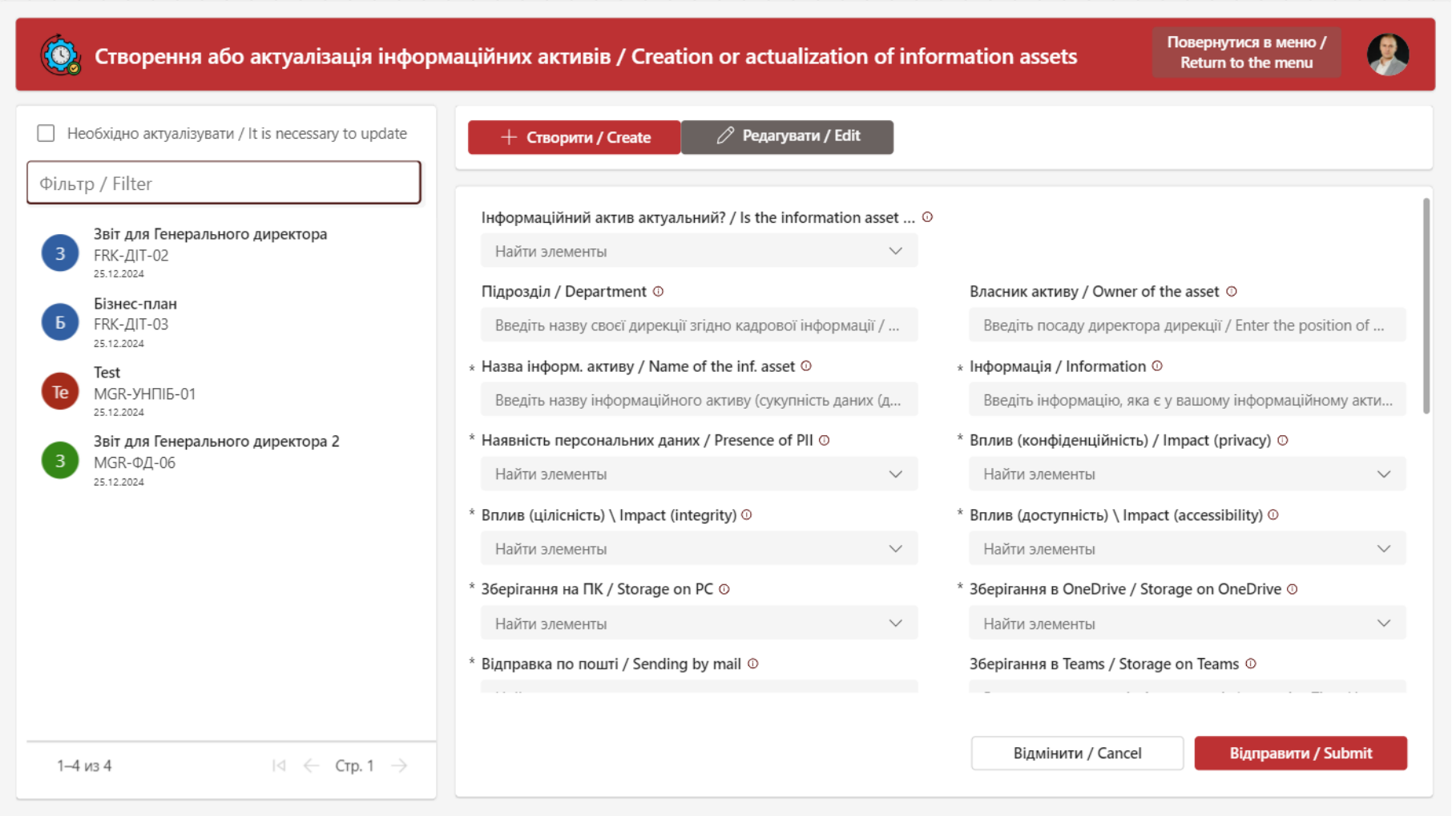


Рисунок 3.8 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (4 з 9) – Функціональність активації створення нового активу (1 з 4)

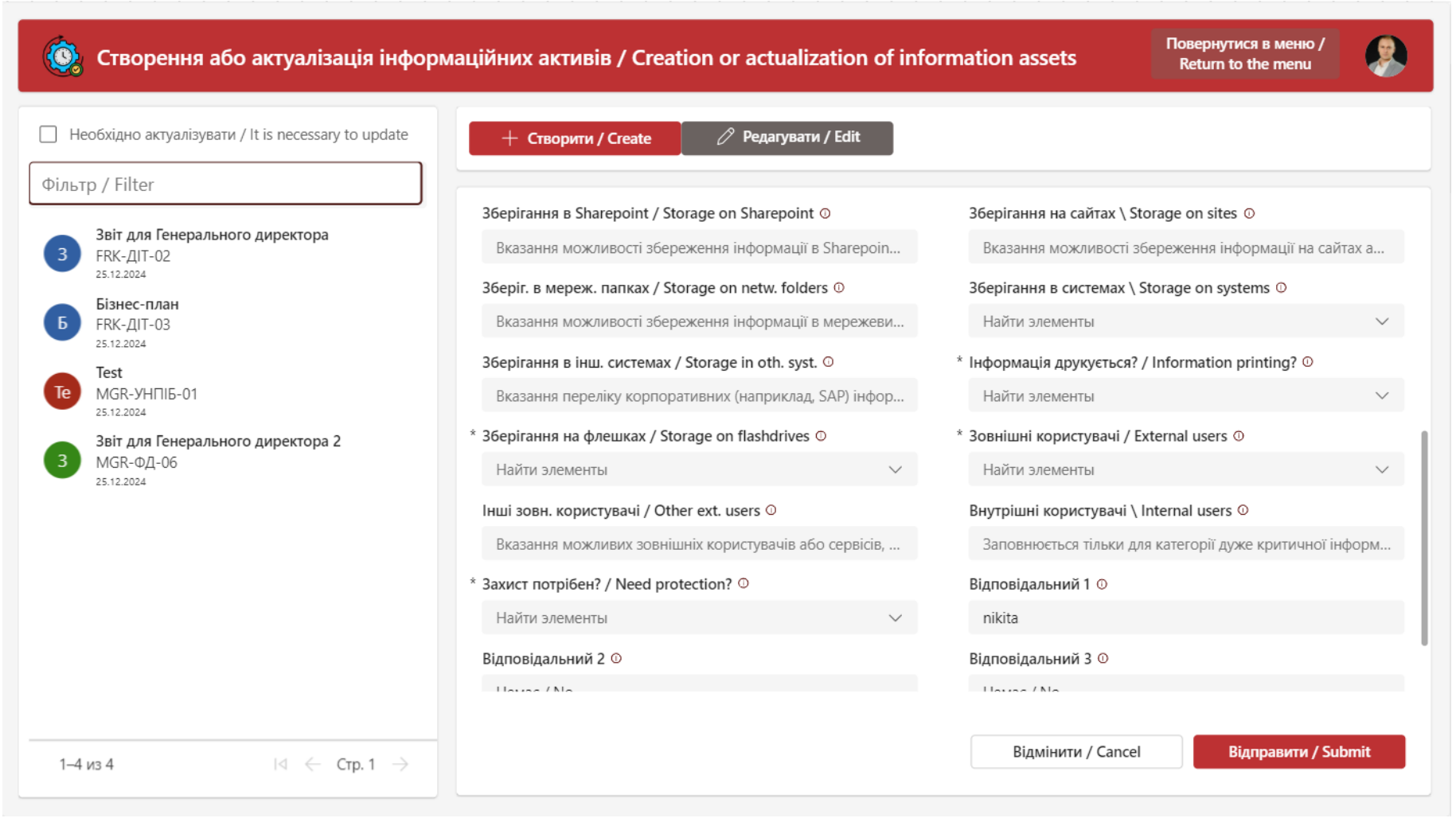


Рисунок 3.9 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (5 з 9) – Функціональність активації створення нового активу (2 з 4)

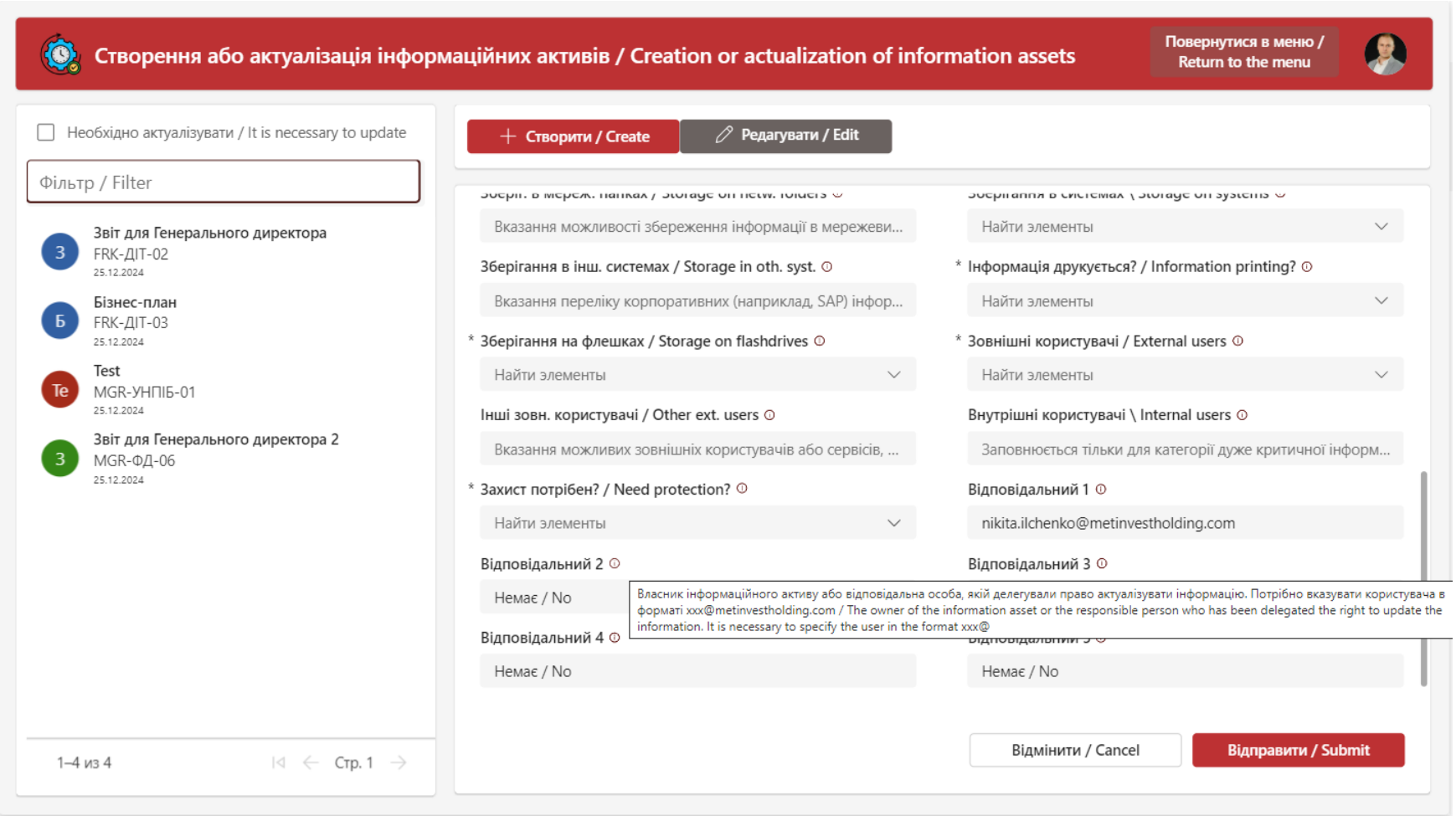


Рисунок 3.10 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (6 з 9) – Функціональність активації створення нового активу (3 з 4), відображення підказки

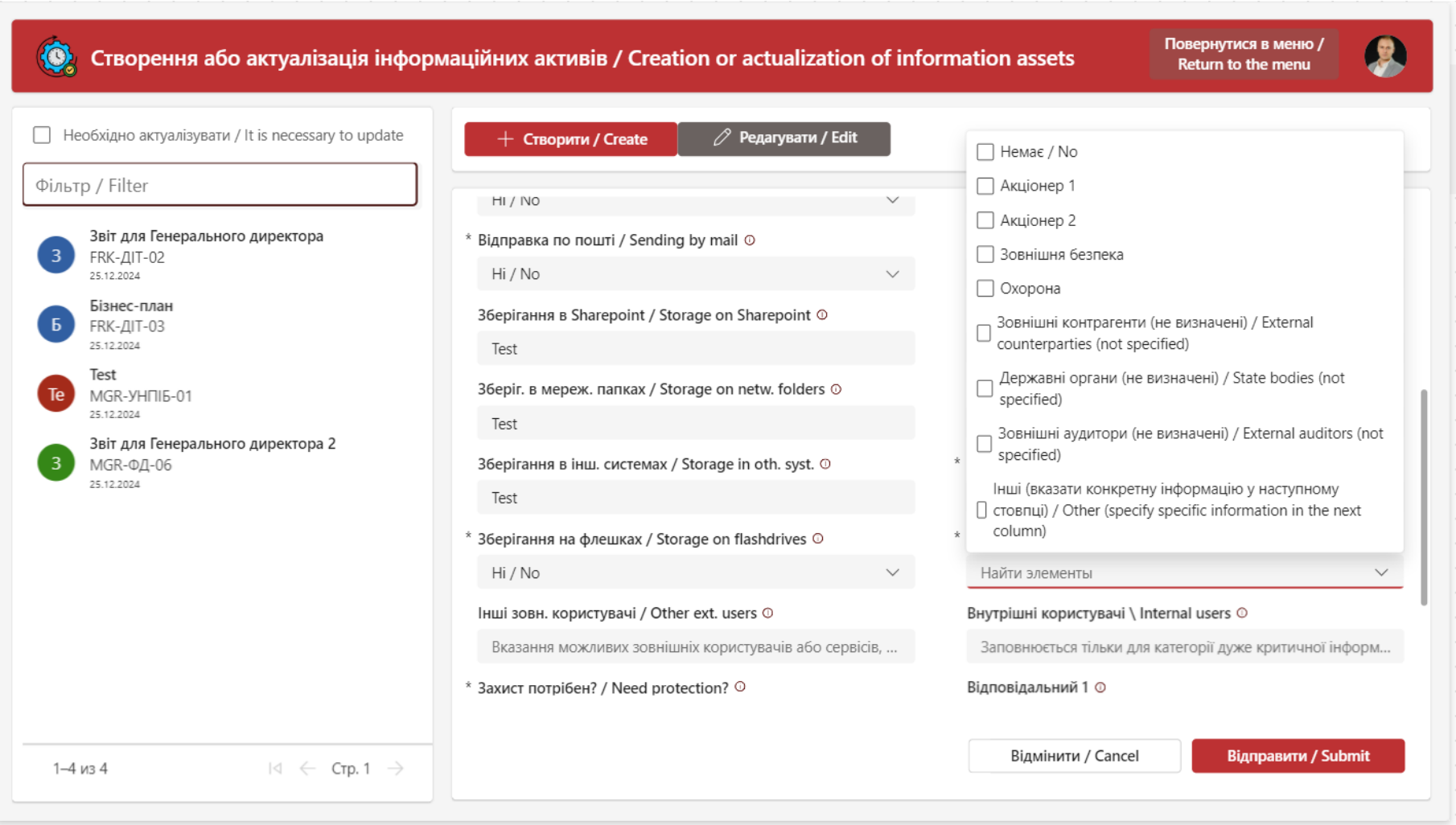


Рисунок 3.11 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (7 з 9) – Функціональність активації створення нового активу (4 з 4), відображення випадаючого меню

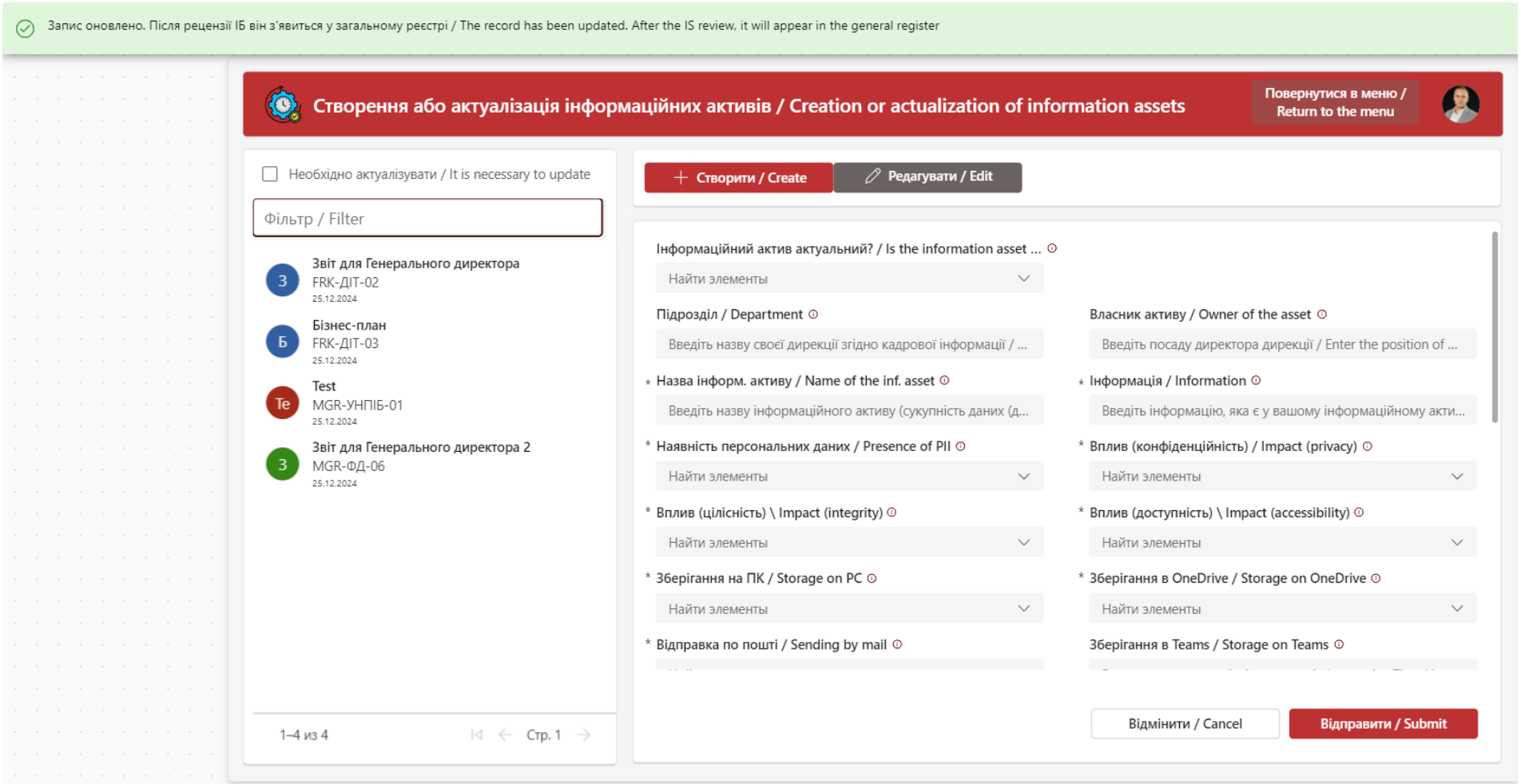


Рисунок 3.12 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (8 з 9) – Функціональність підтвердження активу та відображення повідомлення

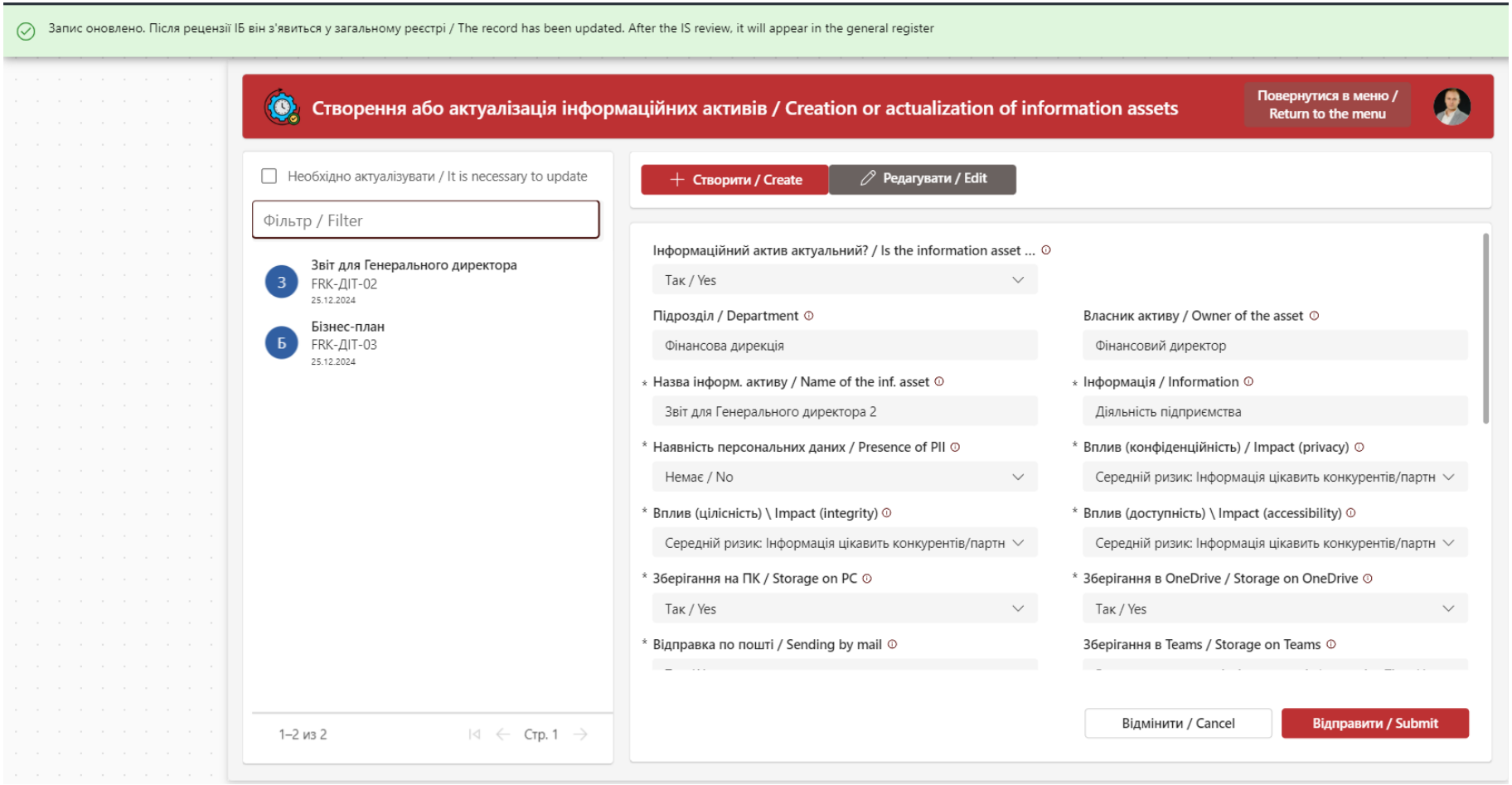


Рисунок 3.13 – Дизайн і функціональність інтерфейсу Створення або актуалізація інформаційних активів (9 з 9) – Функціональність зміни активу, відправки зміни і встановлення стану рецензії після якого активи зникають зі списку

3.3.4 Support – інтерфейс для відправки листів на технічну підтримку. Компоненти інтерфейсу наведені у таблиці 3.6. Розроблений інтерфейс наведено на рисунках 3.15 – 3.17.

Таблиця 3.6 – Компоненти інтерфейсу Support

Компонент	Опис
ButtonCanvas	Кнопка для повернення до інтерфейсу Main page, має код для переходу: Navigate('Inventory Assets'; ScreenTransition.Fade)
PeopleBrowserGallery	Зона для пошуку користувачів, використовую компонент пошуку Office365
LblEmailMessage	Поле для вводу повідомлення
LblEmailSubject	Поле для вводу теми листа
HeaderContainer	Зона для розміщення заголовку
IconButton	Кнопка відправлення листа, після відправки виводиться повідомлення для користувача. Код: *Set(_emailRecipientString; Concat(MyPeople; Mail & ";"));;* *Office365Outlook.SendEmail(_emailRecipientString; TextEmailSubject1.Text; TextEmailMessage1.Text; {Importance:"Normal"});;* *Reset(TextEmailSubject1);;* *Reset(TextEmailMessage1);;* *Clear(MyPeople);;* *Notify("Лист відправлено. З вами зв'яжеться відподільна особа і надасть зворотній зв'язок. / The mail has been sent. A separate person will contact you and provide feedback."; NotificationType.Success);;*

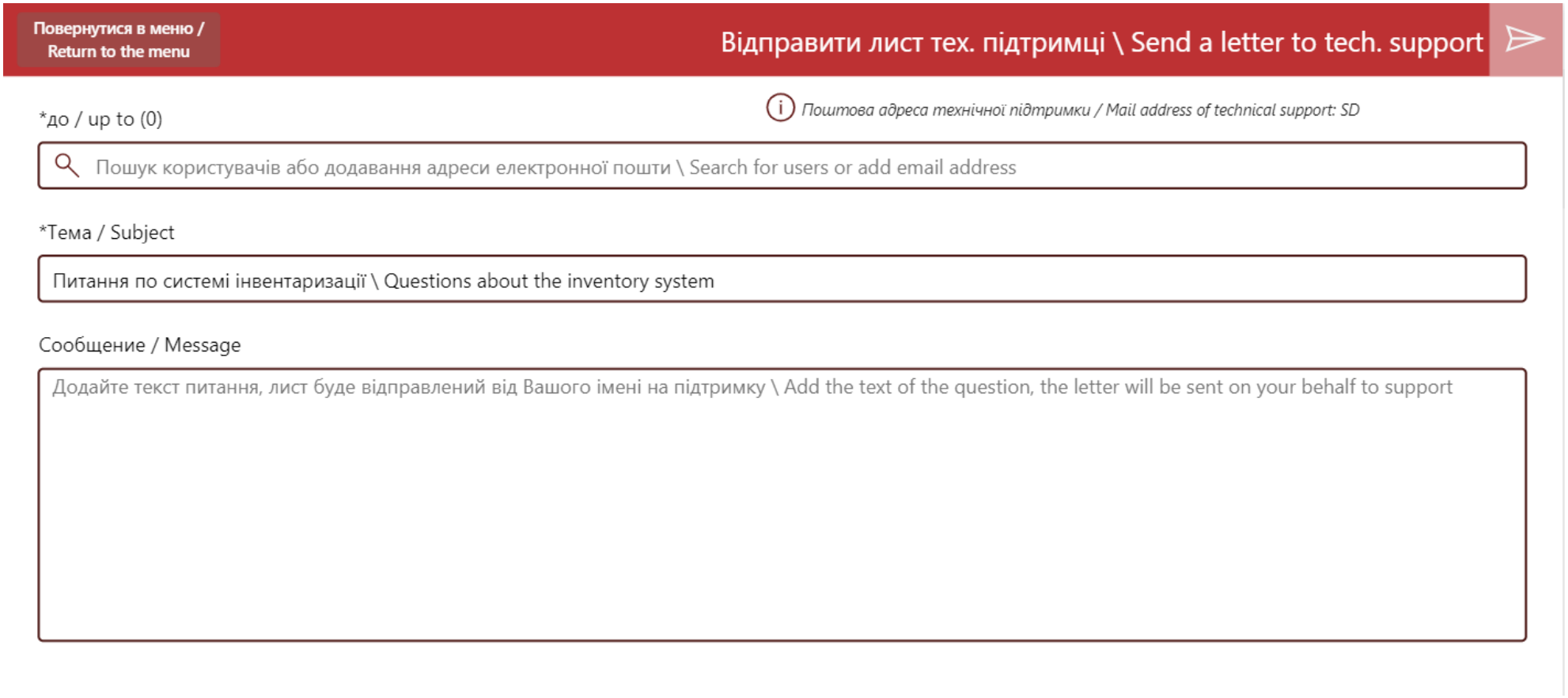


Рисунок 3.15 – Дизайн і функціональність інтерфейсу Support (1 з 3) – Функціональність створення листів

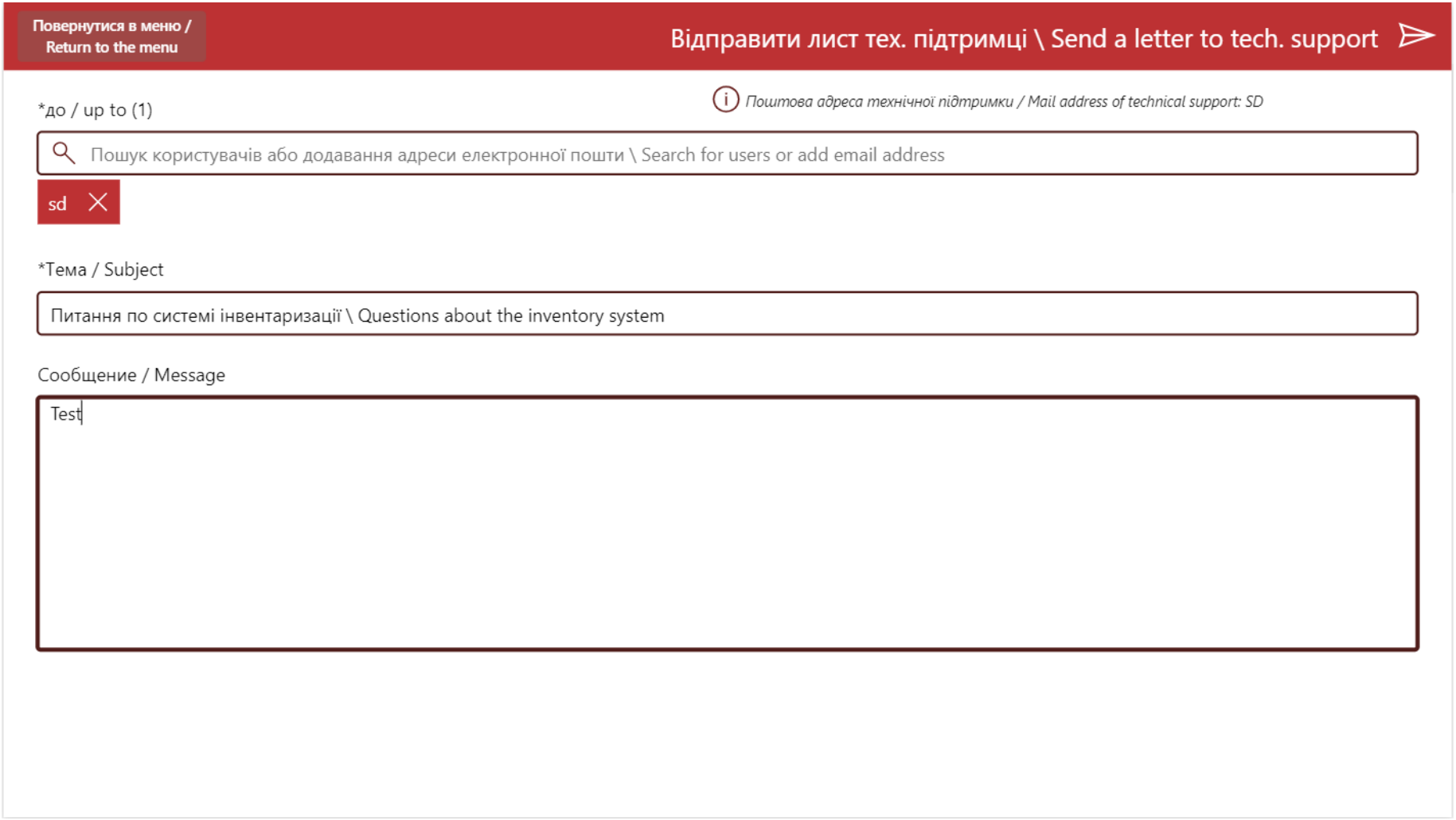


Рисунок 3.16 – Дизайн і функціональність інтерфейсу Support (2 з 3) – Пошук і додання користувача, ввід повідомлення

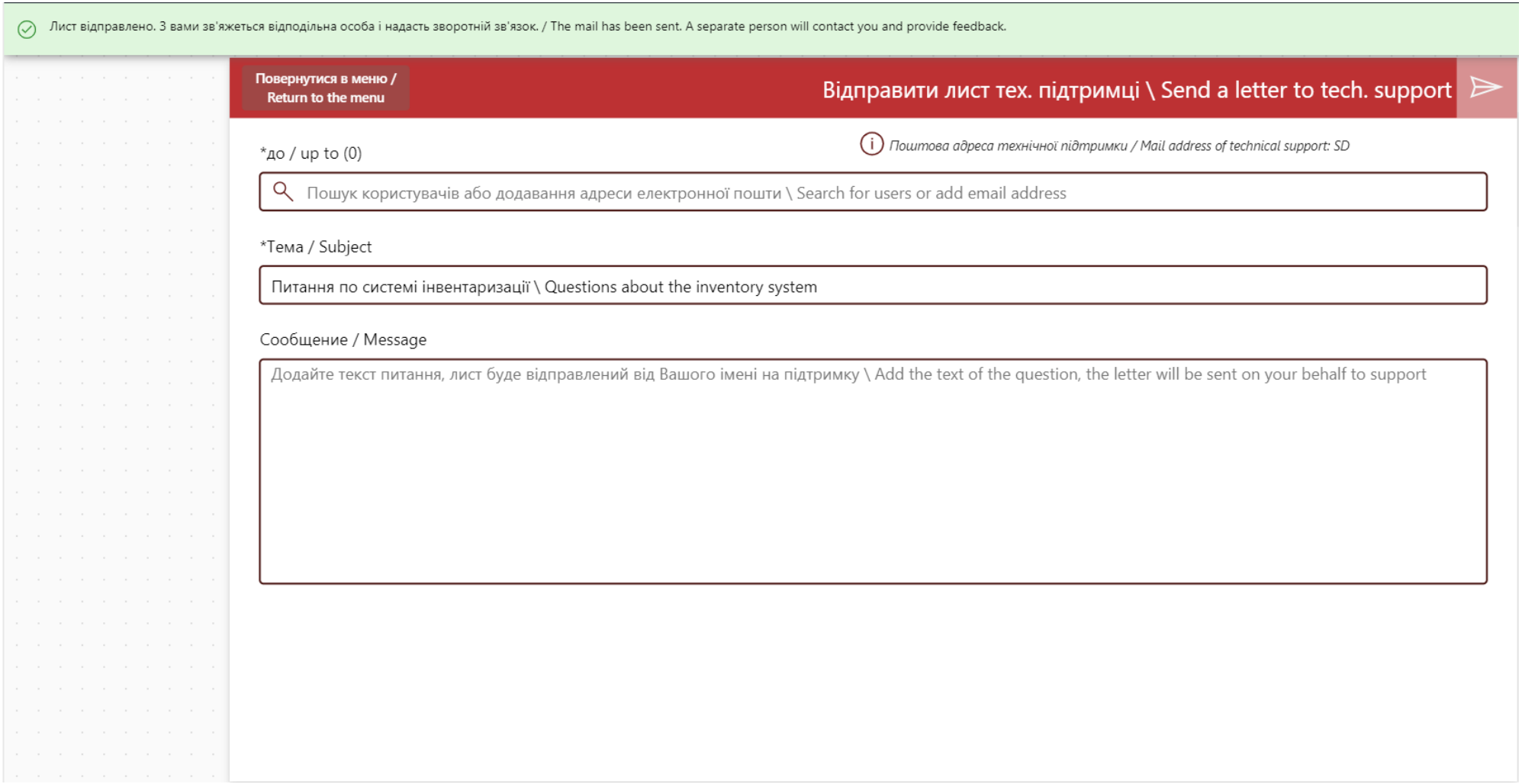


Рисунок 3.17 – Дизайн і функціональність інтерфейсу Support (3 з 3) – Відправка листа, відображення повідомлення для користувача

3.3.5 Learning – інтерфейс для навчання користувача по роботі в системі, виконує вимогу BR03. Компоненти інтерфейсу наведені у таблиці 3.7. Розроблений інтерфейс наведено на рисунках 3.19 – 3.22.

Таблиця 3.7 – Компоненти інтерфейсу Learning

Компонент	Опис
ButtonCanvas	Кнопка для повернення до інтерфейсу Main page, має код для переходу: Navigate('Inventory Assets'; ScreenTransition.Fade)
HeaderContainer	Зона для розміщення заголовку
TutorialImage 1-12	Відображення матеріалів по візуалізації навчання
iconPrev	Кнопка для переходу на попередній слайд навчання
iconNext	Кнопка для переходу на наступний слайд навчання
TutorialText	Зона для виводу тексту згідно обраного варіанту в TutorialNavigator, iconPrev, iconNext
TutorialNavigator	Компонент (точковий) для переключення слайдів навчання.

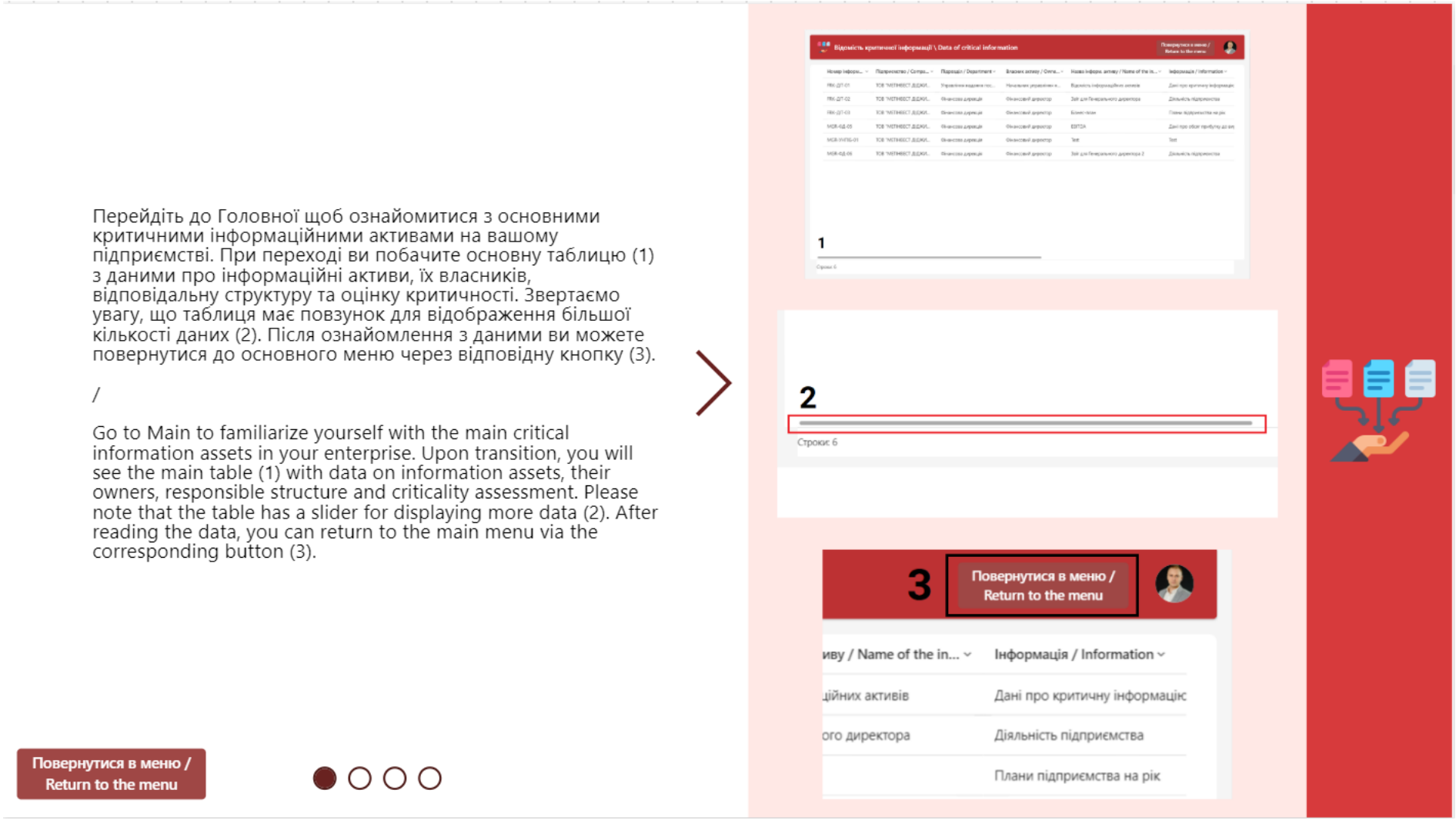


Рисунок 3.19 - Дизайн і функціональність інтерфейсу Learning (1 з 4) – Слайд 1 з навчанням по інтерфейсу Main Page

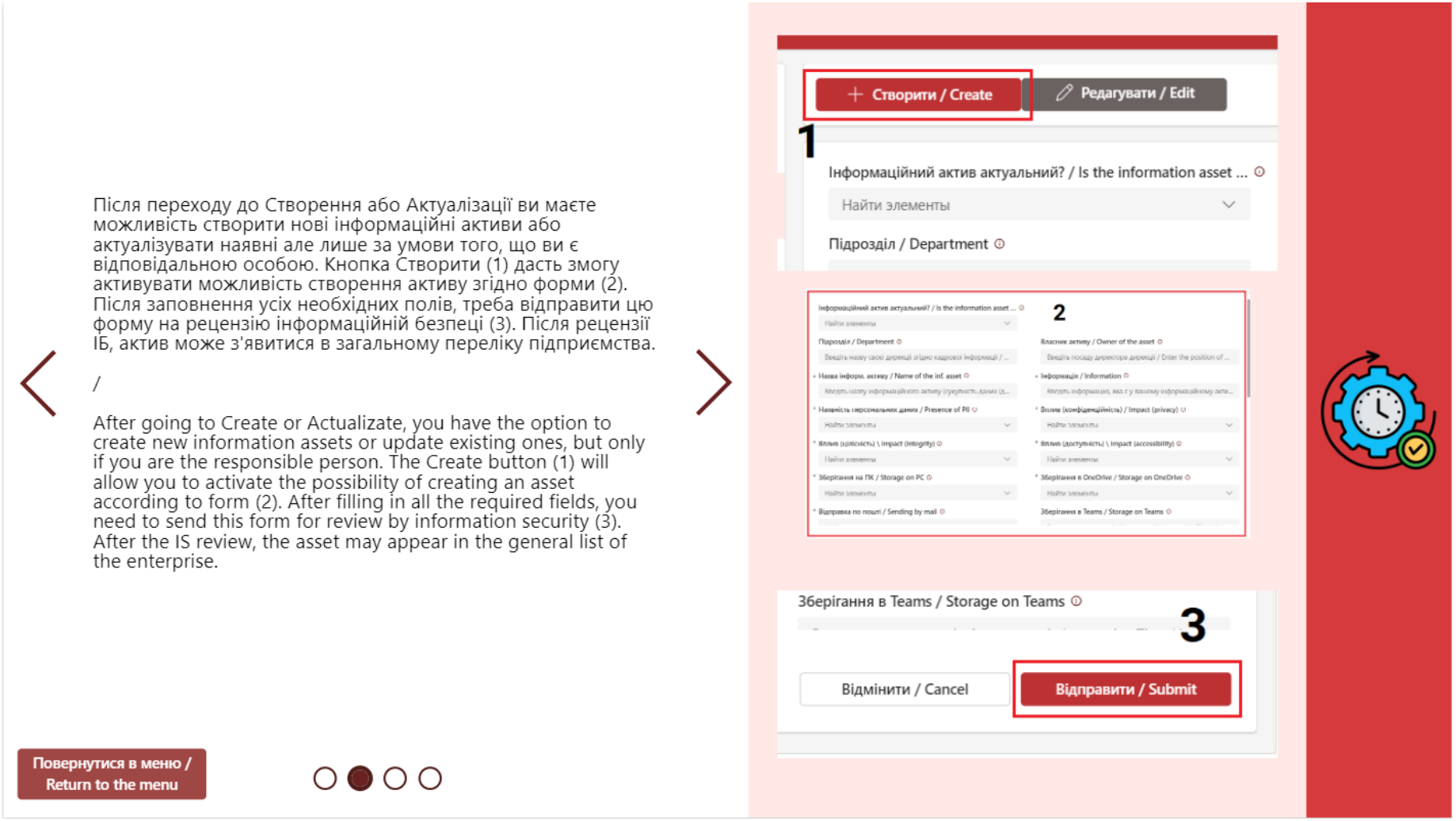


Рисунок 3.20 - Дизайн і функціональність інтерфейсу Learning (2 з 4) – Слайд 2 з навчанням по інтерфейсу Inventory Assets (створення активів)

Після переходу до Створення або Актуалізації ви маєте можливість актуалізувати наявні інформаційні активи але при умові, що ви є відповідальною особою. Якщо ви є відповідальною особою, в меню зліва (1) ви зможете побачити ті інформаційні активи за які ви відповідаєте. При натисканні галки Необхідно актуалізувати з'являться активи, які потребують актуалізації згідно термінів актуалізації (щорічно), про це ви повинні були отримувати повідомлення. Після натискання певного інформаційного активу є можливість активувати його редагування після натискання відповідної кнопки (2). Редагуйте усю необхідну інформацію і після закінчення роботи натискайте на кнопку Відправити (3). Після рецензії інформаційної безпеки, інформаційний актив може з'явитися в загальному переліку.

/

After going to Create or Actualizate, you have the opportunity to update existing information assets, but on the condition that you are the responsible person. If you are a responsible person, in the menu on the left (1) you will be able to see the information assets for which you are responsible. When you click on the It is neccessary to update check box, assets that need to be updated according to the update terms (annually) will appear, you should have received a notification about this. After clicking on a certain information asset, it is possible to activate its editing after pressing the corresponding button (2). Edit all the necessary information and when finished, press the Send button. After the review of information security, the information asset may appear in the general list.

Повернутися в меню / Return to the menu

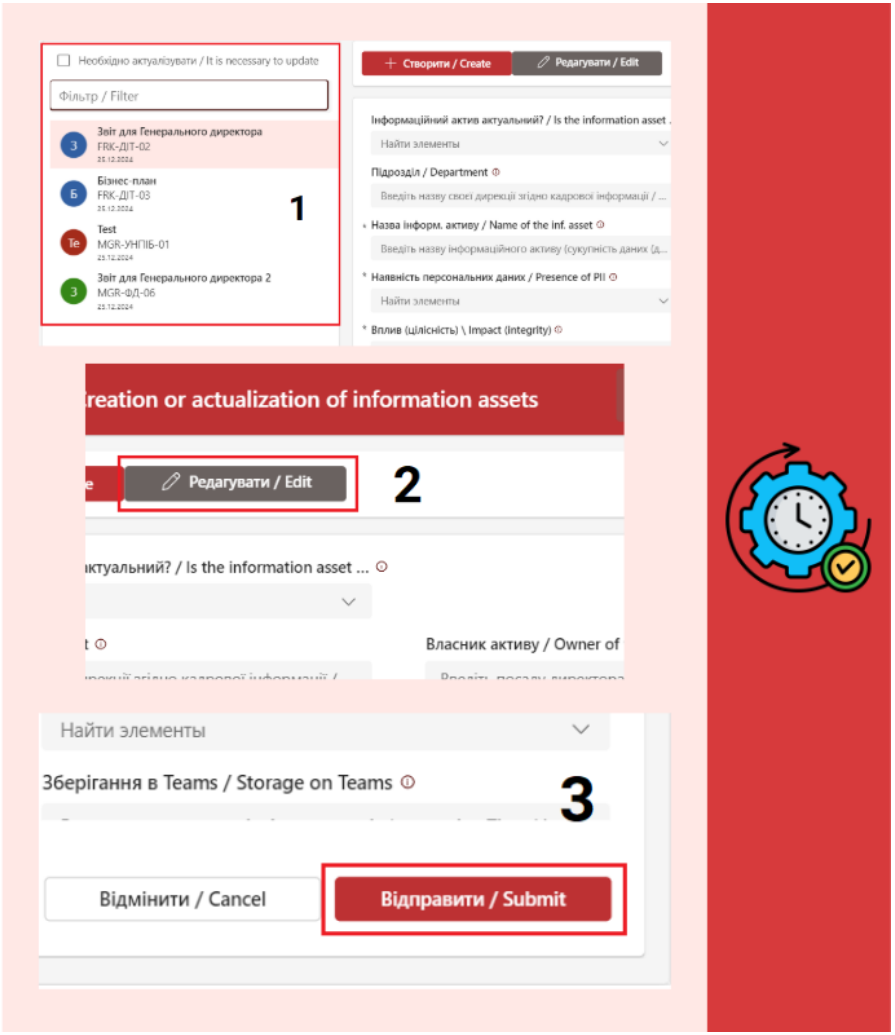


Рисунок 3.21 - Дизайн і функціональність інтерфейсу Learning (3 з 4) – Слайд 3 з навчанням по інтерфейсу Inventory Assets (актуалізація активів)

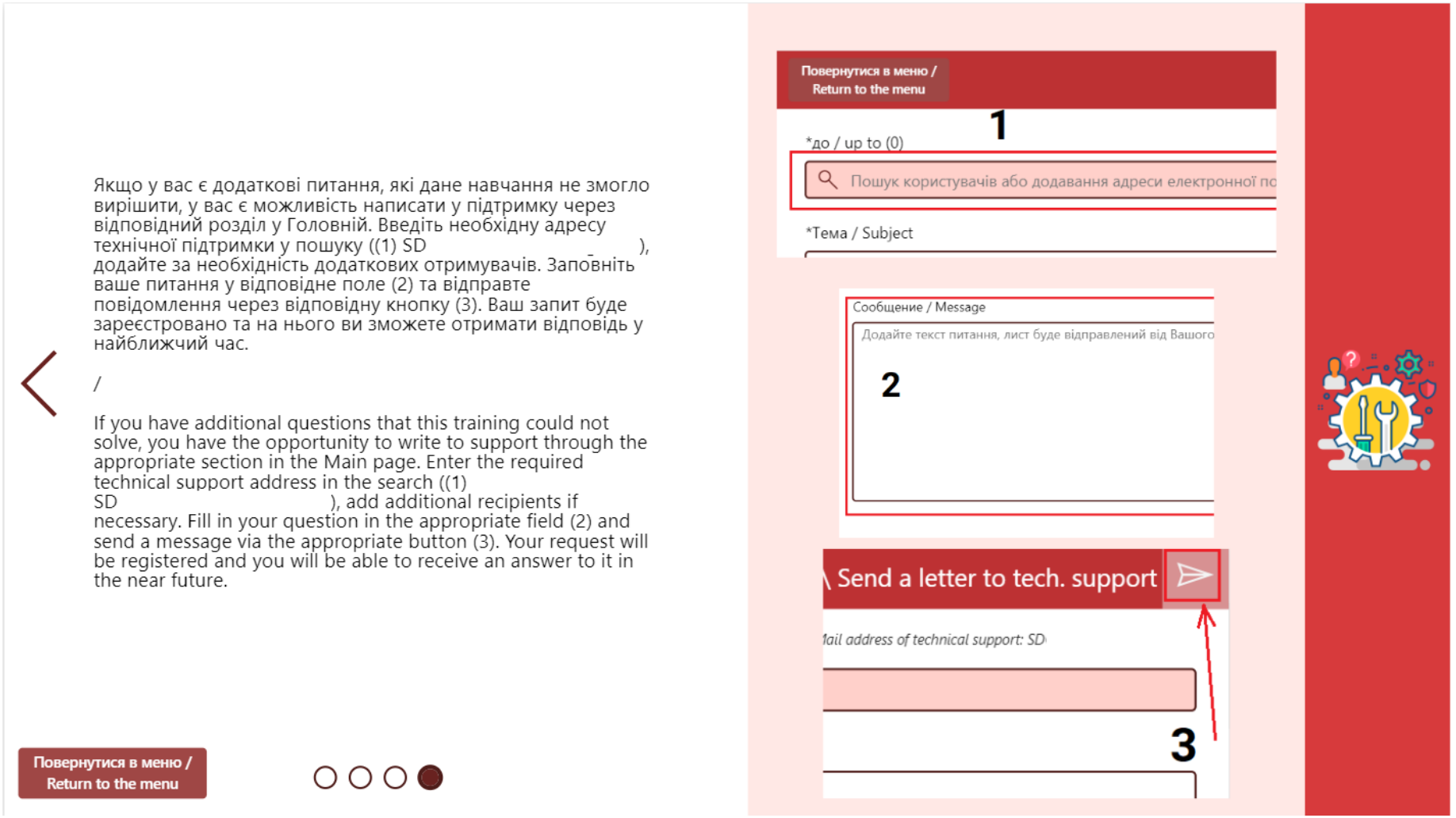


Рисунок 3.22 - Дизайн і функціональність інтерфейсу Learning (4 з 4) – Слайд 4 з навчанням по інтерфейсу Support

3.4 Автоматизація повідомлень про актуалізацію

Виконуючи вимогу BR04 розроблений механізм актуалізації даних через Microsoft Power Automate, який повинен на щомісячній основі перевіряти дату останньої актуалізації активів і відправляти відповідальним особам листи про необхідність актуалізації якщо дата останньої актуалізації вже більше чим 1 рік від наявної дати. Початок схеми наведено на рисунку 3.23.

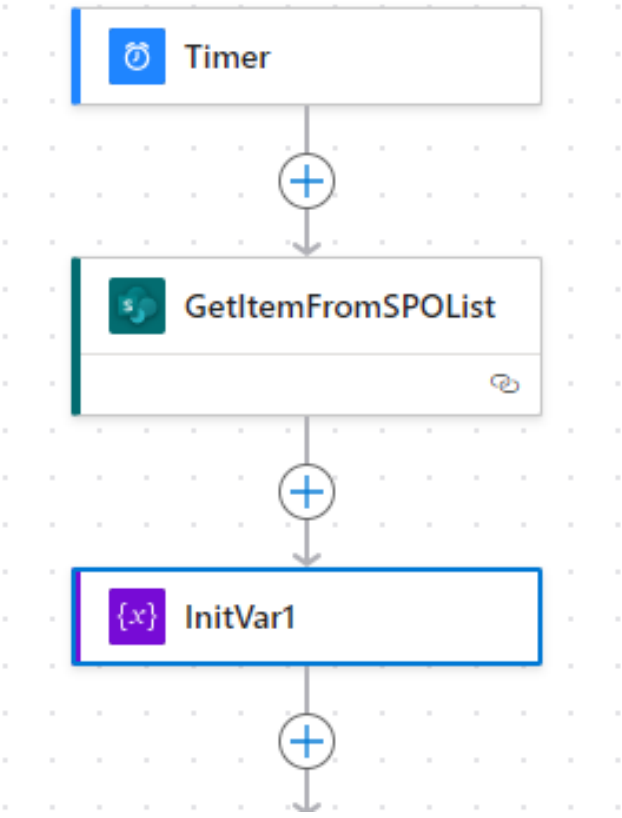


Рисунок 3.23 – Послідовні компоненти Flow

На описаному рисунку 3.23 представлені наступні компоненти:

– Timer – компонент щомісячної активації Flow (тригер). Налаштування зображено на рисунку 3.24.

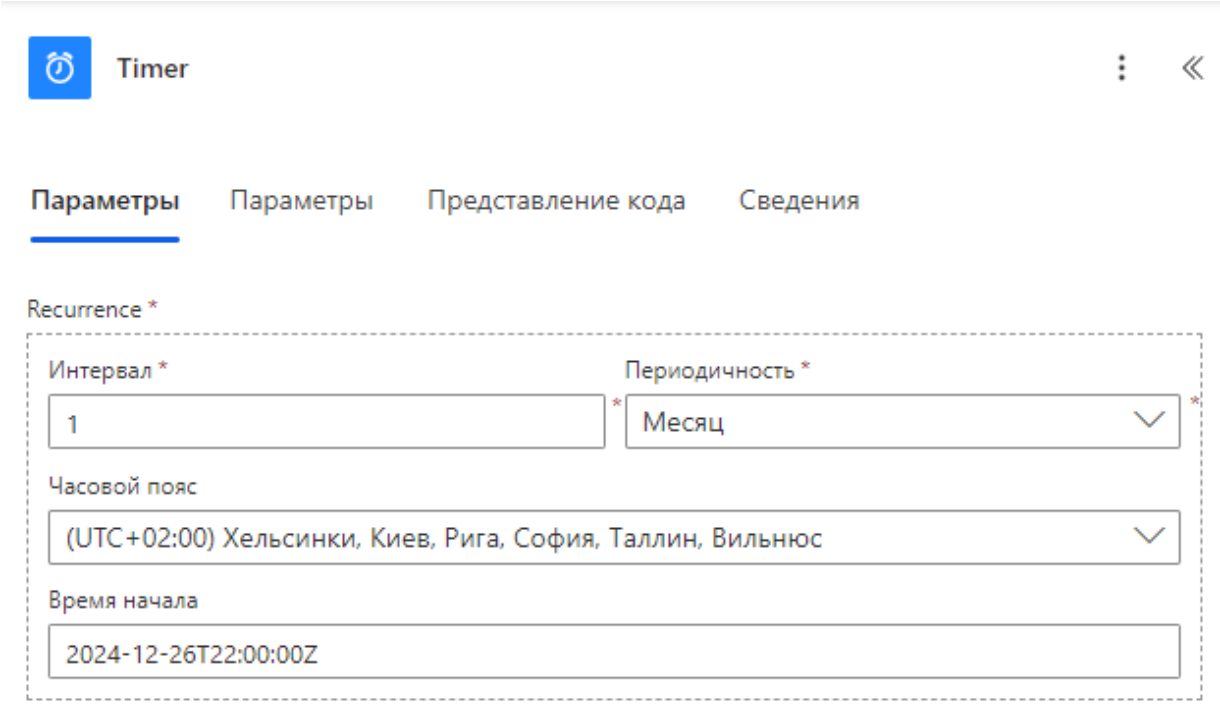


Рисунок 3.24. – Налаштування Timer

– GetItemFromSPOList – компонент імпорту даних з Sharepoint List [32]. Налаштування зображено на рисунку 3.25.

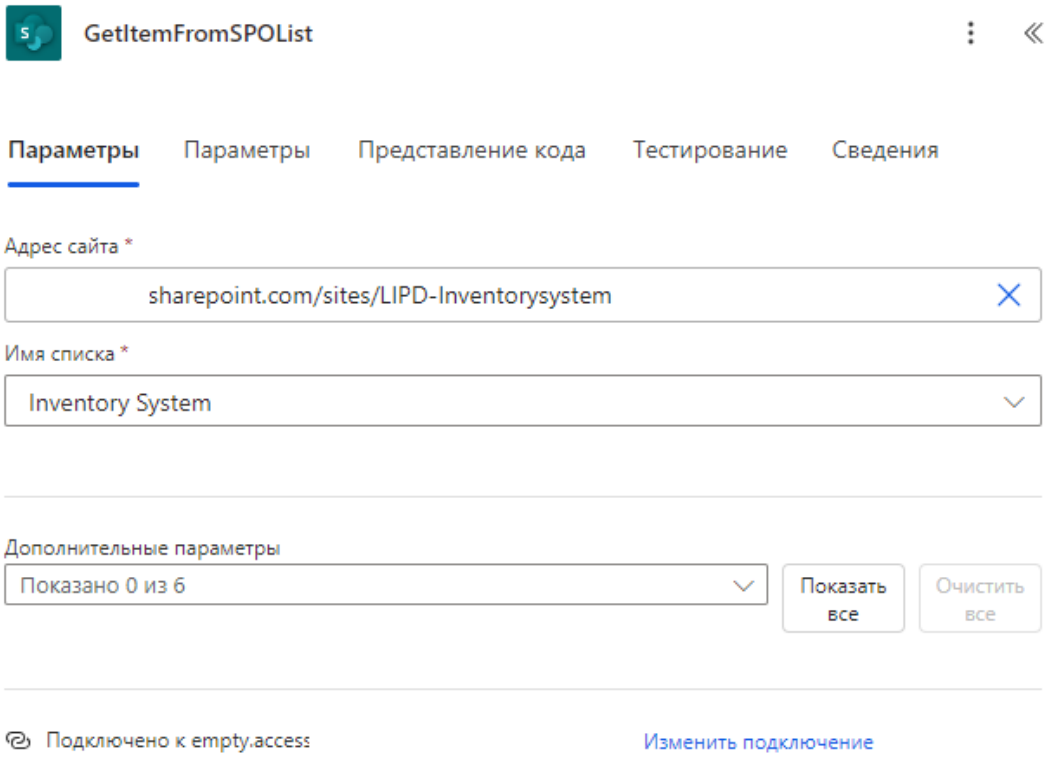


Рисунок 3.25 – Налаштування GetItemFromSPOList

– InitVar – ініціювання змінних для заповнення п’яти масивів [7, 13, 17], які будуть потім наповнятися даними по відповідальним з Sharepoint списку. Налаштування зображено на рисунку 3.26.

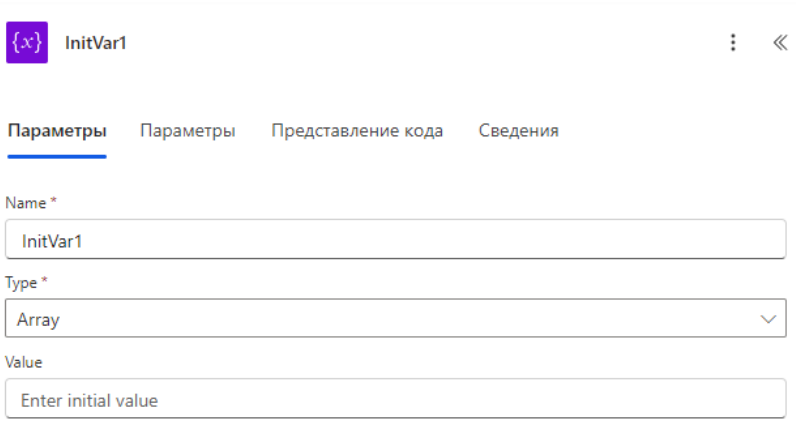


Рисунок 3.26 – Налаштування InitVar

Наступний послідовник блок представлений на рисунку 3.27.

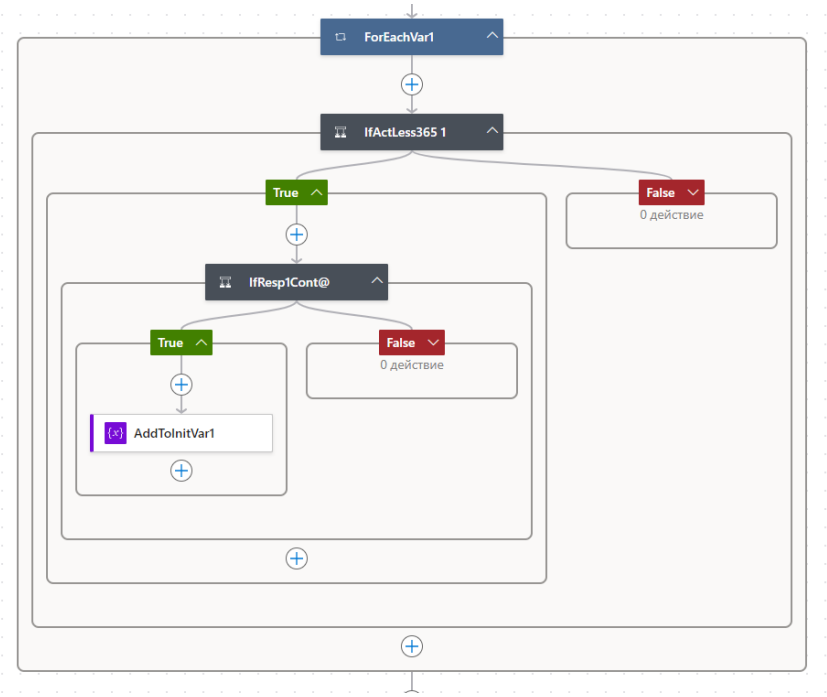


Рисунок 3.27 – Блок для перевірки кожного елементу Sharepoint списку, який перевіряє дату актуалізації та наявності в списку відповідальних осіб @ і додання цих осіб до масиву

На описаному рисунку 3.27 представлені наступні компоненти:

– ForEachVar – цикл для перевірки кожного елементу в таблиці. Налаштування зображено на рисунку 3.28.

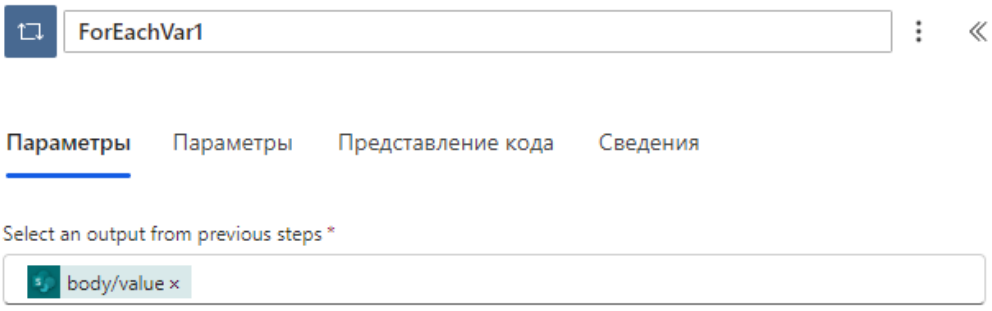


Рисунок 3.28 – Налаштування ForEachVar

– IfActLess365 – перевірка того, що дата актуалізації активу менша чим наявна дата мінус 1 рік. Налаштування зображено на рисунку 3.29 та 3.30.

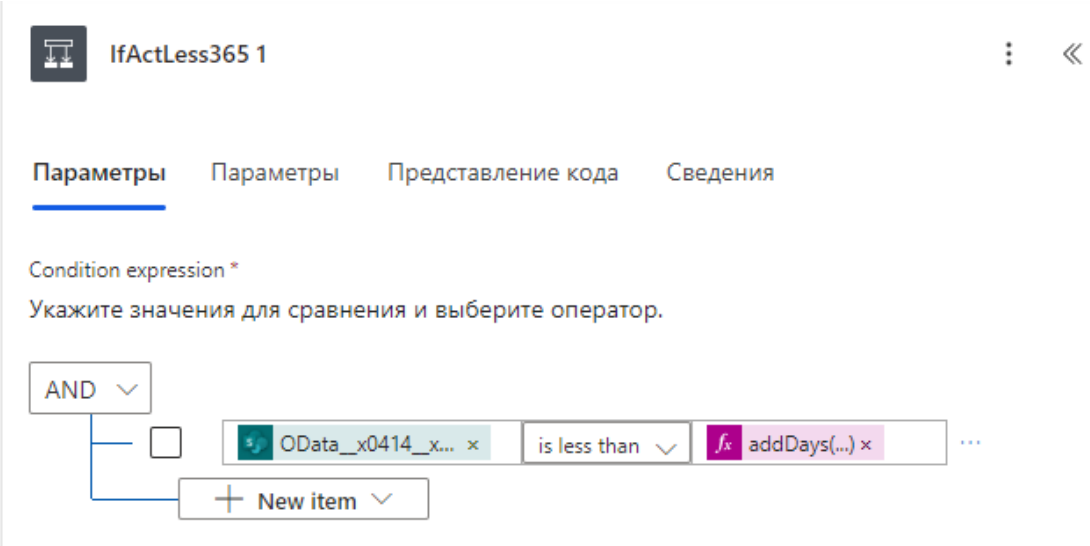


Рисунок 3.29 – Схема налаштування

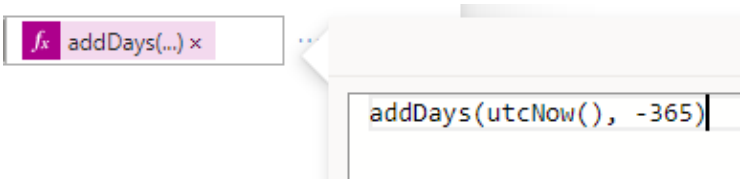


Рисунок 3.30 – Формула налаштування

– IfRespConf@ - перевірка того, що відповідальна особа містить елемент @ для фільтрування тих записів, які є поштою. Налаштування зображено на рисунку 3.31.

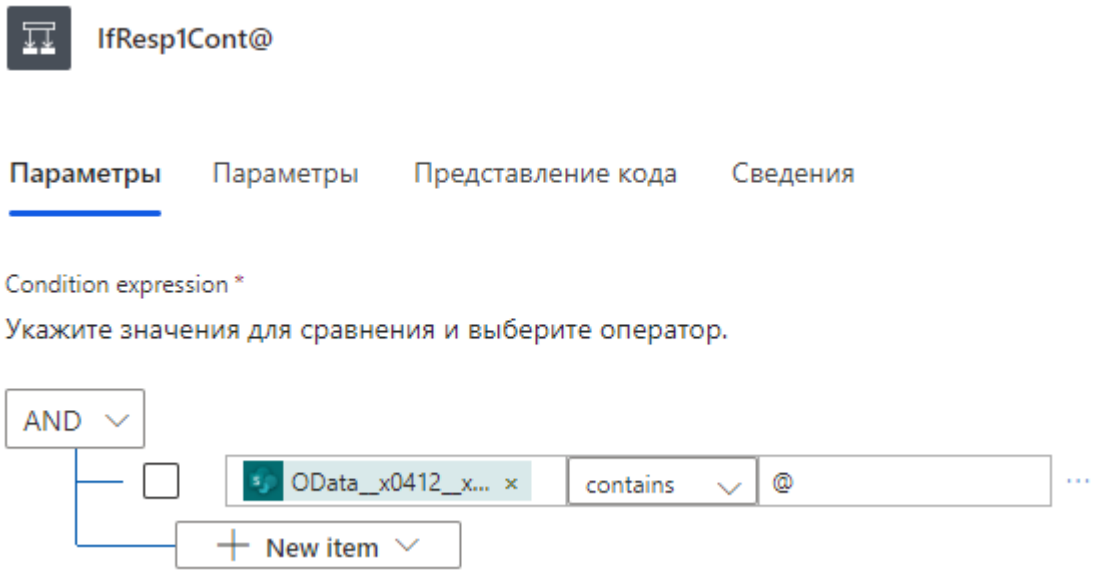


Рисунок 3.31 – Схема налаштування IfRespConf@

– AddToInitVar – додавання до масиву InitVar значення, які відфільтрувалось на попередніх етапах. Налаштування зображено на рисунку 3.32.

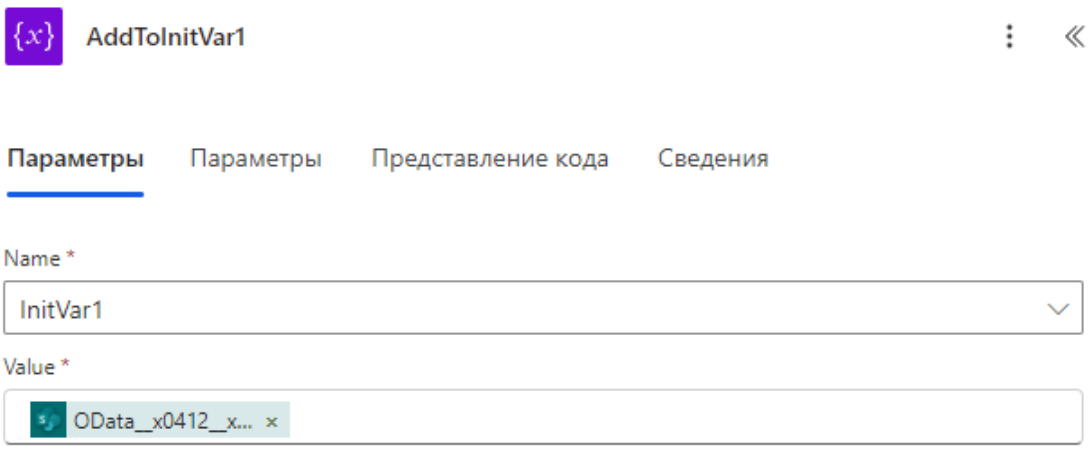


Рисунок 3.32 – Схема налаштування AddToInitVar

Варто зазначити, що таких ініціацій масиви та циклів перевірки є п’ять, по одному на кожну можливі відповідальну особу. Кожна особа перевіряється послідовно п’ять раз і наповняє п’ять різних масивів.

Далі схема завершується елементами, які представлені на рисунку 3.33.

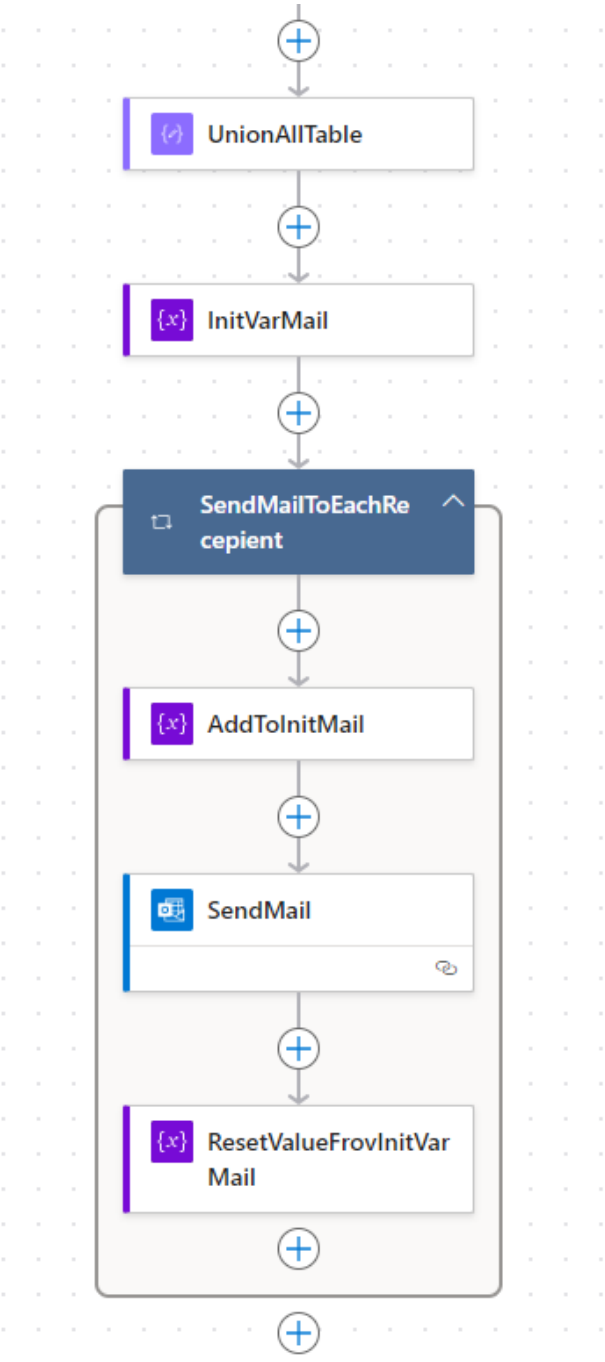


Рисунок 3.33 – Схема налаштування об’єднання масиву в єдиний список, ініціювання строкової змінної і написання кожному значенню з цієї змінної певного листа

На описаному рисунку 3.33 представлені наступні компоненти:

– UnionAllTable – елемент, який об’єднує попередні п’ять масивів у послідовний один з видаленням дублікатів по значенням. Налаштування зображено на рисунку 3.34 та 3.35.

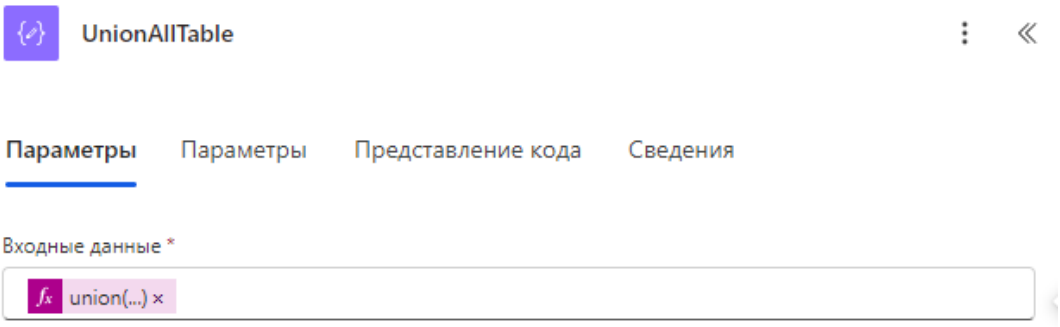


Рисунок 3.34 – Схема налаштування UnionAllTable

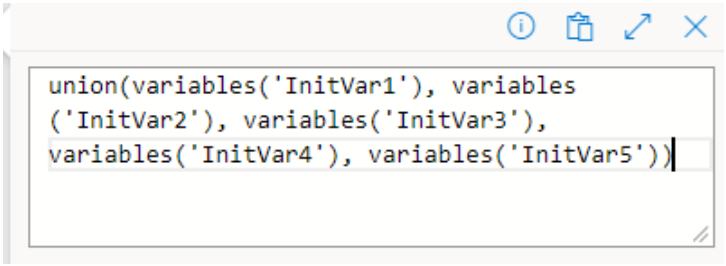


Рисунок 3.35 – Формула об’єднання і видалення дублікатів у масивів

– InitVarMail – ініціювання строкової змінної для відповідальних

– SendMailToEachRecepient – цикл, який бере кожен елемент масиву. Налаштування зображено на рисунку 3.36.

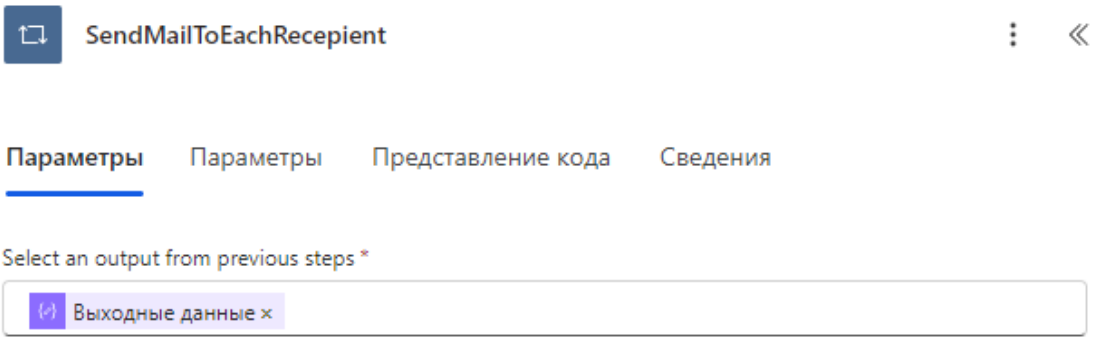


Рисунок 3.36 – Схема налаштування SendMailToEachRecepient

– AddToInitMail – додавання кожного елементу з UnionAllTable у InitVarMail. Налаштування зображено на рисунку 3.37.

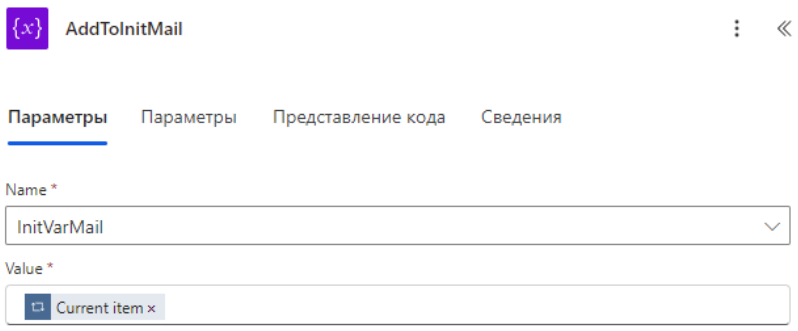


Рисунок 3.37 – Схема налаштування AddToInitMail

– SendMail – елемент відправки листа по кожному значенню з AddToInitMail. Налаштування зображено на рисунку 3.38 та 3.39.

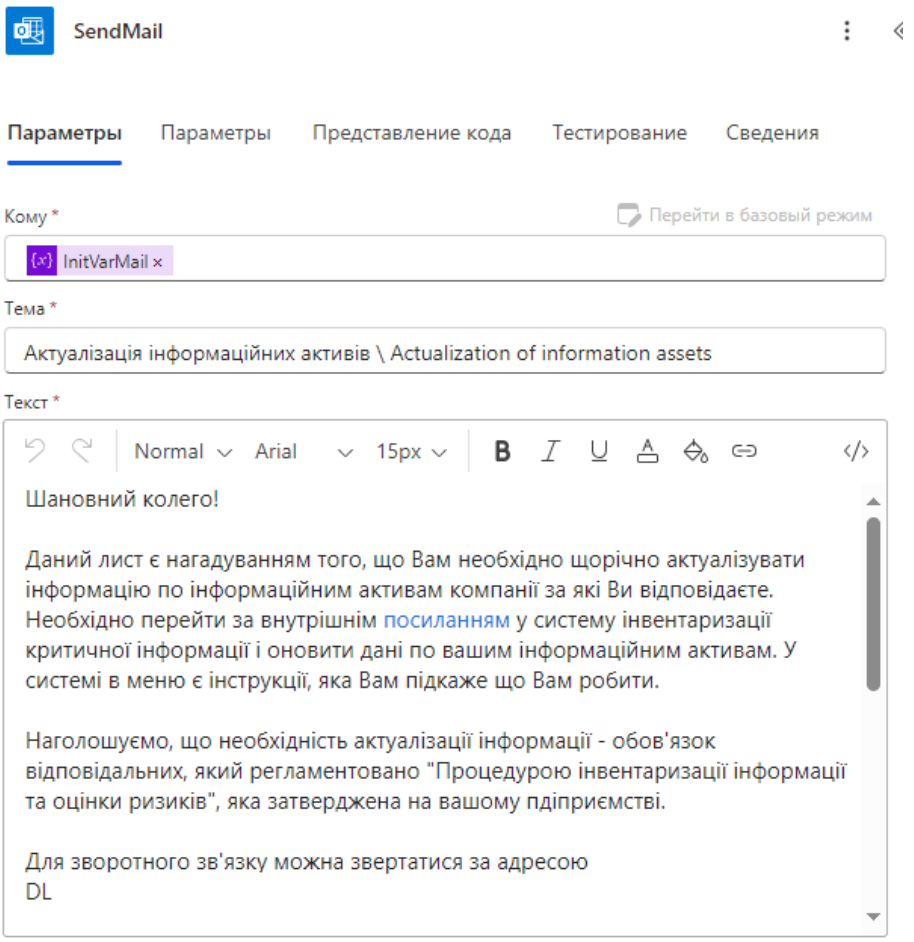


Рисунок 3.38 – Налаштування елементу SendMail (1 з 2)

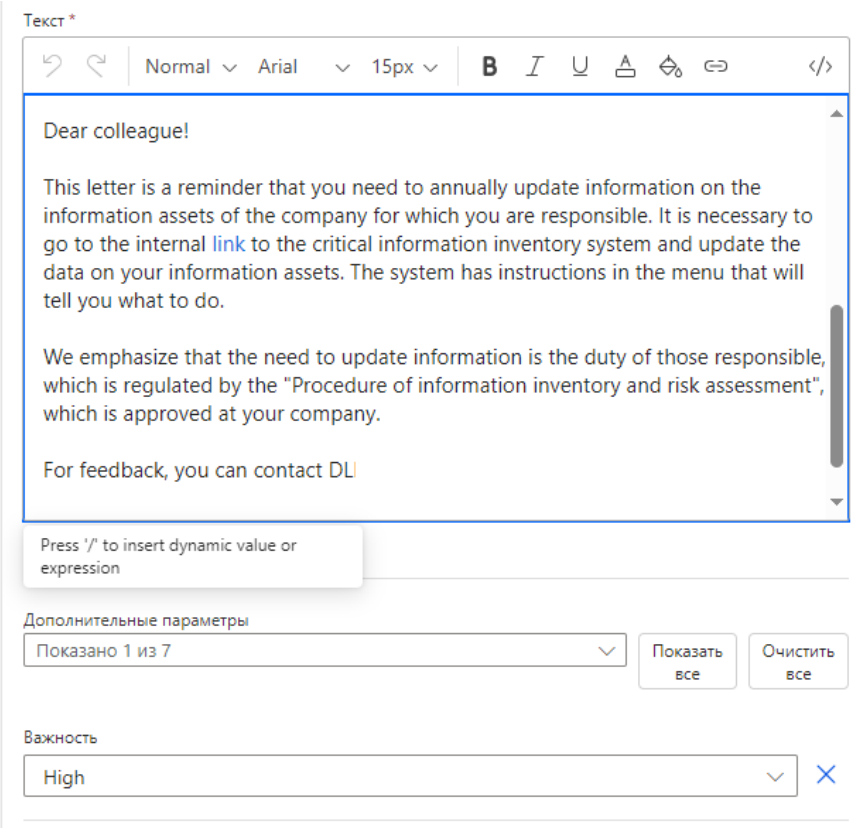


Рисунок 3.39 – Налаштування елементу SendMail (2 з 2)

– ResetValueFromInitVar – очистка значення з InitVarMail. Налаштування зображено на рисунку 3.40.

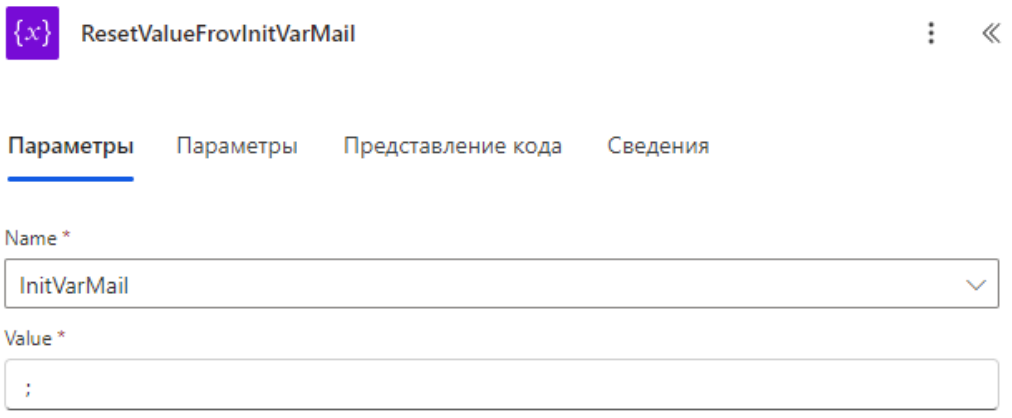


Рисунок 3.40 – Налаштування елементу ResetValueFromInitVar

Розроблені інтерфейси та їх компоненти протестовані у середовищі замовника. Результати тестування та реалізації бізнес-вимог будуть надані у Розділі 4.

РОЗДІЛ 4. ПРОВЕДЕННЯ ТА РЕЗУЛЬТАТИ ТЕОРЕТИЧНИХ ТА ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ЗАДАНОГО ОБ'ЄКТА

4.1 Тестування програмного забезпечення

Процеси, які досліджувалися у проєкті діляться на наступні напрямки:

- Створення нових інформаційних активів
- Актуалізації наявних інформаційних активів
- Перегляд наявних інформаційних активів
- Створення запитів на консалтинг
- Навчання.

Трансформуємо дані процеси в сценарії використання (use cases) для наступного дослідження. Сценарії використання наведені у таблиці 4.1.

Таблиця 4.1 – Сценарії використання

Номер сценарію використання	Опис сценарію використання
UC01	Новий інформаційний актив не створено, так як не заповнено усі обов’язкові поля
UC02	Новий інформаційний актив створено успішно
UC03	Отримано лист про створення нового інформаційного активу
UC04	Новий інформаційний актив не з’явився в загальному переліку після створення, так як потребує рецензії
UC05	Новий інформаційний актив рецензовано і він з’явився у загальному переліку

Продовження таблиці 4.1

Номер сценарію використання	Опис сценарію використання
UC06	Отримано лист по відповідальному власнику коли дата актуалізації інформаційного активу більше 1 року
UC07	Сценарій потоку не завершився помилкою
UC08	У загальному переліку для актуалізації доступні тільки ті інформаційні активи, за які відповідає відповідальна особа
UC09	При використанні пошуку наявні інформаційні активи фільтруються
UC10	При використанні галки про активи, які потребують актуалізації, тільки вони і фільтруються після її активації
UC11	Інформаційний актив успішно змінено
UC12	Отримано лист про зміну інформаційного активу
UC13	Після зміни інформаційного активу, він зникає із загального переліку, так як потребує рецензії
UC14	Інформаційний актив рецензовано і він з’явився у загальному переліку
UC15	Змінена дата актуалізації після актуалізації інформаційного активу
UC16	Запит на консалтинг успішно створено
UC17	Лист по консалтингу успішно отримано
UC18	Кнопки у навчанні функціонують та дають змогу переключатися між навчанням
UC19	Кнопка повернення у головне меню повертає користувача у головне меню

Тестування сценаріїв використання:

4.1.1 Сценарій використання UC01 – результат відсутності створення нового інформаційного активу наведено на рисунку 4.1. На рисунку видно, що не заповнене одне поле і воно підсвічене червоним.

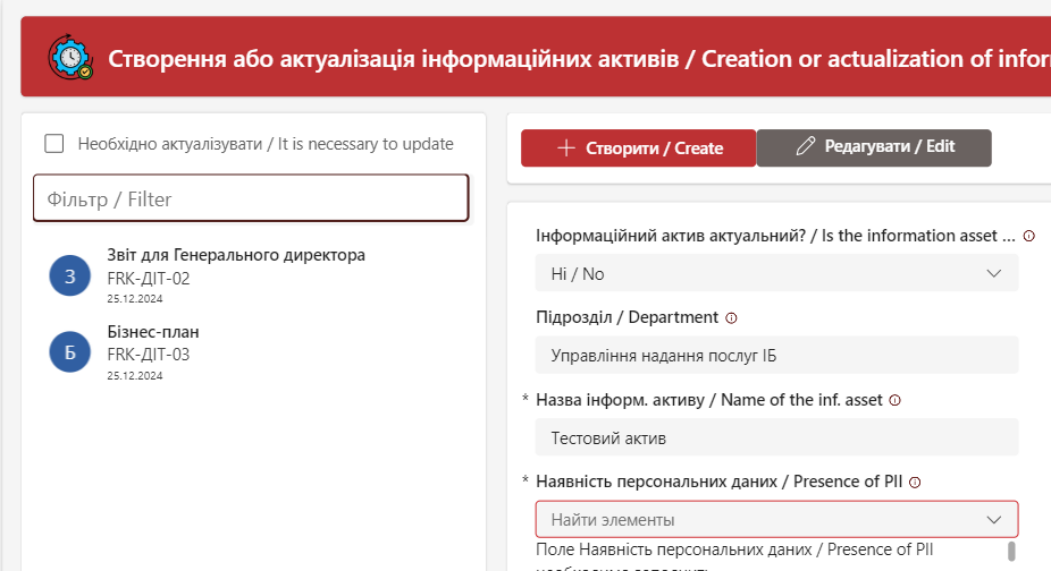


Рисунок 4.1 – Помилка при створенні активу

4.1.2 Сценарій використання UC02 – результат створення нового інформаційного активу наведено на рисунку 4.2. Варто відмітити, що створення і актуалізація повертають одне і теж системне повідомлення про «оновлення» інформаційних активів.

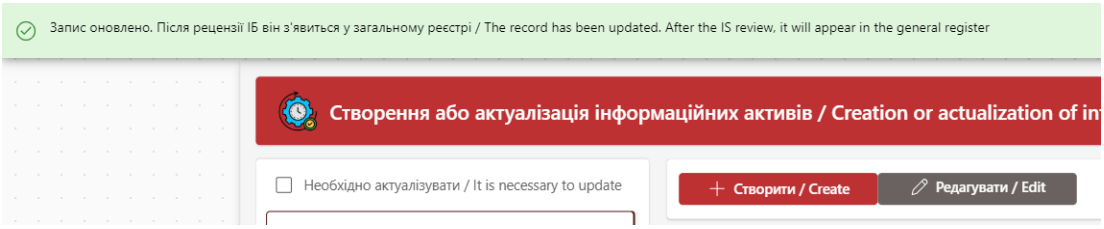


Рисунок 4.2 – Результат оновлення активу

4.1.3 Сценарій використання UC03 - результат отримання листа наведено на рисунку 4.3. Варто відмітити, що створення і актуалізація повертають листи з контекстом «зміна» в обох випадках.

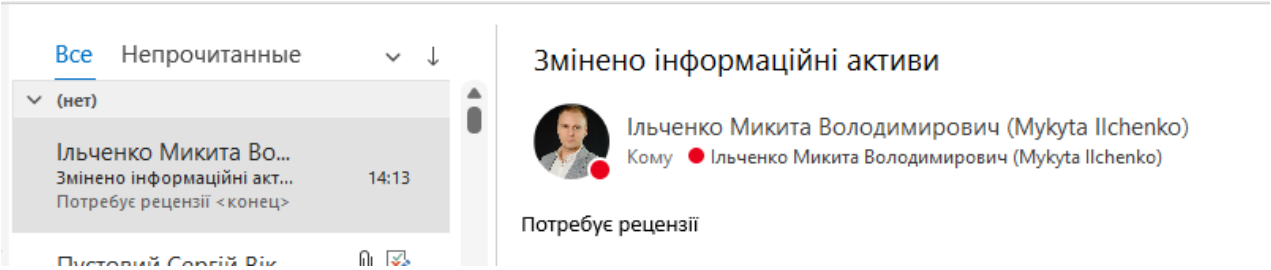


Рисунок 4.3 – Отриманий лист про зміну інформаційних активів

4.1.4 Сценарій використання UC04 – результат відображення відсутній, так як актив потребує рецензії. Результат наведено на рисунках 4.4 та 4.5.

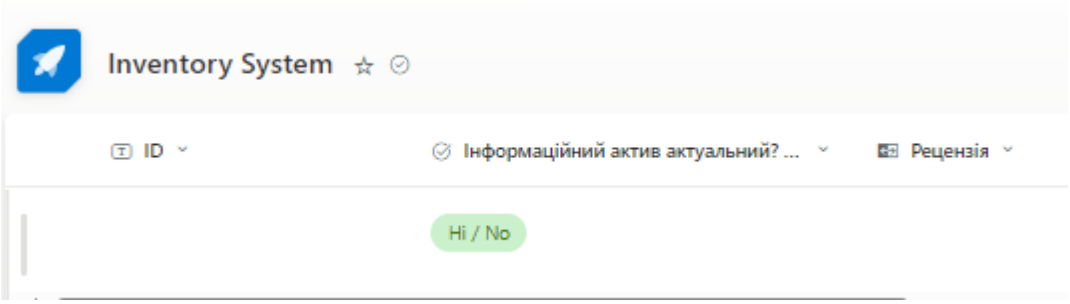


Рисунок 4.4 – Порожній статус рецензії при створенні або зміні активу

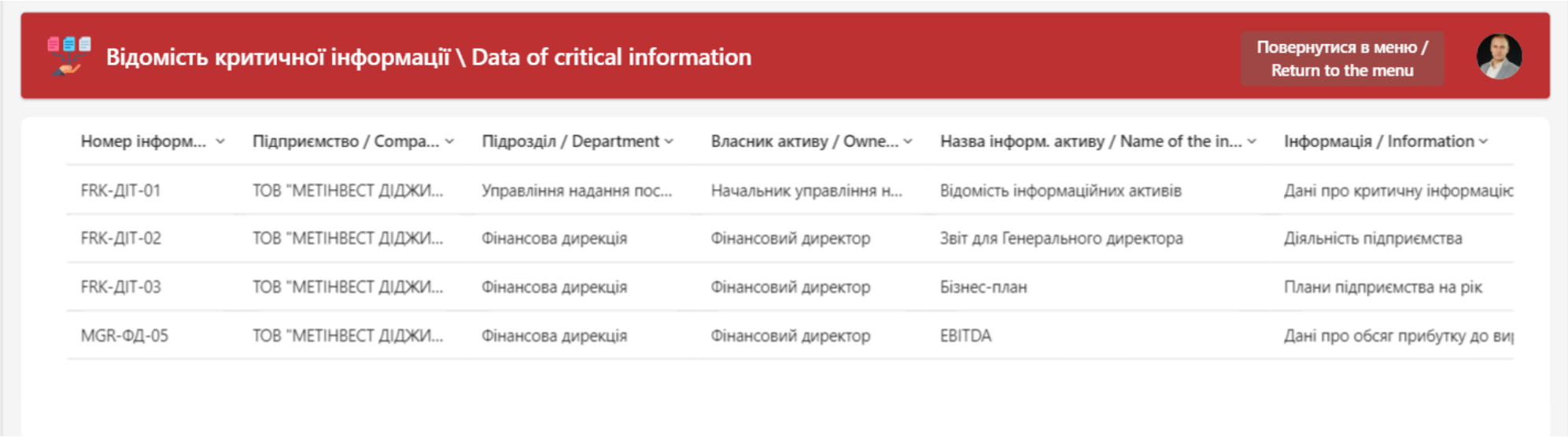


Рисунок 4.5 – Відсутній новий тестовий інформаційний актив у загальному списку, якщо він не рецензований

4.1.5 Сценарій використання UC05 – після встановлення статусу рецензії для нового тестового активу, він відображається у загальному списку. Результат наведено на рисунках 4.6 та 4.7.

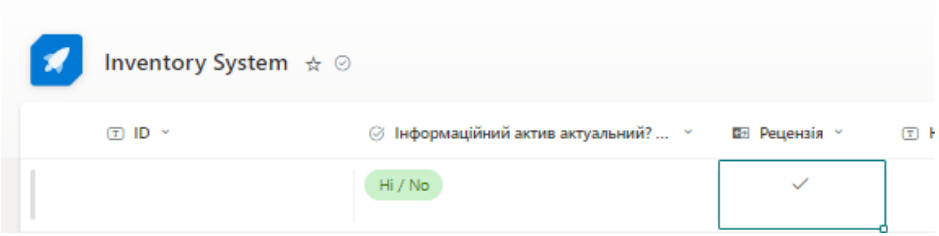


Рисунок 4.6 – Встановлення статусу рецензії

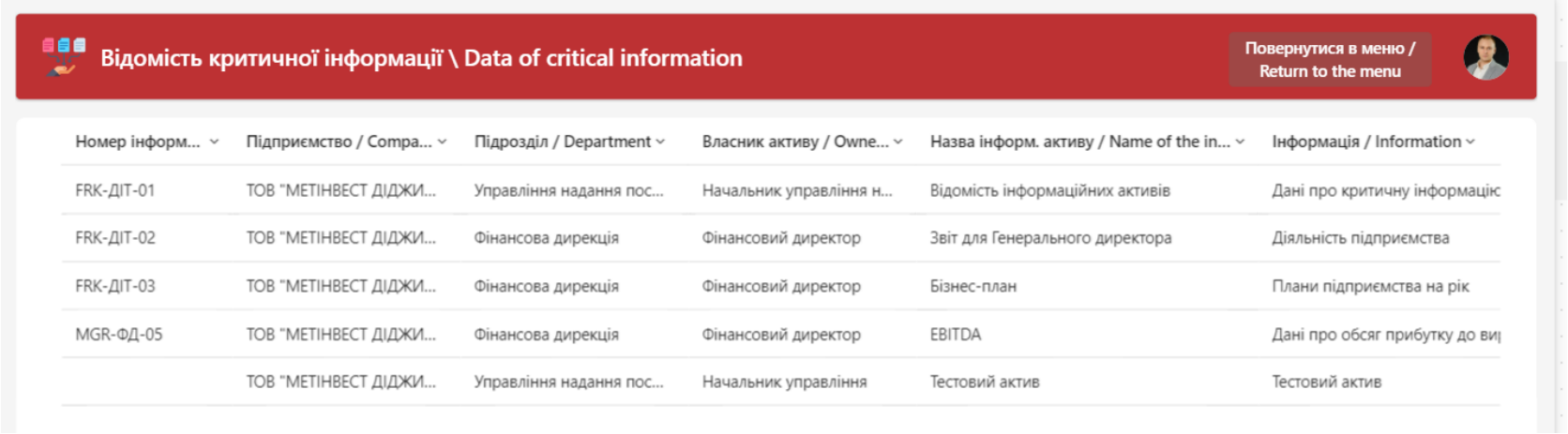


Рисунок 4.7 – Поява інформаційного активу в переліку після встановлення статусу рецензії

4.1.6 Сценарій використання UC06 – отриманий лист на тестового власника (відповідального) наведено на рисунку 4.8.

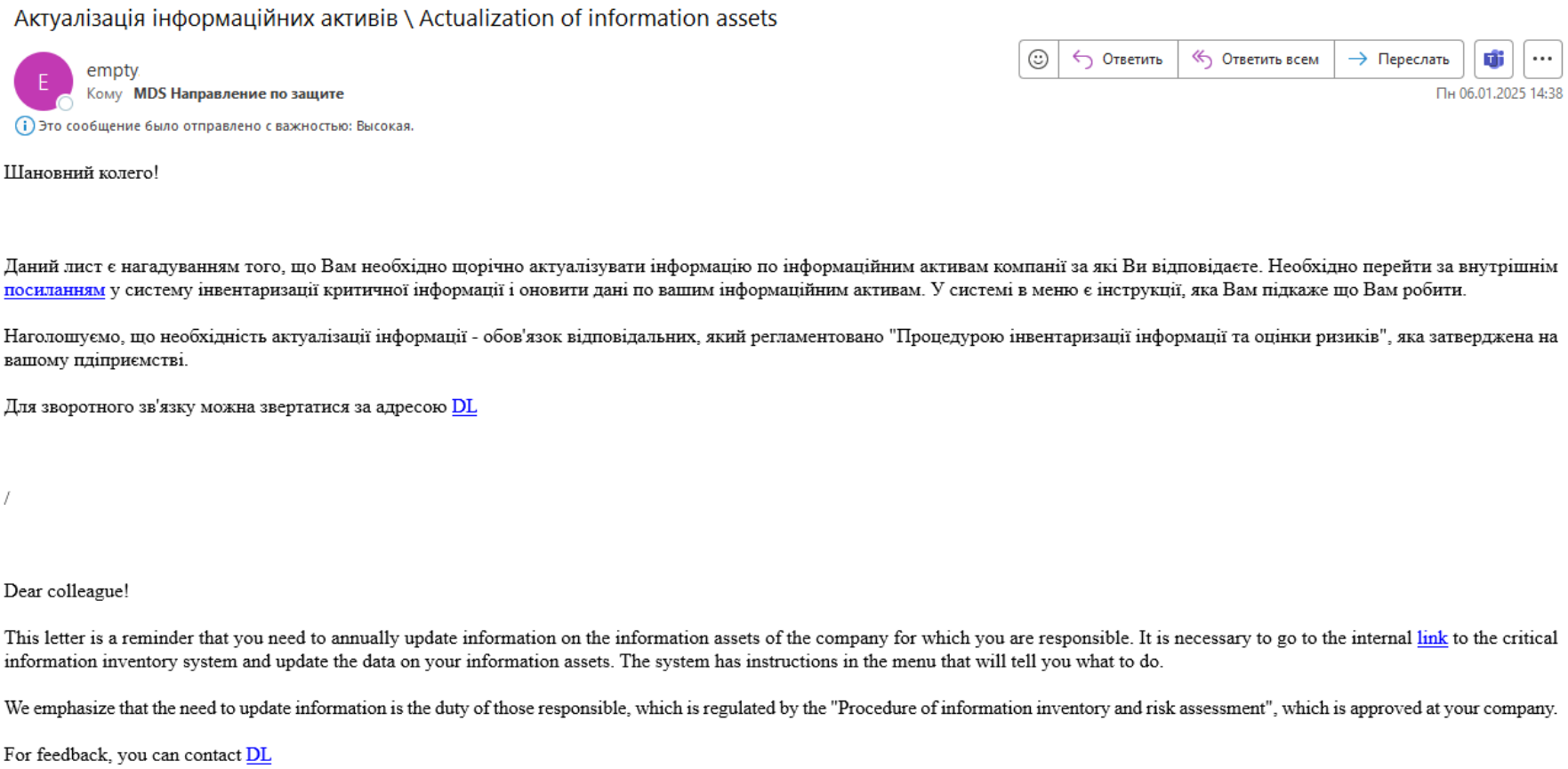


Рисунок 4.8 – Отриманий лист на відповідальну особу

4.1.7 Сценарій використання UC07 – результат відпрацювання потоку наведено на рисунку 4.9.

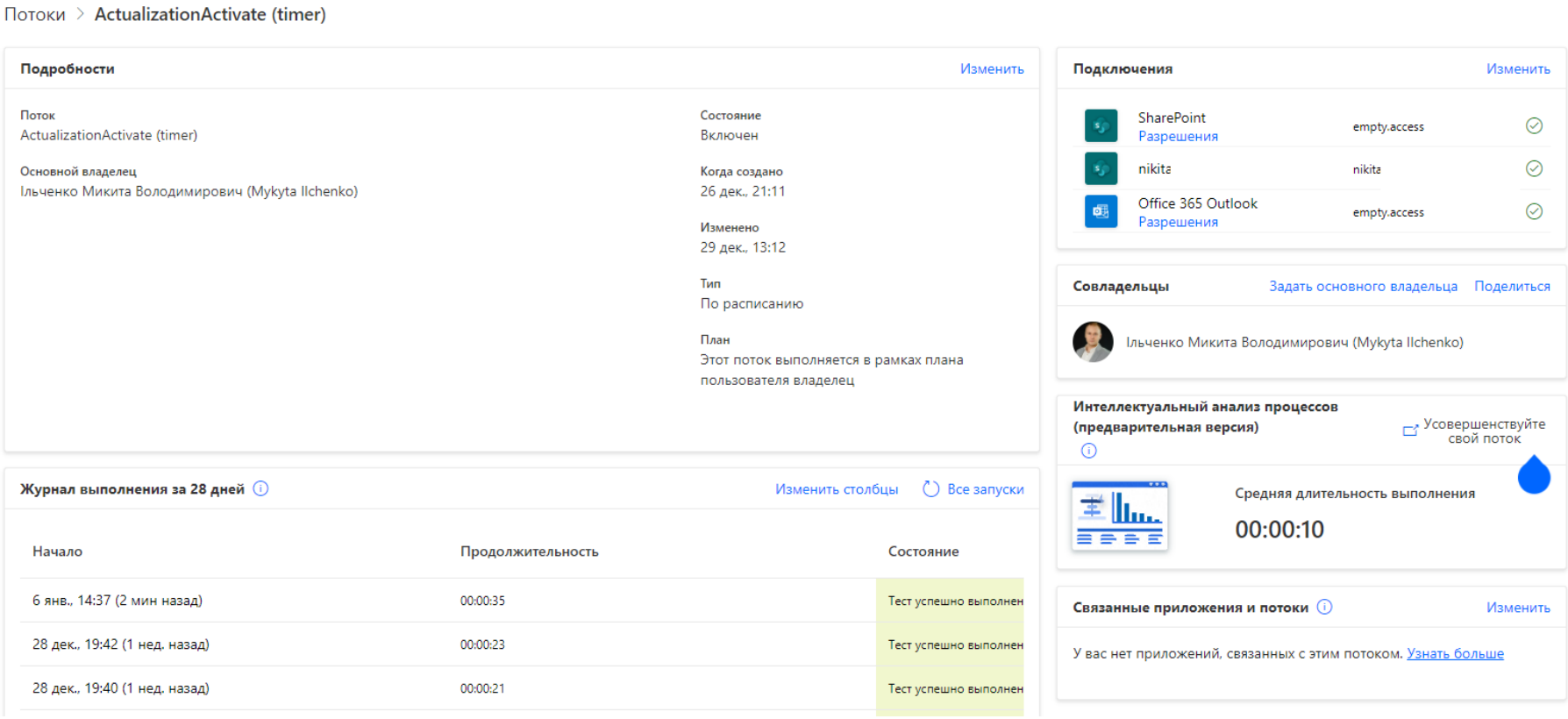


Рисунок 4.9 – Результати тестування з Microsoft Flow

4.1.8 Сценарій використання UC08 – загальний перелік інформаційних активів доступний відповідальній особі наведено на рисунку 4.10. Загальна кількість тестових даних більше десяти, наявно на одному відповідальному у тестовій виборці лише чотири.

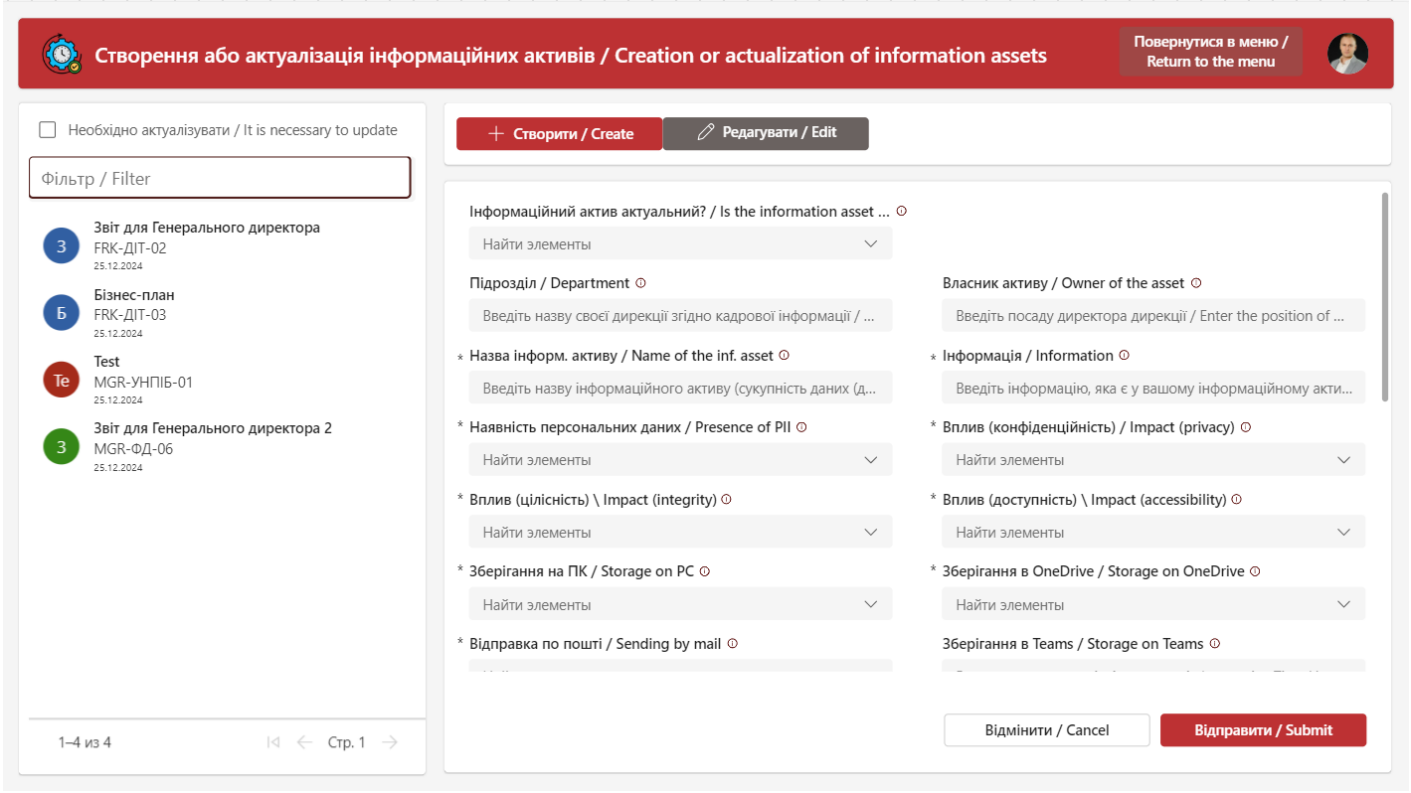


Рисунок 4.10 – Доступні інформаційні активи власника

4.1.9 Сценарій використання UC09 – результат фільтрування даних наведено на рисунку 4.11.

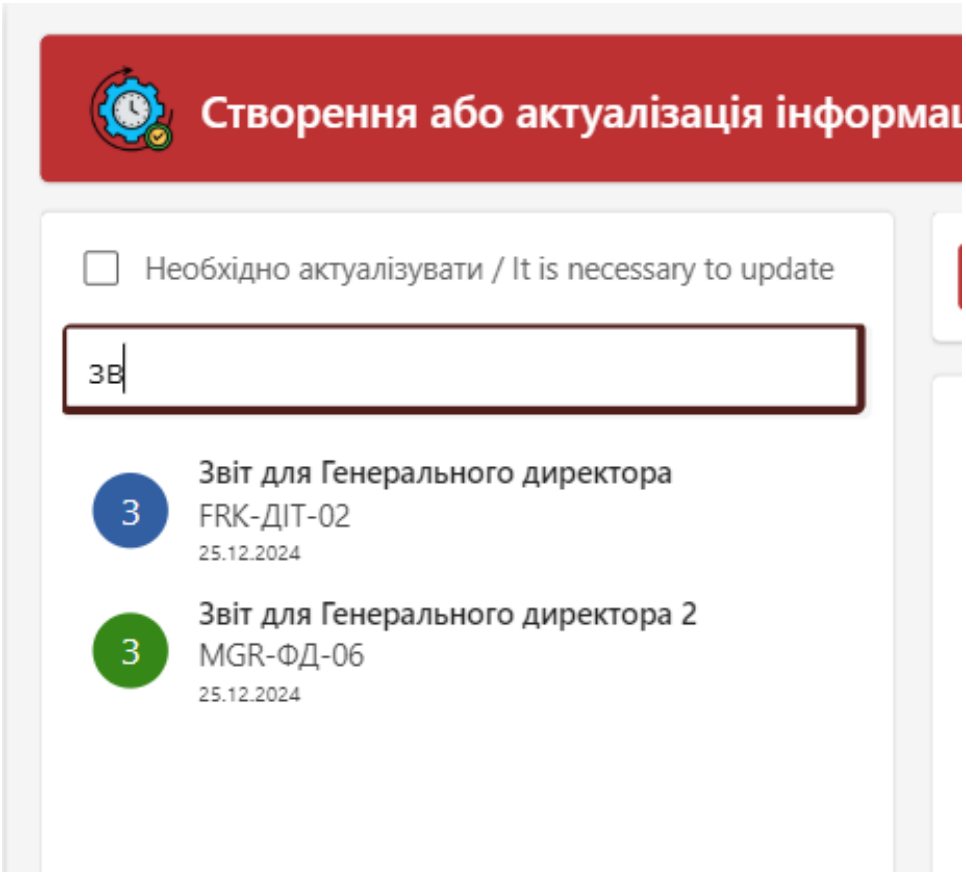


Рисунок 4.11 – Результат фільтрації

4.1.10 Сценарій використання UC10 – результат фільтрації через галочку актуалізації активів наведено на рисунку 4.12.

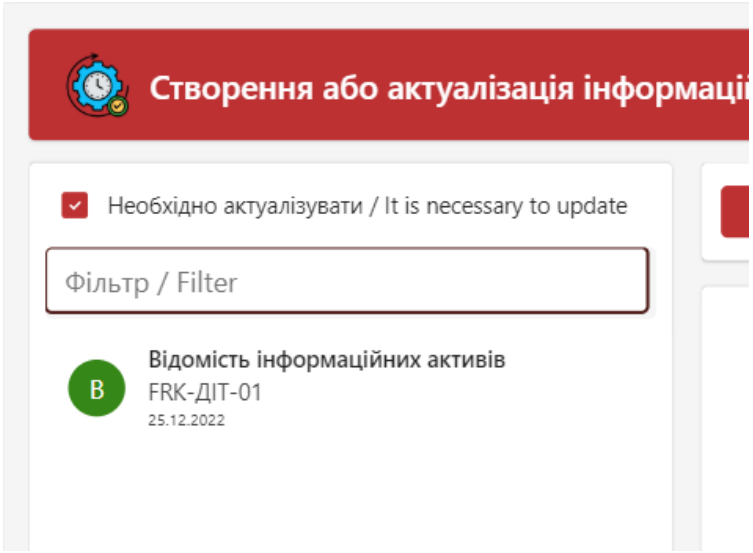


Рисунок 4.12 – Результат активації галочки по фільтру актуалізації

4.1.11 Сценарій використання UC11 – результат успішного оновлення наведено на рисунку 4.13.

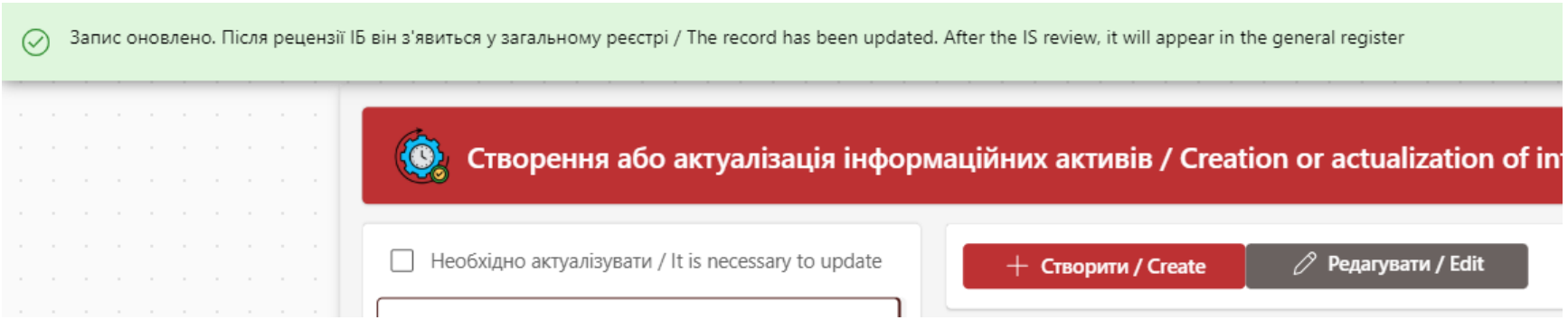


Рисунок 4.13 – Результат оновлення активу

4.1.12 Сценарій використання UC12 - результат отримання листа наведено на рисунку 4.14.

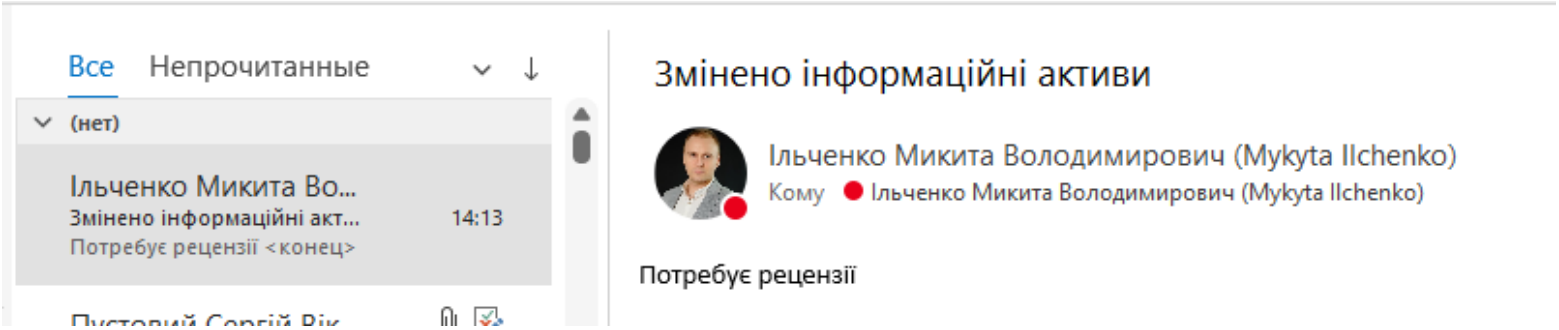


Рисунок 4.14 – Отриманий лист про зміну інформаційних активів

4.1.13 Сценарій використання UC13 – результат аналогічний UC04.

4.1.14 Сценарій використання UC14 – результат аналогічний UC05.

4.1.15 Сценарій використання UC15 – результат зміни дати наведено на рисунку 4.15.

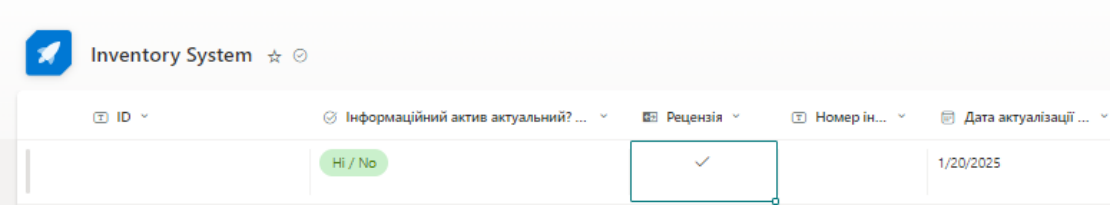


Рисунок 4.15 – Змінена дата у Дата актуалізації

4.1.16 Сценарій використання UC16 – результат створення запиту наведено на рисунку 4.16.

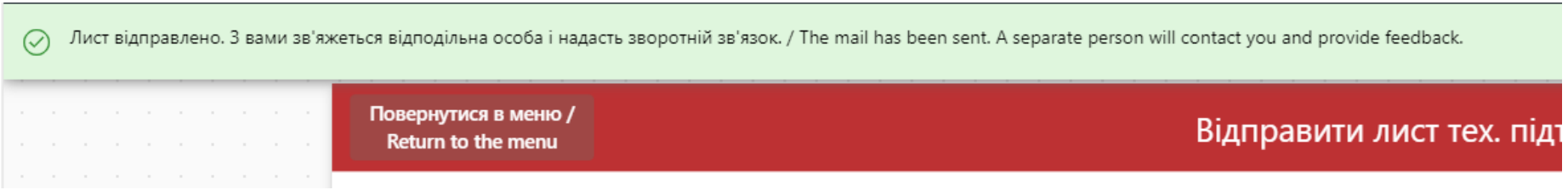


Рисунок 4.16 – Повідомлення про успішне відправлення листа

4.1.17 Сценарій використання UC17 – результат отримання листа наведено на рисунку 4.17.

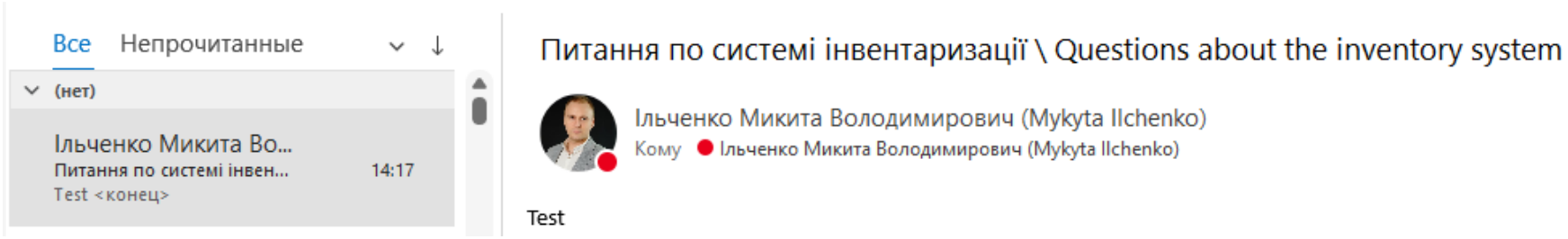


Рисунок 4.17 – Отриманий лист про необхідність надання консалтингу

4.1.18 Сценарій використання UC18 – кнопки функціонують у двох режимах:

– Режим 1 – переключення між точками, які відповідають чотирьом станам навчання, а саме створенню, актуалізації, перегляду та створенню запитів на консалтинг;

– Режим 2 – послідовне переключення через візуальні трикутники «право» і «ліво».

Візуалізувати результат не має сенсу, так як це можливо побачити лише у відео потоці.

4.1.19 Сценарій використання UC19 – кнопка функціонує і повертає користувача у головне меню, працює через посилання з плавним переходом. Візуалізувати результат не має сенсу, так як це можливо побачити лише у відео потоці.

4.2 Виконання бізнес-вимог

Продублюємо інформацію про наявні бізнес-вимоги у таблицю 4.2.

Таблиця 4.2 – Бізнес-вимоги

Посилання	Вимоги	Пріоритет
BR01	Централізована база даних для всіх інформаційних активів.	M
BR02	Інтуїтивно зрозумілий користувацький інтерфейс.	S
BR03	Підтримка та навчання користувачів системи.	S
BR04	Автоматизація актуалізації даних.	M
BR05	Автоматичне оновлення даних з зовнішніх джерел.	M

Продовження таблиці 4.2

Посилання	Вимоги	Пріоритет
BR06	Використання технологій, які зможуть використовувати або інтегрувати Office365 з рішенням	M
BR07	Мінімально достатня ціна використання рішення (політика ліцензування), яке доступне без бюджетуванню окремих ліцензій.	M
BR08	Система повинна бути розробленою згідно вимог інформаційної безпеки замовника, які наведені у Додатку Б.	M

Виконання вимог:

3.4.1 BR01 – усі створювані інформаційні активи та ті, які актуалізуються, знаходяться в одній централізованій базі, яка розміщена в Sharepoint Online

3.4.2 BR02 – інтерфейс, який розроблено, має максимально просте сприйняття і розділений на зрозумілі інтерфейси з інтуїтивною назвою та підказками. На скільки вимога виконана покаже продуктивна експлуатація та зворотній зв’язок користувачів.

3.4.3 BR03 – для виконання даної вимоги розроблено окремий інтерфейс, який допоможе користувачу підвищити свою обізнаність та отримати відповіді по використанню системи.

3.4.4 BR04 – для виконання даної вимоги розроблено паралельний процес у Microsoft Flow, який автоматизує перевірку актуальності інформаційних активів згідно їх дати та відправляє лист відповідальній особі щомісячно до тих пір, поки власник не актуалізує дані.

3.4.5 BR05 – використана архітектура має підключення, які автоматично передають або приймають дані із компонентів системи.

3.4.6 BR06 – використана архітектура має компоненти, які легко інтегруються з іншими продуктами Office365. Тісна інтеграція можлива за рахунок внутрішньої екосистеми Microsoft.

3.4.7 BR07 – використана архітектура має компоненти, які входять до плану ліцензування P1 та P2, які вже придбані та не потребують додаткового бюджетування. Використані компоненти не відносяться до рівня Premium

3.4.8 BR08 – деталізація виконання вимог інформаційної безпеки уточнена у п. 4.3.

4.3 Виконання вимог інформаційної безпеки

Деталізація вимог інформаційної безпеки надана у Додатку Б. Загальний коментар до вимог – використовується хмарна архітектура Microsoft, яка по замовчуванню має відповідність різнім світовим стандартам з безпеки. Виконання вимог:

4.3.1 ISR01 – архітектура системи не містить зайвих або надлишкових взаємозв’язків, мережева зв’язність повністю хмарна та внутрішня без додаткових налаштувань.

4.3.2 ISR02 – компонент Power Apps має можливість інтегруватися та контролюватися умовним доступом замовника (Azure AD Conditional Access).

4.3.3 ISR03 – компоненти архітектури системи мають змогу контролюватися Azure Defender for Cloud при наявних ліцензіях.

4.3.4 ISR04 – компоненти архітектури повністю хмарні та підтримують сучасні протоколи шифрування даних, включно з TLS 1.2 та вище.

4.3.5 ISR05 – в архітектурі системи використовується один сервісний обліковий запис, який використовуються для запуску завдань

в Power Automate та читання або запису інформації до бази даних, інших прав обліковий запис не має.

4.3.6 ISR06 – сесії та облікові записи контролюються наявним постачальним посвідчень ідентифікації Azure AD, правила встановлюються Microsoft.

4.3.7 ISR07 – компоненти системи мають інтеграцію з Azure Log Analytics та Compliance Audit та мають журнали не менше 1 місяця глибини.

4.3.8 ISR08 – наявні журнали в Azure Log Analytics та Compliance Audit мають необхідну деталізацію журналів згідно вимог.

4.3.9 ISR09 - наявні журнали в Azure Log Analytics та Compliance Audit мають необхідну деталізацію журналів згідно вимог.

4.3.10 ISR10 – за оновлення компонентів архітектури відповідає Microsoft (SaaS сервіс), включно з контролем вразливостей.

4.3.11 ISR11 – компоненти архітектури обов’язково використовують автентифікацію користувача, анонімні користувачі не допускаються.

4.3.12 ISR12 – компоненти автентифікації архітектури мають змогу використовувати SSO.

4.3.13 ISR13 - компоненти автентифікації архітектури мають змогу використовувати Azure AD Conditional Access та виклик Azure AD MFA.

4.3.14 ISR14 - компоненти автентифікації архітектури використовують сучасні бібліотеки автентифікації, які надає Microsoft, включно з названими.

4.3.15 ISR15 – система не має вбудованих замовлених ролей, які призначені для користувачів. Доступ до системи має кожен користувач домену замовника. Доступ до інформаційних активів певного підприємства або певного власника фільтрується на базі моделі

ABAC згідно атрибутів, які заповнені у картці користувача (пошта, підприємство).

4.3.16 ISR16 - компоненти автентифікації архітектури мають змогу використовувати Azure AD Conditional Access та виклик Azure AD Identity Protection.

4.3.17 ISR17 – компоненти автентифікації архітектури використовують сучасні бібліотеки автентифікації, які надає Microsoft, включно з використанням хешування та шифрування.

4.3.18 ISR18 - компоненти архітектури розміщені в хмарних сервісах Microsoft та підтримують внутрішнє шифрування даних, дані, що передаються, використовують захищений HTTPS протокол

4.3.19 ISR19 – інформація, яка буде зберігатися в системі ідентифікована та має наступні атрибути:

– Інформація з обмеженим доступом – скорочений список інформаційних активів, який доступний усім користувачам підприємства;

– Конфіденційна інформація – повний список інформаційних активів з усіма атрибутами, доступ до яких має лише відповідальна особа та інформаційна безпека.

4.3.20 ISR20 – архітектура системи та її компоненти описані у Розділі 3.

4.3.21 ISR21 – за резервування компонентів та даних у системі відповідає постачальник послуг Microsoft (SaaS сервіс).

4.4 Висновки по виконанню вимог

Якщо підсумовувати результати по розробці ПЗ та його тестуванню, то можна прийти до висновку:

– Розроблені сценарії використання успішно протестовані та готові до тестової продуктивної експлуатації.

– Система розроблювалась згідно бізнес-вимог, вони перевірені, система їм відповідає.

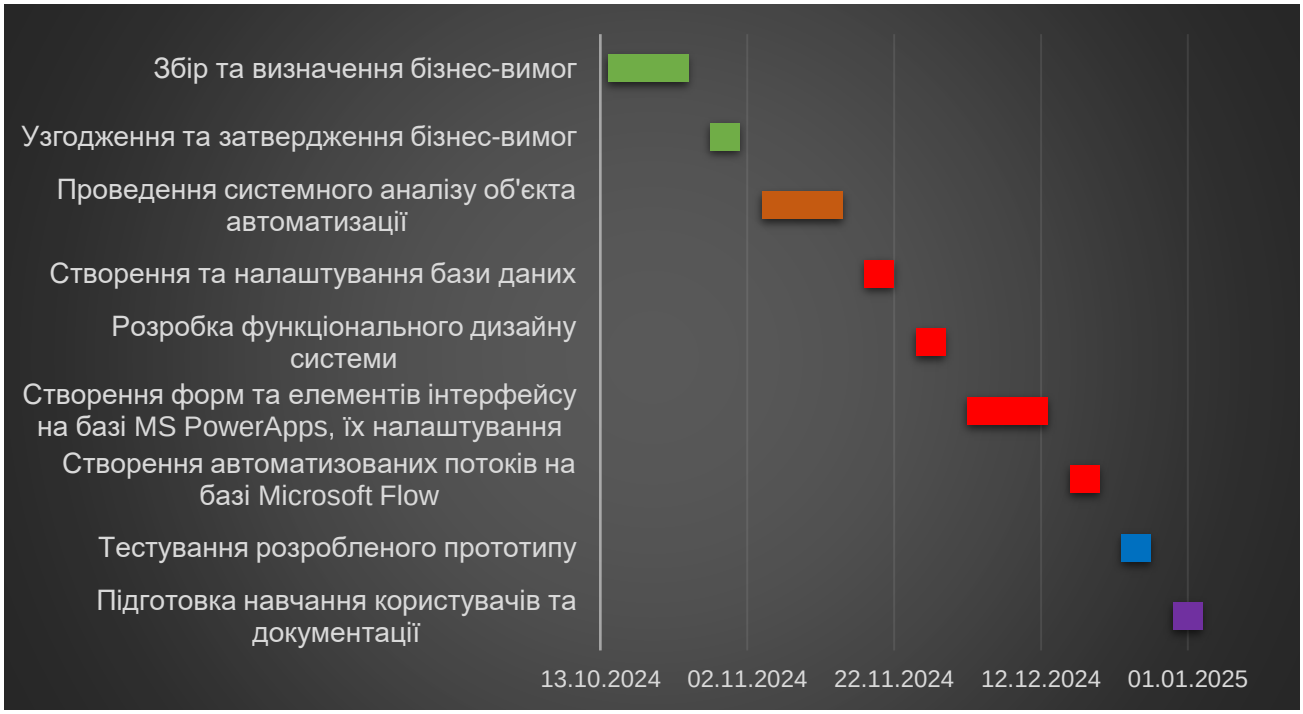
– Система розроблювалась згідно вимог інформаційної безпеки, вони перевірені, система їм відповідає.

Оцінка економічної доцільності розробки, ефектів та дослідження досягнутої мети буде описано у Розділі 5.

РОЗДІЛ 5. ЕКОНОМІЧНІ РОЗРАХУНКИ

5.1 Оцінка трудовитрат по проєкту та кошторис

Проєкт та розробка ПЗ розроблялися напротязі жовтня-грудня 2024 року з різною тривалістю та трудовитратами. На рисунку 5.1 зображена діаграма графіку проєкту, а в таблиці 5.1 вказані дані про тривалості проєкта та приблизним трудовитратам.



Діаграма 5.1 – Етапи та графік проєкту

Таблиця 5.1 – Деталізація проєкту

Назва завдання	Роль	Старт	Кінець	Трудовитрати (%)	Трудовитрати (годин)	Тривалість (днів)
Збір та визначення бізнес-вимог	BA Senior	14.10.2024	25.10.2024	7,00%	6,72	11

Продовження таблиці 5.1

Назва завдання	Роль	Старт	Кінець	Трудовитрати (%)	Трудовитрати (годин)	Тривалість (днів)
Узгодження та затвердження бізнес-вимог	BA Senior	28.10.2024	01.11.2024	10,00%	4,00	4
Проведення системного аналізу об'єкта автоматизації	BA Senior	18.11.2024	15.11.2024	25,00%	24,00	11
Створення та налаштування бази даних	Power Apps Developer Junior	25.11.2024	22.11.2024	25,00%	10,00	4
Розробка функціонального дизайну системи	Power Apps Developer Junior	02.12.2024	29.11.2024	25,00%	10,00	4
Створення форм та елементів інтерфейсу на базі MS PowerApps, їх налаштування	Power Apps Developer Junior	16.12.2024	13.12.2024	25,00%	24,00	11
Створення автоматизованих потоків на базі Microsoft Flow	Power Apps Developer Junior	23.12.2024	20.12.2024	25,00%	10,00	4
Тестування розробленого прототипу	QA Tester Junior	30.12.2024	27.12.2024	15,00%	6,00	4
Підготовка навчання користувачів та документації	BA Senior	28.10.2024	03.01.2025	20,00%	8,00	4
Всього:		**14.10.2024**	**03.01.2025**	**19,67%**	**129,01**	**81**

В проєкті працювали співробітники з наступними ролями, розподілом трудовитрат та середньою вартістю (таблиця 5.2).

Таблиця 5.2 – Розподіл ролей в проєкті та їх вартість

Роль	Вартість однієї години ролі (грн)	Кількість годин в проєкті	Загальний бюджет (грн)
Business analyst (senior)	1200	43,72	52464
Power Apps developer (junior)	700	44	30800
QA tester (junior)	600	6	3600
		Всього:	**86864**

З урахуванням того, що вартість платформи наявного програмного забезпечення входить до наявних ліцензій, а хмарні технології нам дають можливість не витрачати кошти на серверні потужності або обслуговування ЦОД, бюджет на розробку є фінальним. Години, як і вартість годин, є приблизною величиною і тому округлимо бюджет до 87 тис. грн.

5.2 Цільові ефекти та користь від системи

Нагадаємо які самі проблеми ми хотіли вирішити через розробку системи автоматизації:

– Відсутність актуального єдиного переліку інформації інформаційних активів, які є у наявності у великій кількості окремих файлів. При формування у ручному режимі спільного файлу, є необхідність і його підтримувати в актуальному стані після зміни будь-якого окремого;

– Не системність частини записів, які ведуться у формах процесу, що породжує складність роботи з масивами даних;

– Формування запитів на періодичну актуалізацію у ручному режимі;

– Необхідність порівняння даних в пошті та окремих файлах при питаннях перевірки цілісності даних.

Сформуємо основні контрольні точки, які могли покращити загальну ефективність процесу:

5.2.1 Зниження трудовитрат інформаційної безпеки на підтримку окремих файлів Excel, так як інформація тепер зберігається в єдиній базі і там же оброблюється власниками.

Підготовка даних у різних розрізах не буде потребувати окремої підтримки і копіювання даних з різних файлів, дані можливо експортувати одразу з єдиного місця. Якщо допустити:

– Система підтримує 20 підприємств;

– Кожне підприємство підтримує до 12 дирекцій;

– Співробітник інформаційної безпеки кожен раз витрачає зайві 15 хвилин щорічно на кожну дирекцію для уніфікації записів і їх централізації. Також можливі окремі запити по неплановій зміні, що буде породжувати необхідність зміни даних в обох місцях (локальному і централізованому), таких кейсів до двох щомісячно, що еквівалентно зайвим 20 хвилинам щомісячно;

– Якщо підсумувати економію, то співробітник інформаційної безпеки не буде витрачати щорічно: (20 підприємств * 12 дирекцій * 15 хвилин + 12 місяців * 20 хвилин) = 3840 хвилин або 64 години.

5.2.2 Стандартизація формату і типів даних дозволяє витрачати менше часу інформаційній безпеці на приведення до цілісного варіанту даних в базі при заповненні нових інформаційних активів або актуалізації наявних. Розрахунок по даному пункту вказаний в пункті 5.2.1;

5.2.3 Автоматизація процесу актуалізації інформації у відомостях і зниження трудовитрат інформаційної безпеки на формування окремих файлів, листів і їх підтримку.

Підготовка даних для актуалізації потребує:

– Формуванню окремого листа з шаблоном тексту (15 хвилин щоквартально);

– Відправки окремого листа на окремого власника з вкладанням відомості в Excel (10 хвилин на кожний лист щорічно);

– Періодичному нагадуванню власникам інформації про необхідність зворотного зв'язку (5 хвилин на нагадування для 40% від об'єму відомостей);

– Якщо підсумувати економію, то співробітник інформаційної безпеки не буде витрачати щорічно: (4 квартали * 15 хвилин + 20 підприємств * 12 дирекцій * 10 хвилин + 20 підприємств * 12 дирекцій * 40% * 5 хвилин) = 2940 хвилин або 49 годин.

5.2.4 Систематизація і безальтернативна обробка власниками інформації даних у єдиному місці і єдиній системі, що дасть змогу більш якісно актуалізувати і переглядати дані у формі замість даних в Excel. Економії не планується, підвищується лише якість обробки і знижується кількість помилок при обробці;

5.2.5 Відсутність розпорошування даних по всій інфраструктурі і їх централізації в єдиному місці з доступом усіх користувачів, більш висока вірогідність успішних маркетингових компаній по системі, підвищення рівня преміальності сервісу та послуги по інвентаризації критичної інформації. Економії не планується, планується зниження ризиків інформаційної безпеки при більш частому користуванню користувачами даних системи і підвищенню їх обізнаності в питаннях роботи з критичними даними. Зменшується ризик інцидентів ІБ.

Якщо підсумувати загальні ефекти:

– При допущенні того, що кошт одного часу співробітника інформаційної безпеки рівня Senior дорівнює 1 тис. грн, економія через різ досягне позначки у 113 тис. грн ((64 год. + 49 год.) * 1 тис. грн), а через 3 роки з урахуванням інфляції у 10% (дуже оптимістичний сценарій) економія досягне позначки у 374 тис. грн ((64 год. + 49 год.) * 1 тис. грн + (64 год. + 49 год.) * 1 тис. грн * 1,1 + (64 год. + 49 год.) * 1 тис. грн * (1+0,10) * 2);

– Підвищиться якість і уважність обробки даних власниками інформації;

– Підвищиться рівень преміальності сервісу та послуги;

– Підвищиться рівень обізнаності користувачів і знизиться ризик інциденту ІБ.

ЗАГАЛЬНІ ВИСНОВКИ

В умовах швидкого розвитку технологій та зростання кількості кібератак сучасні підприємства стикаються з необхідністю забезпечення кіберстійкості. Одним з важливих елементів цього процесу є інвентаризація критичної інформації. Процес інвентаризації дозволяє виявити та класифікувати інформаційні активи (форму в якій обробляється інформація), що є критично важливими для підприємства, а також ідентифікувати потенційні ризики та загрози для їх безпеки. Процес необхідний для ефективного управління інформаційною безпекою, збереженням даних та їх плануванням їх захисту, зменшенням ризиків впливу на репутацію компанії, довіри клієнтів та партнерів, а також її фінансової стабільності.

Одним з ключових аспектів інвентаризації критичної інформації є її відповідність міжнародним стандартам, таким як ISO/IEC 27001:2022. Цей стандарт надає керівництво щодо встановлення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Відповідність стандартам ISO дозволяє підприємствам організувати процеси інвентаризації та управління ризиками більш структуровано, що сприяє підвищенню загальної ефективності системи безпеки. Крім того, наявність сертифікації ISO 27001 може бути додатковою перевагою при співпраці з партнерами та клієнтами, оскільки це підтверджує високу якість управління інформаційною безпекою на підприємстві.

Процес інвентаризації критичної інформації допомагає підприємствам зосередити ресурси на найбільш важливих активах, знижуючи при цьому витрати та підвищуючи ефективність захисту. В умовах обмежених ресурсів та високої конкуренції важливо забезпечити, щоб вкладені в безпеки інвестиції мали максимальний ефект. Автоматизація процесів інвентаризації, впровадження

інтелектуальних систем для аналізу та оцінки ризиків, а також інтеграція з іншими системами управління інформаційною безпекою дозволяють підприємствам оптимізувати використання ресурсів та підвищити загальну ефективність роботи.

Інвентаризація критичної інформації включає в себе кілька етапів: виявлення інформаційних активів, їх класифікація, оцінка ризиків та загроз, а також розробка заходів для їх мінімізації (може існувати окремо). Виявлення інформаційних активів передбачає створення повного переліку всіх даних, що є критичними для роботи підприємства. Класифікація інформаційних активів дозволяє визначити їх важливість та пріоритетність, що допомагає у подальшому розподілі ресурсів для їх захисту. Оцінка ризиків та загроз включає в себе аналіз потенційних вразливостей та ймовірності їх реалізації, а також визначення можливих наслідків для підприємства. На основі цього аналізу розробляються заходи для мінімізації ризиків, включаючи впровадження технічних, організаційних та процедурних заходів безпеки.

Розвиток процесу інвентаризації критичної інформації включає кілька ключових напрямків:

– автоматизація збору та обробки даних;

– використання сучасних технологій, таких як машинне навчання та штучний інтелект, для підвищення точності та швидкості процесів інвентаризації;

– впровадження інтелектуальних систем для аналізу та оцінки ризиків, що дозволяють прогнозувати можливі загрози та розробляти заходи для їх запобігання.

Великі підприємства для ефективної обробки цього процесу повинні мати систему, яка буде мати можливість електронно обслуговувати процеси збору та актуалізації інформаційних активів за допомогою розроблених стандартизованих даних з урахуванням

сучасних можливостей інтеграцій зі штучним інтелектом. Зв’язок зі штучним інтелектом дасть можливість аналітикам, інформаційній безпеці та бізнес-власникам інформації економити свій час для заповнення і скорочувати загальні терміни процесу.

В межах проєкту було досягнуто:

– Дослідження предметної області та виявлення процесних та функціональних дефіцитів на підприємстві в процесах інвентаризації критичної інформації;

– Розробки бізнес-вимог та реалізації інформаційної системи, яка задовольняє ці вимоги, включно з вимогами інформаційної безпеки;

– Протестовані сценарії використання системи, що дає змогу зробити певний пілот в одній дирекції одного з підприємств;

– Зроблені допущення ефективності проєкту, які полягають:

a) Економії у 113 тис. грн при експлуатації системи двадцятьма підприємствами в період одного року та 374 тис. грн в період до трьох років з витратами на розробку системи у 87 тис. грн;

b) Підвищиться якість і уважність обробки даних власниками інформації;

c) Підвищиться рівень преміальності сервісу та послуги;

d) Підвищиться рівень обізнаності користувачів і знизиться ризик інциденту ІБ.

ДОДАТОК А. ВІДОМОСТІ РОБОТИ

Формат	№ п/п	Назва документу	Найменування об'єкту або виробу	Кількість сторінок
А4	1	Пояснювальна записка	КЦТПАР.122-22-1м.01.00.КР.ПЗ	136
Графічна частина				
А4	2	Актуальність	КЦТПАР.122-22-1м.02.00.КР.ПЛ	1
А4	3	Мета, об’єкт, предмет дослідження	КЦТПАР.122-22-1м.03.00.КР.ПЛ	1
А4	4	Аналіз предметної області	КЦТПАР.122-22-1м.04.00.КР.ПЛ	5

ДОДАТОК Б. ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Таблиця Б.1 – Вимоги інформаційної безпеки

Номер вимоги	Опис вимоги
ISR01	Перелік мережевих взаємодій повинний бути мінімально достатнім для забезпечення бізнес-процесів
ISR02	Публікація в Інтернет додатку виконується з використанням умовного доступу (conditional access)
ISR03	Усі компоненти системи повинні бути забезпечені наявним антивірусним ПЗ
ISR04	Виклики при інтеграціях повинні організовуватися з використанням криптографічних стійких алгоритмів шифрування (TLS 1.2 та вище)
ISR05	Права доступу технологічних облікових записів повинні обмежуватися мінімально достатніми правами
ISR06	Строк життя неактивної сесії повинен бути обмежений та параметризований
ISR07	Збір і збереження журналів в оперативному доступі не менше 30 днів
ISR08	Збираються журнали: журнал дій користувача, у т. ч. події входу, виходу, доступу до інтерфейсу; журнал дій адміністратору, у т. ч. події додавання або видалення повноважень.

Продовження таблиці Б.1

Номер вимоги	Опис вимоги
ISR09	В журналах фіксуються події: дата і час, адреса\назва пристрою, суб’єкт, об’єкт, опис події, результат успіху\невдачі
ISR10	Відсутність вразливостей рівня Critical, High, Medium
ISR11	Обов’язкова автентифікація користувача та заборона анонімних користувачів
ISR12	Підтримка SSO (Single-Sign On) з використанням AD або Azure AD
ISR13	Підтримка та використання Azure AD MFA
ISR14	Використання бібліотек автентифікації Microsoft (MSAL), Azure SDK
ISR15	Підтримка рольової моделі до системи для авторизації
ISR16	Доступ в систему повинний бути обмежений географічно із заборонених держав або при наявності ризику користувача
ISR17	Дані авторизації повинні зберігатися і передаватися з використанням хешування та шифрування
ISR18	Використання захищених стандартних алгоритмів шифрування з достатньою складністю і довжиною ключа для даних, що передаються, та даних, які зберігаються
ISR19	Інформація в системі повинна бути ідентифікованою, визначений її власник і оцінена конфіденційність

Продовження таблиці Б.1

Номер вимоги	Опис вимоги
ISR20	Система повинна мати задокументовану і узгоджену архітектуру
ISR21	Система регулярно резервує свої компоненти, має задокументований план резервування та план відновлення

ДОДАТОК В. КОД ДЛЯ КОМПОНЕНТУ «TABLE» ІНТЕРФЕЙСУ «СТВОРЕННЯ АБО АКТУАЛІЗАЦІЯ ІНФОРМАЦІЙНИХ АКТИВІВ»

```
Sort(

If(And(Len(TextInput1.Text)<=0; CheckboxCanvas1.Checked = false);

Filter('Inventory System'; 'Підприємство / Company' = ПользователиOffice365.MyProfile().CompanyName; Рецензія = true; Or('Відповідальний 1' = User().Email; 'Відповідальний 2' = User().Email; 'Відповідальний 3' = User().Email; 'Відповідальний 4' = User().Email; 'Відповідальний 5' = User().Email); 'Дата актуалізації / Actualization date' > (Today()-365));

If(And(Len(TextInput1.Text)>0; CheckboxCanvas1.Checked = false);

Filter('Inventory System'; 'Підприємство / Company' = ПользователиOffice365.MyProfile().CompanyName; Рецензія = true; Or('Відповідальний 1' = User().Email; 'Відповідальний 2' = User().Email; 'Відповідальний 3' = User().Email; 'Відповідальний 4' = User().Email; 'Відповідальний 5' = User().Email); TextInput1.Text in 'Назва інформ. активу / Name of the inf. asset'&" "&'Номер інформаційного активу / Information asset id'; 'Дата актуалізації / Actualization date' > (Today()-365));

If(And(Len(TextInput1.Text)<=0; CheckboxCanvas1.Checked = true);

Filter('Inventory System'; 'Підприємство / Company' = ПользователиOffice365.MyProfile().CompanyName; Рецензія = true; Or('Відповідальний 1' = User().Email; 'Відповідальний 2' = User().Email;
```

'Відповідальний 3' = User().Email; 'Відповідальний 4' = User().Email; 'Відповідальний 5' = User().Email); 'Дата актуалізації / Actualization date' < (Today()-365));

Filter('Inventory System'; 'Підприємство / Company' = ПользователиOffice365.MyProfile().CompanyName; Рецензія = true; Or('Відповідальний 1' = User().Email; 'Відповідальний 2' = User().Email; 'Відповідальний 3' = User().Email; 'Відповідальний 4' = User().Email; 'Відповідальний 5' = User().Email); 'Дата актуалізації / Actualization date' < (Today()-365); TextInput1.Text in 'Назва інформ. активу / Name of the inf. asset'&" "&'Номер інформаційного активу / Information asset id'))));

'Номер інформаційного активу / Information asset id'; SortOrder.Ascending)

ПЕРЕЛІК ПОСИЛАНЬ

1. Fotis Kitsios, Elpiniki Chatzidimitriou, Maria Kamariotou. The ISO/IEC 27001 information security management standard: how to extract value from data in the it sector. Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece. URL: https://www.mdpi.com/2071-1050/15/7/5828 (дата звернення: 15.12.2024).

2. ISO/IEC 27001:2022 – Міжнародний стандарт управління інформаційною безпекою. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 15.12.2024).

3. Microsoft Purview: Захист інформації – Офіційна документація Microsoft, що описує інструменти захисту інформації. URL: https://learn.microsoft.com/en-us/purview/information-protection (дата звернення: 15.12.2024).

4. Privacy Engine: ISO 27001 vs NIST Cybersecurity Framework – Стаття, що порівнює ISO 27001 та NIST Cybersecurity Framework. URL: https://www.privacyengine.io/blog/iso-27001-vs-nist-cybersecurity-framework/ (дата звернення: 15.12.2024).

5. Privacy Engine: Порівняння ISO 27001 та NIST Cybersecurity Framework – Стаття, що аналізує відмінності та подібності двох міжнародних стандартів кібербезпеки. URL: https://www.privacyengine.io/blog/comparing-iso-27001-and-nist-key-differences/ (дата звернення: 15.12.2024).

6. Вацлавик О., Явин Х. Технології ідентифікації і аналізу конфіденційних даних в DLP системах. Львівський державний університет безпеки життєдіяльності, Львів, Україна. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/5337/1/2.pdf (дата звернення: 15.12.2024).

7. Відео про операції з масивами в Power Automate - Відео на YouTube, де показано, як працювати з масивами в Power Automate. URL: https://www.youtube.com/user/sixtyfiveford (дата звернення: 19.12.2024).

8. Відео про створення програми для відстеження запасів в Power Apps - Відео на YouTube, де показано, як створити програму для відстеження запасів в Power Apps. URL: https://www.youtube.com/post/Ugkxw1YGXgPNTO7Y_ogxloZFJ0fiAvE5767U (дата звернення: 26.12.2024).

9. Закон України "Про інформацію" – Закон, що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.12.2024).

10. Закон України "Про доступ до публічної інформації" – Закон, що визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.12.2024).

11. Закон України "Про захист персональних даних" – Нормативний акт, що регулює обробку персональних даних в Україні. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.12.2024).

12. Муравський В. Автоматизація інвентаризації в комп’ютерно-комунікаційній формі обліку. URL: https://dspace.wunu.edu.ua/bitstream/316497/25773/1/Муравський%20В..pdf (дата звернення: 15.12.2024).

13. Найшвидший спосіб додавання до масиву в Power Automate (3 методи) - Блог Метью Девані, де він розглядає різні способи

додавання елементів до масиву в Power Automate. URL: https://www.matthewdevaney.com/fastest-way-to-append-to-array-in-power-automate-3-methods/ (дата звернення: 19.12.2024).

14. Цілина М. М. Сучасні технології захисту й опрацювання конфіденційної документної інформації в організаціях і установах різних форм власності. *Бібліотекознавство. Документознавство. Інформологія. 2021.* № 4. С. 15–23. URL: https://journals.uran.ua/bdi/article/download/249320/246584 (дата звернення: 15.12.2024).

15. Нашинець-Наумова А. Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві. URL: https://core.ac.uk/download/pdf/296373018.pdf (дата звернення: 15.12.2024).

16. Обговорення на Reddit щодо дозволів доступу до списку SharePoint - Обговорення на Reddit, де користувачі обговорюють питання доступу та дозволів до списків SharePoint. URL: https://www.reddit.com/r/PowerApps/comments/19dp4xs/restrict_user_sharepoint_list_access/ (дата звернення: 19.12.2024).

17. Обговорення на форумі Power Platform щодо додавання до масиву - Обговорення на форумі Power Platform, де користувачі діляться своїми порадами та рішеннями щодо додавання елементів до масиву. URL: https://community.powerplatform.com/ (дата звернення: 19.12.2024).

18. Огляд Power Apps - Офіційна документація Microsoft, що надає огляд Power Apps. URL: https://learn.microsoft.com/en-us/power-apps/powerapps-overview (дата звернення: 25.12.2024).

19. Операції з даними в Power Automate - Офіційна документація Microsoft, що описує різні операції, які можна виконувати з даними в Power Automate. URL: https://www.youtube.com/watch?v=qxFx0hqJxj4 (дата звернення: 19.12.2024).

20. Отримання значення стовпця вибору в Power Apps - Обговорення на Stack Overflow, де користувачі шукають рішення для отримання значення стовпця вибору в Power Apps. URL: https://www.reddit.com/r/PowerBI/comments/133l06y/values_from_choices_columns_imported_from/ (дата звернення: 24.12.2024).

21. Підключення до Office 365 Users в Power Apps - Офіційна документація Microsoft, що описує підключення до Office 365 Users в Power Apps. URL: https://learn.microsoft.com/en-us/power-apps/maker/canvas-apps/connections/connection-office365-users (дата звернення: 24.12.2024).

22. Реєстрація для Power Apps Admin - Офіційна документація Microsoft, що описує процес реєстрації для Power Apps Admin. URL: https://learn.microsoft.com/en-us/power-apps/maker/signup-for-powerapps (дата звернення: 25.12.2024).

23. Робота з картками в Power Apps - Офіційна документація Microsoft, що описує роботу з картками в Power Apps. URL: https://m.youtube.com/watch?v=yizPy8_jmYI&pp=ygUOI3Bvd2VyY2FyZHNob3c%3D (дата звернення: 24.12.2024).

24. Створення та редагування зв'язків між сутностями в Power Apps - Офіційна документація Microsoft, що описує процес створення та редагування зв'язків між сутностями в Power Apps. URL: https://learn.microsoft.com/en-us/power-apps/maker/data-platform/create-edit-1n-relationships-portal (дата звернення: 25.12.2024).

25. Типи даних формул стовпців в Power Apps - Офіційна документація Microsoft, що описує типи даних, які можна використовувати у формулах стовпців в Power Apps. URL: https://learn.microsoft.com/en-us/power-apps/maker/data-platform/formula-column-data-types (дата звернення: 22.12.2024).

26. Фрундіна Л. І., Артюх О. В. Вдосконалення процесу інвентаризації шляхом застосування комп'ютерних технологій. URL:

https://www.ukrlogos.in.ua/10.11232-2663-4139.16.64.html (дата звернення: 15.12.2024).

27. Функції Filter та Lookup в Power Fx - Офіційна документація Microsoft, що описує функції Filter та Lookup в Power Fx. URL: https://learn.microsoft.com/en-us/power-platform/power-fx/reference/function-filter-lookup (дата звернення: 22.12.2024).

28. Функції у формулах стовпців Power Apps - Офіційна документація Microsoft, що описує функції, які можна використовувати у формулах стовпців в Power Apps. URL: https://learn.microsoft.com/en-us/power-apps/maker/data-platform/formula-columns (дата звернення: 22.12.2024).

29. Функція Concatenate в Power Fx - Офіційна документація Microsoft, що описує функцію Concatenate в Power Fx. URL: https://learn.microsoft.com/en-us/power-platform/power-fx/reference/function-concatenate (дата звернення: 25.12.2024).

30. Ціни та тарифні плани на Power Platform - Офіційна документація Microsoft, що описує ціни та тарифні плани на Power Platform. URL: https://www.microsoft.com/en-us/power-platform/products/power-apps/pricing (дата звернення: 25.12.2024).

31. Шевченко В.В., Тимчик Г.С. Основи автоматизації технологічних процесів. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». URL: https://ela.kpi.ua/bitstream/123456789/57481/1/Osnovi_avtomatizaciyi_%20tehnologichnih_%20procesiv_%20Konspekt%20lekcij.pdf (дата звернення: 15.12.2024).

32. Інструкція з делегування SharePoint для Power Apps - Блог Метью Девані, де він надає корисну інструкцію з делегування SharePoint для Power Apps. URL: https://www.matthewdevaney.com/sharepoint-delegation-cheat-sheet-for-power-apps/ (дата звернення: 22.12.2024).

33. Johnson Th. Protecting company information assets. URL: https://www.piranirisk.com/blog/protecting-company-information-assets. (дата звернення: 01.02.2025).

34. Moazam Niaz. Revolutionizing Inventory Planning: Harnessing Digital Supply Data through Digitization to Optimize Storage Efficiency Pre- and Post-Pandemic. *BULLET : Jurnal Multidisiplin Ilmu*. 2022. Vol. 1(03). URL: https://journal.mediapublikasi.id/index.php/bullet/article/view/3534 (дата звернення: 01.02.2025).

35. Hu C., Li Y., & Zheng X. Data assets, information uses, and operational efficiency. *Applied Economics*. 2022. Vol. 54(60), P. 6887–6900. DOI: https://doi.org/10.1080/00036846.2022.2084021 (дата звернення: 01.02.2025).

36. Abraham R., Schneider J., Brocke J. Data Governance: A Conceptual Framework, Structured Review, and Research Agenda. *International Journal of Information Management*. 2019. Vol. 49. P. 424–438. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.07.008 (дата звернення: 01.02.2025).

37. Fu S., Zhou Hj., Xiao Yz. Research on information system assets risk assessment and defense decision-making. *J. Ambient. Intell. Human. Comput*. 2023. Vol. 14. P. 1229–1241. DOI: https://doi.org/10.1007/s12652-021-03375-7 (дата звернення: 01.02.2025).

38. Arafat M. Information security management system challenges within a cloud computing environment. *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. ICFNDS ’18. New York, NY, USA: Association for Computing Machinery, 2018. DOI: https://doi.org/10.1145/3231053.3231127 (дата звернення: 01.02.2025).

39. Wong WP., Tan K.H., Govindan K. et al. A conceptual framework for information-leakage-resilience. *Ann. Oper. Res.* 2023. Vol. 329, P. 931–951. DOI: https://doi.org/10.1007/s10479-021-04219-5 (дата звернення: 01.02.2025).

40. Cheng L., Liu F., Yao D. Enterprise data breach: Causes, challenges, prevention and future directions. *Wires Data Mining and Knowledge Discovery.* 2017. Vol. 7. P. 1–14.