Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

"Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону"

Виконала: ст. 2-го курсу, групи 2КІТС-22м,
спеціальності 125 – Кібербезпека,
Освітня програма – Кібербезпека
інформаційних технологій та систем
(шифр і назва напряму підготовки, спеціальності)

Яремчук Я. Ю.
(прізвище та ініціали)

Керівник: к.т.н., доц., завідувач каф. МБІС

Карпінець В. В.
(прізвище та ініціали)

«04» грудня 2023 р.

Опонент: к.т.н., доц., доцент каф. ОТ

Колесник І. С.
(прізвище та ініціали)

«04» грудня 2023 р.

Допущено до захисту
Голова секції УБ кафедри МБІС

Юрій ЯРЕМЧУК
“04” грудня 2023 р.

Вінниця ВНТУ – 2023 рік

Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти – ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма – Кібербезпека інформаційних технологій та систем

ЗАТВЕРДЖУЮ
Голова секції УБ кафедри МБІС

_____ **Юрій ЯРЕМЧУК**
“20” вересня 2023 р.

З А В Д А Н Н Я
на магістерську кваліфікаційну роботу студентки
Яремчук Яна Юріївна
(прізвище, ім`я, по-батькові)

1. Тема роботи:

«Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону»

Керівник роботи: к.т.н., доц., зав. каф. МБІС Карпінець В.В.
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “18” вересня 2023 року № 247.

2. Строк подання студентом роботи за тиждень до захисту .

3. Вихідні дані до роботи:
Стандарти, електронні джерела, підручники та наукові статті по темі, які стосуються теми магістерської кваліфікаційної роботи.

4. Зміст текстової частини:
Для досягнення мети роботи було поставлено такі задачі: проаналізувати основні засади забезпечення безпеки об’єктів критичної інфраструктури та, зокрема, її складової – фінансової інфраструктури; дослідити методи системного аналізу безпеки об’єктів, а також сучасні методи автентифікації користувачів інформаційного ресурсу; розробити базу даних консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури, виконати декомпозицію та отримати кінцеві відношення за методом нормалізації відношень; забезпечити захист створеного консолідованого інформаційного ресурсу; здійснити програмну реалізацію захищеного консолідованого інформаційного ресурсу та програмних модулів забезпечення захисту інформаційного ресурсу; здійснити системний аналіз безпеки фінансової інфраструктури регіону на основі реалізованих програмних засобів.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень)
У першому розділі магістерської кваліфікаційної роботи наведено 3 рисунки, у другому розділі – 9 рисунків, у третьому розділі – 20 рисунків.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина			
I	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		
II	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		
III	Карпінець В.В. к.т.н., доц., зав. каф. МБІС		
Економічна частина			
IV	Причепа І.В., к.е.н., доц. каф. ЕПВМ		

7. Дата видачі завдання 20 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	31.09.2023	
2.	Аналіз предметної області обраної теми	01.10.2023	15.10.2023	
3.	Розробка роботи	16.10.2023	26.10.2023	
4.	Написання магістерської роботи на основі розробленої теми	27.10.2023	15.11.2023	
5.	Передзахист магістерської кваліфікаційної роботи	16.11.2023	24.11.2023	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	27.11.2023	04.12.2023	
7.	Захист магістерської кваліфікаційної роботи	11.12.2023	17.12.2023	

Студентка _____ Яремчук Я.Ю.
(підпис)

Керівник роботи _____ Карпінець В.В.
(підпис)

АНОТАЦІЯ

УДК 004.56.5(043.2)

Яремчук Я.Ю. Розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки фінансової інфраструктури регіону. Магістерська кваліфікаційна робота зі спеціальності 125 – «Кібербезпека», освітня програма «Кібербезпека інформаційних технологій та систем». Вінниця: ВНТУ, 2023. 157 с.

На укр.мові. Бібліогр.: 65 назв; рис.: 32; табл. 13.

Метою магістерської роботи є розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки фінансової інфраструктури регіону, який призначений для покращення її безпеки.

Пропонується методологія розробки захищеного консолідованого інформаційного ресурсу для системного аналізу безпеки фінансової інфраструктури регіону.

Проводиться аналіз поточного стану фінансової інфраструктури регіону та виявляються основні проблеми та вразливі місця в цій роботі для аналізу чи обмеження фінансової інфраструктури. Розроблено концептуальні та функціональні вимоги до захищеного консолідованого інформаційного ресурсу.

Описано архітектуру та основні компоненти інформаційного ресурсу, включаючи систему збору, обробки та аналізу даних, а також систему забезпечення безпеки.

Розглядається питання забезпечення захищеності та конфіденційності інформації в ресурсі, включаючи використання шифрування, доступу на основі ролей та ідентифікації користувачів.

Також, обраховано необхідні економічні показники та доведена економічна доцільність розробки цього ресурсу.

ANNOTATION

Yaremchuk Y.Y. Development of a Secure Consolidated Information Resource for System Analysis of Financial Infrastructure Security in the Region. Master's Thesis in Cybersecurity, Educational Program "Cybersecurity of Information Technologies and Systems." Vinnytsia: VNTU, 2023. 157 p.

In Ukrainian language. Bibliographer: 65 titles; figures: 32; tables: 13.

The purpose of the master's work is to develop a protected consolidated information resource of a system analysis of the security of the financial infrastructure of the region, which is intended to improve its security.

A methodology for the development of a protected consolidated information resource for the systematic analysis of the security of the financial infrastructure of the region is proposed.

An analysis of the current state of the financial infrastructure of the region is carried out, and the main problems and vulnerabilities in this work for the analysis or limitation of the financial infrastructure are revealed. Developed conceptual and functional requirements for a protected consolidated information resource.

The architecture and main components of the information resource are described, including the data collection, processing and analysis system, as well as the security system.

The issue of ensuring security and confidentiality of information in the resource is considered, including the use of encryption, role-based access and user identification.

Also, the necessary economic indicators were calculated and the economic feasibility of developing this resource was proven.

ЗМІСТ

ВСТУП

Актуальність теми.

Фінансова інфраструктура – це сукупність установ, які функціонують на ринку фінансових послуг, таких як банки, страхові компанії, пенсійні фонди, платіжні системи та інші. Важливо забезпечувати безпеку критичних об’єктів цих установ, оскільки будь-яке порушення може мати серйозні наслідки для економіки і фінансової системи регіону та країни в цілому. Зростання кіберзлочинності та швидкий розвиток технологій також роблять цю тему актуальною. Необхідно завжди бути в курсі останніх тенденцій у сфері безпеки та застосовувати відповідні технології та методи для запобігання загрозам.

Створення консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури є дуже актуальною темою, оскільки вона спрямована на забезпечення безпеки фінансової системи та запобігання потенційним загрозам, допоможе проводити моніторинг безпеки фінансової інфраструктури, аналізувати загрози та виявляти можливі проблеми.

Така система допоможе забезпечити цілісний погляд на безпеку фінансової інфраструктури, а також забезпечить зручний доступ до інформації для аналітиків. Це дозволить вчасно приймати рішення щодо запобігання потенційним загрозам.

Мета дослідження.

Дослідження методів оцінювання стану безпеки об’єктів фінансової критичної інфраструктури і розробка консолідованого інформаційного ресурсу аналізу безпеки цих об’єктів.

Задачі дослідження:

1. Аналіз сучасних підходів та методів до аналізу безпеки об`єктів фінансової інфраструктури.

2. Вивчення основних проблем та загроз для безпеки критичних об`єктів фінансової інфраструктури.

3. Розробка архітектури та функціоналу консолідованого інформаційного ресурсу.

4. Створення бази даних та інтеграція з різними інформаційними джерелами.

5. Розробка алгоритмів обробки та аналізу інформації про безпеку об’єктів фінансової інфраструктури.

6. Розробка інструментів візуалізації та звітності для аналізу даних.

7. Проведення тестування роботи.

8. Оцінювання ефективності та користі від використання консолідованого інформаційного ресурсу.

Об’єкт дослідження.

Об’єктом дослідження є оцінювання стану безпеки критичних об’єктів фінансової інфраструктури.

Предмет дослідження.

Сукупність теоретичних засад і практичних заходів створення консолідованого інформаційного ресурсу.

Наукова новизна.

Вперше розроблено захищений консолідований інформаційний ресурс аналізу безпеки фінансової інфраструктури регіону, що дозволило вирішити проблему комплексного аналізу безпеки критичних об’єктів фінансової інфраструктури і урахуванням економічних показників.

Практична цінність. Розроблений консолідований інформаційний ресурс аналізу безпеки фінансової інфраструктури, який дозволяє отримати аналітичні висновки щодо безпеки відповідних підприємств й їх об’єктів критичної інфраструктури.

За тематикою роботи опубліковано 12 публікацій, зокрема 5 статей у фахових виданнях та 7 тез доповідей на наукових конференціях [54–65].

РОЗДІЛ І. ТЕОРЕТИЧНІ ЗАСАДИ СТВОРЕННЯ КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ АНАЛІЗУ БЕЗПЕКИ ФІНАНСОВОЇ ІНФРАСТРУКТУРИ

1.1 Актуальність, особливості та основні засади забезпечення безпеки об’єктів критичної інфраструктури

Актуальність забезпечення безпеки критичної інфраструктури є надзвичайно важливою в сучасному світі тому, що вона є життєво важливою для функціонування суспільства.

Критична інфраструктура – це сукупність об’єктів державної інфраструктури, найбільш важливих для економіки і промисловості, функціонування суспільства і безпеки населення, а також виведення з ладу або руйнування яких може вплинути на національну безпеку і обороноздатність, природне середовище, призвести до значних фінансових і людських втрат [1].

Об’єкти критичної інфраструктури – це об’єкти, системи чи послуги, без яких може настати значна негативна дія на національну безпеку, економіку, здоров’я чи забезпечення життєво важливих потреб населення. Ці об’єкти є важливими для нормального функціонування суспільства та їх ураження може призвести до серйозних наслідків.

Об’єктом критичної інформаційної інфраструктури є комунікаційна або технічна система об’єкта критичної інфраструктури, її кібератаки безпосередньо впливають на стале функціонування такого об’єкта критичної інфраструктури [2].

Віднесення об’єктів до критично важливих інфраструктури здійснюється відповідно до набору критеріїв, що визначають соціальну, політичну, економічну та екологічну важливість забезпечення оборони країни, безпеки громадян, суспільства, держави, верховенства закону, зокрема, для здійснення життєво важливих функцій та охорони навколишнього середовища, надання життєво важливих послуг, наявність загроз для них, їх функціонування, припинення функцій внаслідок несанкціонованого втручання людського фактора або

стихійних лих, ймовірність виникнення кризової ситуації, у період проведення робіт з усунення таких наслідків, до повного відновлення нормальної роботи.

До таких критеріїв належать:

1) виконання функцій по забезпеченню життєво важливих національних інтересів;

2) наявність викликів і загроз, які можуть виникнути у зв’язку з об’єктами критично важливої інфраструктури;

3) можливість нанесення значної шкоди нормальним умовам життєдіяльності населення;

4) Уразливість таких об’єктів визначається можливістю виникнення серйозних негативних наслідків, що призведуть до серйозної шкоди для здоров’я населення. Ця шкода вимірюється кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення. Негативні наслідки також поширюються на соціальну сферу, включаючи руйнування систем соціального захисту та втрату здатності держави виправдовувати критичні потреби суспільства. На державний суверенітет впливає зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та обмеження можливостей виконання державою своїх функцій. Економічні наслідки охоплюють внутрішній валовий продукт та розмір економічних втрат, як прямих, так і непрямих. Крім того, така уразливість має вплив на природні ресурси загальнодержавного та місцевого значення, створюючи загрозу їхньому стійкому використанню та збереженню;

5) масштаби негативного впливу на державу, що зачіпає діяльність стратегічно важливих об’єктів для деяких секторів життєзабезпечення або призводить до втрати унікальних національно значущих активів, систем і ресурсів, матимуть довгострокові наслідки для держави і вплинуть на діяльність багатьох інших секторів;

6) період усунення таких наслідків та вплив подальших негативних наслідків на інші сектори держави;

7) вплив на функціонування суміжних секторів критично важливої інфраструктури.

Класифікація об’єктів інфраструктури – визначення об’єктів інфраструктури за категоріями критичності.

Категорія критичності об’єкта інфраструктури (критерій) – це важливість об’єкта критичної інфраструктури (відносний рівень), яка є відносним рівнем як самого об’єкта КІ, так і його відносним рівнем критичної функції.

Для визначення рівня вимог до забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня важливості для забезпечення окремих критичних функцій у секторі критичної інфраструктури її об’єкти класифікуються відповідно до категорії важливості.

Були встановлені такі категорії важливості об’єктів критичної інфраструктури [3]:

1) І категорія – істотності – особливо важливі об’єкти загальнодержавного значення, що надають значний вплив на інші об’єкти критичної інфраструктури, і порушення їх функціонування може призвести до кризової ситуації загальнодержавного значення;

2) ІІ категорія – життєво важливі об’єкти, руйнування яких призводить до кризової ситуації регіонального значення;

3) ІІІ категорія – важливий об'єкт, руйнування якого призводить до кризової ситуації регіонального значення;

4) IV категорія - об’єкт, порушення функціонування якого призведе до виникнення кризової ситуації локального значення.

Забезпечення безпеки об’єктів критичної інфраструктури має на меті запобігання можливому пошкодженню, знищенню або порушенню роботи цих об’єктів. Такі ситуації можуть виникнути внаслідок терористичних актів, кібератак, природних катастроф, техногенних аварій або інших небажаних подій.

Одним з основних викликів у забезпеченні безпеки об’єктів критичної інфраструктури є загрози, які постійно змінюються. Терористичні групи та хакери постійно шукають нові способи атаки, що ставлять під загрозу роботу цих

об’єктів. Тому важливо постійно вдосконалювати системи безпеки, враховуючи нові технології та методи захисту.

Крім того, забезпечення безпеки об’єктів критичної інфраструктури має стати пріоритетним завданням для урядів та організацій. Вони повинні виділити достатні ресурси для розвитку та підтримки систем безпеки, проводити регулярні перевірки та оцінювання ризиків, інвестувати у навчання та підготовку персоналу.

Отже, актуальність забезпечення безпеки об’єктів критичної інфраструктури не може бути переоцінена. Вона відіграє важливу роль у забезпеченні безпеки та стійкості суспільства, економіки та національної безпеки країни.

Важливість забезпечення безпеки об’єктів критичної інфраструктури відображається у кількох ключових аспектах:

1. Соціальна стійкість: об’єкти критичної інфраструктури відповідають за надання послуг, які є необхідними для життєдіяльності суспільства. Безпека об’єктів критичної інфраструктури допомагає забезпечити стабільність та функціонування суспільства і включає у себе забезпечення безперебійного доступу до основних послуг, збереження комунікаційних мереж та засобів зв’язку в екстремальних ситуаціях, збереження систем громадського транспорту і подібне. Розрив у роботі таких об’єктів може мати серйозні наслідки для безпеки людей, здоров’я, безперебійного постачання енергії, транспорту, води тощо.

2. Економічний аспект: Критична інфраструктура впливає на економіку країни. Пошкодження або переривання роботи об’єктів критичної інфраструктури може призвести до значних втрат для бізнесу, зупинки виробництва, зменшення валового внутрішнього продукту.

3. Безпека національної оборони: Забезпечення безпеки об’єктів критично важливої інфраструктури має важливе значення для захисту держави від можливих атак зовні. Це стосується не тільки фізичного захисту об’єктів, але й кібербезпеки, яка стає все більш актуальною в сучасному цифровому світі.

Отже, безпека об’єктів критичної інфраструктури має дуже високу актуальність, оскільки вона впливає на безпеку і добробут суспільства в цілому. Враховуючи зростаючі загрози у сучасному світі, забезпечення безпеки об’єктів

критично важливої інфраструктури стає необхідним завданням для держави, організацій та громадян.

Забезпечення безпеки об’єктів критичної інфраструктури (наприклад, електростанцій, водопостачальних систем, транспортних мереж, інформаційних систем) має свої особливості. Оскільки такі об’єкти є важливими для функціонування суспільства та економіки, їх вразливість може призвести до серйозного збитку і загрози безпеці нації.

Забезпечення безпеки базується на таких основних засадах [3]:

1. Фізична безпека – комплекс режимних, інженерних, технічних та інших заходів, спрямованих на запобігання та/або запобігання або припинення актів незаконного або несанкціонованого втручання, організованих і здійснюваних суб’єктом державної системи захисту критично важливої інфраструктури.
2. Кібербезпека:

– інформаційна безпека – це безпека інформації організації, яка знаходиться у тому числі й в IT системах, включаючи програми та обладнання.

– кібербезпека – це безпека IT систем в інформаційному просторі;

Фізична безпека об’єкта включає різні заходи для захисту фізичних об’єктів, такі як:

– огорожі й інші обмежувальні споруди: використовуються для забезпечення контрольно-пропускного режиму на об’єктах критичної інфраструктури й управляння потоками переміщення персоналу і відвідувачів;

– системи відеоспостереження: використовуються як для догляду за периметром, так і за іншими важливими місцями всередині периметра;

– система контролю фізичного доступу: дозволяє обмежити доступ лише для авторизованих осіб, може включати використання електронних ключів, кодів доступу, бар’єрів або інших методів контролю;

– сигналізація та інші системи сповіщення: використовуються для запобігання несанкціонованого доступу до об’єктів, може включати системи виявлення руху, відчинення дверей, зміни температури тощо;

– системи виявлення пожеж і протипожежного захисту: сукупність технічних засобів та організаційних заходів, які спрямовані на забезпечення запобіганню впливу пожежі і обмежує заподіяну нею матеріальну шкоду (ДСТУ 2272-93);

– резервне енергозабезпечення: об’єкти критичної інфраструктури мають мати системи резервного енергозабезпечення, які дозволяють продовжувати роботу в разі відключення основного джерела енергії. Це може включати використання дизельних генераторів, акумуляторних батарей та інших альтернативних джерел енергії.

– системи моніторингу та автоматизації: для забезпечення безпеки об’єктів критичної інфраструктури необхідно мати системи моніторингу, які постійно слідкують за станом об’єктів. Може бути інтегрованою з іншими системами для використання інформації із сенсорів, датчиків, камер спостереження та інших приладів для виявлення незвичайних подій чи аномалій. Дані з цих систем можуть бути автоматично оброблені та переведені у режим аварійного реагування, що дозволяє оперативно реагувати на потенційні загрози та приймати відповідні заходи;

– захист персоналу: об’єкти критичної інфраструктури повинні мати відповідні заходи для захисту персоналу від можливих загроз. Це може включати навчання персоналу з питань безпеки, а, також, проведення перевірки персоналу.

Кібербезпека – це комплекс технологічних рішень, які призначені для захисту важливих систем і даних від несанкціонованого доступу або їх знищення.

Загальний підхід до забезпечення кібербезпеки [4]:

– аналізувати і визначати поточний стан кібербезпеки щодо критично важливої інформаційної інфраструктури;

– визначити цільовий стан кібербезпеки критично важливих об’єктів інформаційної інфраструктури;

– ідентифікувати та визначити пріоритети, рівень впровадження заходів кібербезпеки в контексті безперервних і повторюваних процесів управління

ризиками в області кібербезпеки критично важливих об’єктів інформаційної інфраструктури;

– оцінити прогрес у досягненні цільового стану кібербезпеки для критично важливих об’єктів інформаційної інфраструктури;

– забезпечити зв’язок між суб’єктами, які розташовані безпосередньо на об’єктах критично важливої інфраструктури, і організації, які є партнерами організації в області управління ризиками в області кібербезпеки.

Для захисту інформаційних систем об’єктів критичної інфраструктури використовуються технології та процедури кібербезпеки, які включають виявлення та запобігання кібератак, захист від вразливостей і відновлення системи або даних після атаки, зокрема:

– ідентифікація і автентифікація користувачів систем: необхідна для забезпечення безпеки доступу до IT-систем об’єктів критичної інфраструктури. Це дозволяє розмежувати доступ до систем або даних і може включати використання багатофакторної автентифікації, біометричних методів, смарт-карт або інших форм ідентифікації; користувачі повинні бути чітко ідентифіковані та мати відповідні права доступу до різних функціональних областей системи; механізми автентифікації (наприклад, паролі, біометричні дані) та авторизації (наприклад, ролі та дозволи) можуть бути використані для забезпечення безпеки доступу;

– інспекція і регулярне оновлення: необхідно своєчасно проводити оновлення операційних систем, програмного забезпечення та мережевих пристроїв; також необхідно відслідковувати появу і встановлювати проміжкові безпекові патчі, що зменшить вірогідність успішної атаки у разі виявлення вразливостей у операційній системі або програмному забезпеченні;

– виявлення і захист від кібератак: об’єкти критичної інфраструктури мають мати захист від кібератак та інших кіберзагроз. Це може включати використання спеціалізованого програмного забезпечення для виявлення і

запобігання кіберзламам, таких як IDS/IPS (Intrusion Detection and Prevention System) – апаратні або програмні системи виявлення та запобігання вторгненням, забезпечують безпеку як мереж, так і окремих пристроїв. IDS аналізує мережеві пакети даних, не модифікуючи їх, і перевіряє співпадіння у базі даних правил або сигнатур атак, виявляючи шкідливий трафік. IPS відслідковує активність у реальному часі і запобігає атакам, розпізнаним за допомогою IDS, здатна модифікувати трафік і запобігти доставці мережевих пакетів, подібно до того, як це робить брандмауер;

– захист інформації: забезпечується безпека конфіденційної інформації, такої як плани захисту, архітектура системи, технічний паспорт і інші важливі дані. Для забезпечення безпеки чутливої інформації об’єктів критичної інфраструктури необхідно захищати інформацію від несанкціонованого доступу, втрати або пошкодження. Це може включати використання шифрування даних, резервного копіювання ізольованих мереж тощо;

– системи моніторингу: надають можливість спостереження та проведення аналізу функціонування інфраструктури у режимі реального часу згідно з даними, отриманими раніше і дозволяють виявити незвичайні або підозрілі дії і активності. Об’єкти критичної інфраструктури повинні мати встановлені системи моніторингу, щоб бути впевненими, що певна система працює як потрібно;

– резервне копіювання – створення копії важливих даних з носіїв, надає можливість відновлення цих даних у разі їх пошкодження або видалення. Резервне копіювання даних можна вважати достатньо надійним, якщо виконується правило 3-2-1: необхідно мати три резервної копії, які повинні зберігатися на двох різних носіях, а один повинен знаходитись у територіально віддаленому окремому місці;

– навчання персоналу з питань кібербезпеки.

Заходи з кібербезпеки, спрямовані на зниження ризиків кібербезпеки, носять постійний характер і являють собою цикл управління кібербезпекою, що складається з 5 функцій кібербезпеки [4] (рисунок 1.1):

– ідентифікація ризиків;

– кіберзахист;

– виявлення кіберінцидентів;

– реагування;

– відновлення поточного стану кібербезпеки.

Рівні впровадження заходів з кіберзахисту [4]:

1. Рівень впровадження заходів кіберзахисту характеризує здатність організації надавати інструменти для оцінки ступеня практичного застосування заходів кіберзахисту організацією, досягнення запланованих результатів кіберзахисту та оцінки ступеня реалізації процесів управління кібербезпекою.

Визначаються наступні чотири рівні:

1. частковий;

2. ризик-орієнтований;

3. повторюваний;

4. адаптивний.

При виборі рівня правозастосування організації рекомендується враховувати існуючі методи управління ризиками, середовище загроз, законодавчі та нормативні вимоги, бізнес-цілі / місії та організаційні обмеження.

2. Рекомендації визначають чотири ієрархічних рівні впровадження заходів кіберзахисту (рисунок 1.2.):

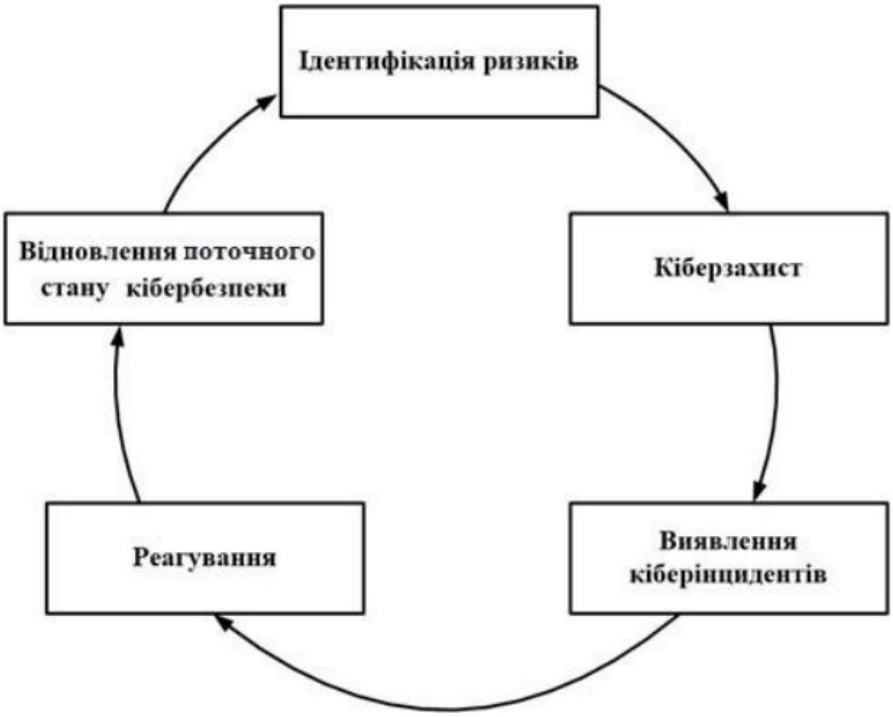


Рисунок 1.1. Цикл управління кібербезпекою

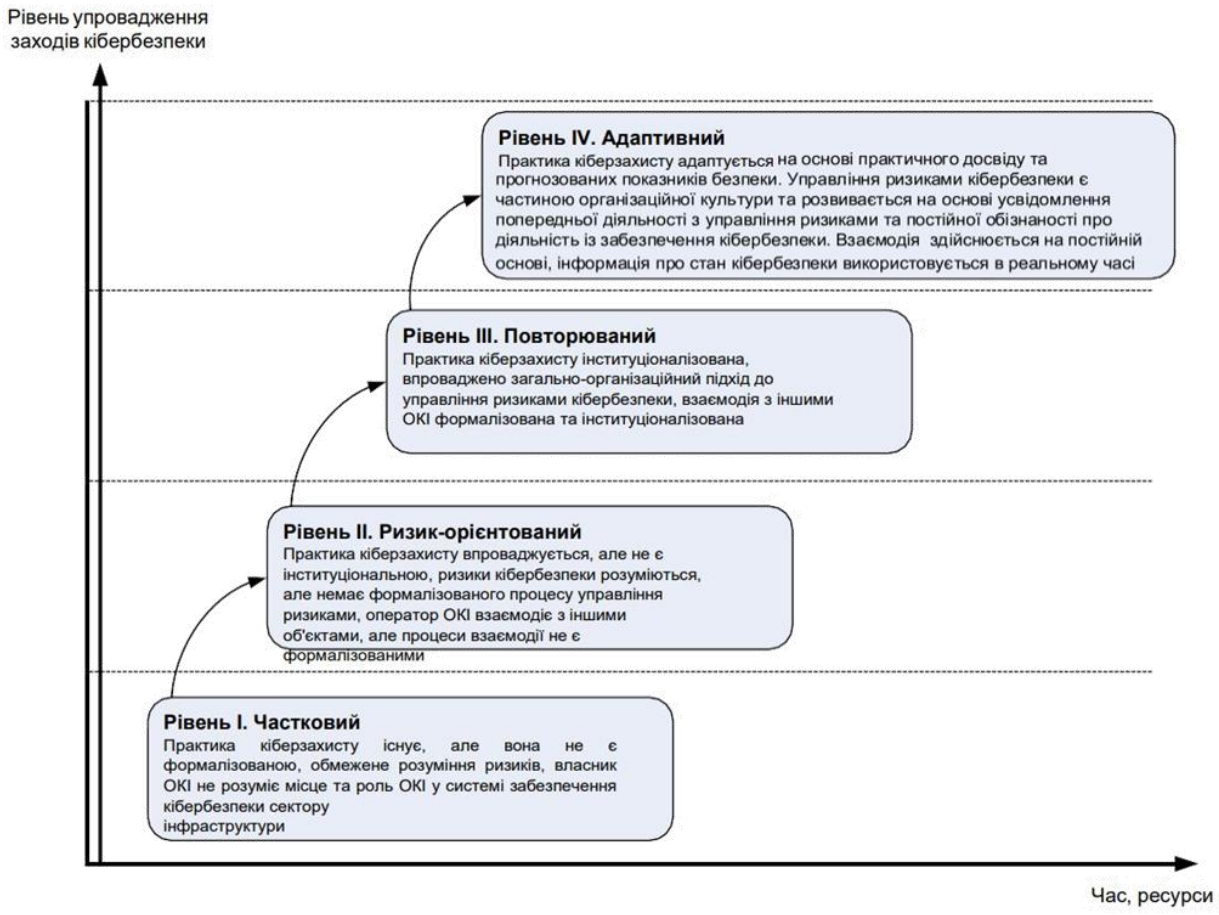


Рисунок 1.2. Рівні впровадження заходів кіберзахисту

Процес вибору рівня впровадження (таблиця 1.1) описує поточну практику впровадження заходів кібербезпеки та управління ризиками кібербезпеки в ОКІІ, характеристики загроз кібербезпеці, законодавчі та нормативні вимоги, комерційні та стратегічні цілі ОКІ, а також ризики кібербезпеки та організаційні обмеження в ланцюжку поставок програмного або апаратного забезпечення. Він враховує вимоги безпеки та інші існуючі обмеження [4].

Таблиця 1.1. Рівні впровадження заходів з кіберзахисту

Рівень	Практика кіберзахисту	Політика управління ризиками	Взаємодія з іншими ОКІ
1	2	3	4
Частковий	Практичні дії щодо впровадження заходів кіберзахисту та управління ризиками кібербезпеки не були формалізовані. Впровадження заходів кібербезпеки та управління ризиками носить довільний і контекстуальний характер. Пріоритет реалізації заходів кіберзахисту безпосередньо не враховує цілі Oka з управління ризиками, характеристики загрози та обов'язки з надання життєво важливих послуг і функцій.	Обмежене розуміння ризиків кібербезпеки на організаційному рівні. Керівництво та персонал організації погано обізнані про ризики кібербезпеки. Загальний підхід до управління ризиками кібербезпеки не встановлений у глобальному масштабі. Заходи кіберзахисту застосовуються нерегулярно і відповідно до ситуації з використанням різного практичного досвіду і знань, отриманих ззовні. Не існує процесу, що забезпечує внутрішній обмін інформацією про стан кібербезпеки.	Організація не розуміє своєї ролі в екосистемі щодо власних залежностей чи інших пов'язаних з нею суб'єктів. Організація може бути відокремлена від інших організацій (споживачів, постачальників, афілійованих або афілійованих організацій, організацій з аналізу та розповсюдження інформації, дослідників та державних установ) (включаючи дослідження загроз, найкращі практики тощо).) Може збирати інформацію.). Організації часто не усвідомлюють ризиків кібербезпеки, пов'язаних із послугами, які вони надають та використовують.

Продовження таблиці 1.1.

1	2	3	4
Ризик-орієнтований	Практика застосування заходів кібербезпеки та управління ризиками затверджується керівництвом організації, але не може бути визначена як загальна політика організації. Пріоритет дій в області кібербезпеки і потреб в захисті безпосередньо залежить від цілей організації щодо ризиків, середовища загроз або вимог до надання критично важливих послуг і функцій.	Незважаючи на те, що на організаційному рівні існує обізнаність про ризики кібербезпеки, загальноорганізаційний підхід до управління ризиками кібербезпеки не розроблений. Інформація, пов'язана з кібербезпекою, поширюється неофіційно всередині організації. Проблеми кібербезпеки в організаційних цілях і програмах можуть виникати на деяких рівнях організації, але не на всіх. Оцінки ризиків кібербезпеки для організацій і зовнішніх організацій проводяться, але зазвичай не повторюються і не виконуються таким же чином.	Як правило, організація розуміє свою роль в екосистемі щодо власних залежностей або інших залежних від неї суб'єктів, але не розуміє обох. Організація обробляє і декомунізує деяку інформацію від інших організацій і на її основі створює свою власну інформацію, але неможливо поширювати таку інформацію серед інших організацій. Крім того, організації усвідомлюють ризики кібербезпеки, пов'язані з наданими та використовуваними ними послугами, але не діють відповідно до узгоджених або затверджених правил.
Повторюваний	Практика застосування заходів кібербезпеки та управління ризиками в організації була офіційно схвалена і визначена як політика. Результати кіберзахисту регулярно контролюються, а заходи кіберзахисту регулярно оновлюються на основі змін критичних функціональних вимог, змін загроз і застосування процесів управління ризиками до технологічного середовища.	Організації дотримуються загального підходу до управління ризиками кібербезпеки. Політики, процеси та процедури, що враховують ризики, визначаються, застосовуються та переглядаються за призначенням. Існують послідовні способи ефективного реагування на зміни ризику. Персонал володіє знаннями і навичками для виконання поставлених завдань. Організації послідовно і точно контролюють ризики кібербезпеки для своїх активів. Керівники вищої ланки з кібербезпеки та не пов'язані з кібербезпекою регулярно спілкуються про ризики кібербезпеки.	Організації можуть розуміти свою роль в екосистемах щодо власної залежності або інших організацій, які залежать від них, і можуть сприяти більш широкому розумінню ризику громадами. Організації регулярно обробляють і декомунізують інформацію від інших організацій, доповнюють інформацію, яку вони створили самі, і поширюють її серед інших організацій. Організації усвідомлюють ризики кібербезпеки, пов'язані з наданими ними послугами та послугами, якими вони користуються.

Продовження таблиці 1.1.

1	2	3	4
Адаптивний	Організації адаптують свої методи кібербезпеки до попередніх і поточних заходів кібербезпеки, включаючи отримані результати і прогнозні показники. Завдяки постійному процесу вдосконалення, що включає передові технології і методи кібербезпеки, організації активно адаптуються до мінливих кіберзагроз, розвиваються і своєчасно і ефективно реагують на все більш складні кіберзагрози..	Організації повинні розробити систему управління ризиками кібербезпеки, яка використовує політику, процеси та процедури, засновані на ризиках, для обробки потенційних кібер-інцидентів. Взаємозв'язок між ризиками кібербезпеки і цілями організації чітко розуміється і враховується при прийнятті рішень. Менеджери контролюють ризики кібербезпеки в тому ж контексті, що і фінансові та інші ризики для організації. Управління ризиками кібербезпеки є частиною організаційної культури і розробляється на основі обізнаності про попередні дії та певної обізнаності про дії в системах та мережах зв'язку. Організації можуть швидко та ефективно пояснювати зміни в підходах до роботи та повідомляти про ризики.	Організації розуміють свою роль в екосистемах щодо власної залежності або інших залежних від них організацій, що сприяє більш широкому розумінню ризиків. Організації отримують, генерують та аналізують пріоритетну інформацію, щоб продовжувати аналізувати ці ризики в міру розвитку загроз та технологічного ландшафту. Організація поширює як внутрішню, так і зовнішню інформацію для отримання більш детальної інформації. Організації використовують інформацію в режимі реального часу або майже в режимі реального часу, щоб послідовно реагувати на ризики кібербезпеки, пов'язані з наданими ними послугами та послугами, якими вони користуються.

Отже, основні завдання забезпечення безпеки таких об’єктів критичної інфраструктури включають:

1. Виявлення і відповідь на загрози: для забезпечення безпеки об'єктів критичної інфраструктури необхідно мати систему виявлення і відповіді на загрози. Здійснюється оцінювання потенційних загроз, які можуть призвести до порушення роботи об’єктів критичної інфраструктури. Це можуть бути терористичні акти, кібератаки, природні катастрофи або техногенні аварії.

2. Концепція захисту: розробляється імовірний сценарій загрози та план захисту для запобігання, виявлення, управління та відновлення від наслідків такої

загрози. Цей план має бути гнучким і включати загальні принципи, які можуть бути застосовані до різних видів загроз. Зокрема, необхідно розробити резервні плани, які призначені для відновлення об’єктів критичної інфраструктури, які передбачають заходи для відновлення роботи після кризових ситуацій. Це можуть бути запасні системи живлення, резервування даних, плани евакуації та інші заходи.

3. Управління кризовими ситуаціями: для забезпечення безпеки об'єктів критичної інфраструктури необхідно мати плани кризового управління для вирішення непередбачених ситуацій. Це може включати використання систем інформування та комунікації, тренування персоналу для дії у надзвичайних ситуаціях, передбачені плани та процедури для управління кризовими ситуаціями, зокрема, реакція на надзвичайні ситуації, координація з іншими командами та органами влади, комунікація з громадськістю та інші аспекти.

4. Співпраця з владними органами та обмін інформацією: забезпечення безпеки об’єктів критичної інфраструктури вимагає співпраці та обміну інформацією з правоохоронними органами та іншими компетентними організаціями та владними структурами. Це може включати спільні вправи та тренування з підрозділами екстреної допомоги, обмін даними про потенційні загрози та вразливості, а також обговорення та впровадження спільних стратегій та стандартів безпеки. Протоколи співпраці й обмін інформацією повинні бути встановлені для швидкого реагування на випадки загроз та для спільного управління у разі кризових ситуацій.

Забезпечення безпеки об’єктів критичної інфраструктури є складним і багатоаспектним процесом. Врахування усіх особливостей і потенційних загроз дозволяє підвищити рівень безпеки та забезпечити стійке функціонування цих об’єктів.

Ці засади забезпечення безпеки об’єктів критичної інфраструктури допомагають забезпечити оптимальний рівень захисту та функціонування таких об’єктів і зменшити ризик виникнення небезпеки або деградації їх роботи у разі загрози або кризової ситуації

1.2 Загальна характеристика предметної області «фінансова інфраструктура» як складова критичної інфраструктури регіону

Фінансова інфраструктура є однією з ключових складових критичної інфраструктури регіону і включає у себе усі фінансові установи, системи й послуги, які забезпечують функціонування економічних процесів у регіоні. Вона включає у себе такі елементи як банки, страхові компанії, фондові біржі, платіжні системи, розрахункові й клірингові центри, кредитні установи, фінансові регулятори та інші фінансові установи.

Основні функції фінансової інфраструктури включають забезпечення доступу до фінансових послуг для господарського сектора й населення, зберігання й переказ грошей, здійснення фінансових операцій, кредитування, збереження та інвестицій.

Фінансова інфраструктура також виконує важливу роль у стабільності й безпечності фінансової системи регіону. Вона забезпечує контроль за фінансовими ризиками та управління фінансовими потоками, сприяє розкриттю фінансової звітності, моніторингу та регулюванню фінансових установ, а також протидії шахрайству й відмиванню грошей.

Для забезпечення безперебійного функціонування фінансової інфраструктури необхідно мати ефективну технічну й кадрову базу, високий рівень кібербезпеки, а також ефективний механізм комунікації й координації між фінансовими установами, правоохоронними органами та регуляторами.

Отже, фінансова інфраструктура є важливою складовою критичної інфраструктури регіону, яка забезпечує стабільність та ефективність фінансової системи, впливає на розвиток економіки та підтримує фінансову безпеку регіону.

Надійність фінансової інфраструктури є критичною для забезпечення фінансової стабільності. Будь-який збій або неправильне функціонування фінансової інфраструктури може мати серйозні наслідки для економічного розвитку регіону, може спричинити фінансову нестабільність, втрати для

інвесторів та населення, а також порушення довіри до фінансової системи в цілому.

Одним з важливих аспектів фінансової інфраструктури є її роль в економічному розвитку регіону. Готовність фінансової системи надавати кредити та фінансові послуги підприємствам та населенню є необхідною умовою для розширення бізнесу, інновацій та зростання економіки. Наявність поліпшеної фінансової інфраструктури може сприяти підтримці підприємств, розвитку сектора малого та середнього бізнесу, залученню інвестицій та розвитку фінансового ринку. У свою чергу, це приводить до зростання валового внутрішнього продукту регіону та підвищення рівня життя населення.

Крім того, безпека фінансової інфраструктури також впливає на фінансову безпеку регіону. Забезпечення безпеки фінансових транзакцій та захист інформації є надзвичайно важливим. Відсутність адекватних заходів кібербезпеки та контролю може призвести до зупинки роботи фінансової установи, крадіжок, шахрайства або відмивання грошей. Тому належний рівень захисту фінансової інфраструктури від злочинної діяльності є ключовим для забезпечення фінансової стабільності та довіри.

Враховуючи все вищезазначене, можна зробити висновок, що фінансова інфраструктура є важливою складовою критичної інфраструктури регіону, яка впливає як на економічний розвиток, так і на фінансову стабільність та безпеку регіону. Це розкриває потребу у розвитку та модернізації фінансової інфраструктури для забезпечення ефективності, надійності та стійкості фінансової системи регіону.

Підтримка і розвиток фінансової інфраструктури також є необхідною для привабливості регіону для іноземних інвесторів. Компанії шукають регіони, де є розвинута та надійна фінансова система, що забезпечує швидке та ефективне розрахункове обслуговування. Готовність фінансової інфраструктури працювати з іноземними валютами, обмін валют та інші міжнародні фінансові операції також є важливим фактором для розвитку зовнішньої торгівлі та економічного зростання.

Також, фінансова інфраструктура регіону має велике значення для забезпечення фінансової включеності населення. Широкий доступ до фінансових послуг дозволяє населенню зберігати гроші, здійснювати безготівкові платежі, отримувати кредити та страхування. Це важливо для зменшення фінансової вразливості, підвищення рівня життя та сприяння соціально-економічному розвитку регіону.

Загалом, фінансова інфраструктура регіону є ключовим елементом для ефективного функціонування економіки та підтримки фінансової стабільності і безпеки. Розвиток та підтримка фінансової інфраструктури є важливим завданням для влади та регуляторних органів, а також для фінансових установ, які мають спільно працювати для забезпечення ефективності, стійкості та розвитку фінансової системи регіону.

Кібербезпека для фінансових послуг є складною, основна причина, це велика різноманітність та частота кіберзагроз, яким піддається сектор. Кіберзлочинці можуть отримати великий прибуток, викрадаючи активи фінансової установи, і це завжди залишатиметься постійною поставкою зловмисників, бажаючих спробувати [9–14].

Компанії, що надають фінансові послуги, приваблюють кіберзлочинців, які постійно винаходять нові способи успішного зламу або витоку даних. Незалежно від того наскільки добре служби безпеки можуть запровадити заходи пом’якшення небезпеки, кіберзлочинці так само швидко розробляють способи їх обійти.

Оскільки найважливішою складовою фінансової системи України є банківська система, Національний банк України не тільки розробив вимоги до функціонування системи кіберзахисту в банківській системі України, а й розробив оновлені стандарти і процедури класифікації банків як об’єктів життєво важливої інформаційної інфраструктури.

Нацбанк нормалізував і прийняв рішення з питання організації та забезпечення кіберзахисту в банківській системі України, зокрема такі:

– основні принципи функціонування системи кіберзахисту;

– вимоги до заходів, що забезпечують кіберзахист критично важливих об'єктів інформаційної інфраструктури;

– вимоги для проведення незалежного аудиту інформаційної безпеки банку.

Були впроваджені і відповідні стандарти, зокрема постанову Ради Національного банку України №178 від 8.2022 р. № 12 "Про затвердження Правил організації кіберзахисту в банківській системі України та внесення змін до Правил ідентифікації об'єктів критично важливої інфраструктури в банківській системі України" [7].

Даний документ враховує вимоги законодавства України "Про основні засади забезпечення кібербезпеки України" та з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021 з урахуванням таких законів і національних стандартів [8]:

1. “Про Національний банк України”

2. “Про основні засади забезпечення кібербезпеки України”, з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021

3. Національний стандарт України ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги” (ISO/IEC 27001:2013, Cor 1:2014, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18 грудня 2015 року № 193

4. Національний стандарт України ДСТУ ISO/IEC 27032:2016 “Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки” (ISO/IEC 27032:2012, IDT), прийнятого наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 27 грудня 2016 року № 448

5. Національний стандарт України ДСТУ ISO/IEC 27010:2018 “Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій” (ISO/IEC 27010:2015, IDT), прийнятого наказом

Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 10 грудня 2018 року № 470.

Банк включає в себе інформаційну систему, яка надає інформацію про стан об’єктів критичної інфраструктури та автоматизує процес надання прямих фінансових послуг "у банківській справі і банківській діяльності" як об’єкта критичної інформаційної інфраструктури та інших видів діяльності банків відповідно до статті 47 Закону України.

Банки зобов’язані забезпечувати дотримання цих стандартів кібербезпеки і покладати функції кіберзахисту на підрозділи інформаційної безпеки або створювати незалежні підрозділи кіберзахисту. Він повинен підпорядковуватися безпосередньо керівнику відділу інформаційної безпеки банку (Ciso) і визначати права та обов’язки, функції, відповідальність, необхідні знання, досвід і кваліфікацію у посадовій інструкції співробітників відділу кіберзахисту.

Дотримання цих стандартів дозволяють забезпечити таки види безпеки:

1. Безпека інформації – охоплює захист інформаційних систем і даних, що зберігаються та передаються у рамках фінансової інфраструктури. До загроз безпеці інформації належать хакерські атаки, кіберзлочинність, витоки даних та несанкціонований доступ до систем.

2. Безпека операцій – охоплює захист фінансових операцій від шахрайства та маніпуляцій. До загроз безпеці операцій належать фінансові шахрайства, відмивання грошей, терористичне фінансування та інші незаконні дії.

3. Безпека платіжних систем – охоплює захист платіжних систем від витоку коштів, збоїв та зловживань. До загроз безпеці платіжних систем належать несанкціоновані транзакції, фальсифікація платежів та зловживання правом на доступ до систем.

4. Безпека систем розрахунків – охоплює захист систем розрахунків від системних ризиків, тобто ризиків, пов’язаних з функціонуванням та взаємозалежністю фінансових інститутів та ринків. До системних ризиків належать збої у системах розрахунків, недостатня ліквідність та дефолти.

Необхідно врахувати ці вимоги законодавства при оцінюванні стану об’єктів критичної інфраструктури при розробці консолідованого ресурсу.

1.3 Консолідація інформації для забезпечення безпеки фінансової інфраструктури

Консолідована інформація – це процес або результат об’єднання, синтезу або узагальнення різних даних, щоб створити цілісне представлення. Цей термін може застосовуватися до різних контекстів, включаючи фінансовий облік, звітність, управління проектами та інші сфери. [15-16]

Щоб розробити базу даних, необхідно орієнтуватися на кінцевого користувача, який є аналітиком, який приймає рішення на основі наданої інформації.

Консолідація інформації для забезпечення безпеки фінансової інфраструктури означає об’єднання даних з різних джерел інформації з метою аналізу безпеки та перевірки дотримання вимог законодавства. Цей процес може включати збір, обробку, аналіз та звітність про стан безпеки фінансової інфраструктури.

Одним з основних елементів консолідації інформації є централізована система, за допомогою якої проводиться збір даних про фінансові установи та їх об’єкти критичної інфраструктури, осіб, відповідальних за безпеку на цих об’єктах, рівень дотримання стандартів, стан безпеки різних систем цих об’єктів, таких як банківські системи, платіжні системи, безпекові системи та інші.

Після збору даних централізована система дозволяє аналітику провести аналіз безпеки об’єктів критичної інфраструктури для виявлення потенційних загроз та вразливостей фінансової інфраструктури. Результати аналізу використовуються для вжиття заходів з покращення безпеки цих об’єктів.

Консолідація інформації також включає у себе звітність про стан безпеки фінансової інфраструктури. Звіти можуть включати статистику по дотриманню безпеки об’єктів критичної інфраструктури у розрізі як одного, так і групи. Ці

звіти можуть використовуватись для рекомендацій щодо покращення і вдосконалення безпеки фінансової інфраструктури установи.

На рисунку 1.3 представлена узагальнена схема процесів, елементів та взаємозв'язків [17–19]. Інтеграція інформації пов'язана з багатьма іншими видами інформаційної діяльності, особливо індексацією та абстрагуванням, але це набагато складніша система з більшими потребами. Це основна проблема інтеграції інформації.

Рисунок 1.3. Узагальнена схема бізнес-процесів консолідації інформації

У порівнянні з багатьма (якщо не з усіма) видами інформаційної діяльності підвищується складність процесу, організації і підвищуються вимоги до людських, технічних і економічних ресурсів. При відборі та оцінюванні інтегрована інформація також включає різні філософії та підходи.

Тісна співпраця між експертами у прикладній та інформаційній галузях має важливе значення для успішної інтеграції.

Інтеграція даних – це багатоетапна, складна процедура та невід'ємний компонент процесу аналізу, що забезпечує рішення для аналізу високого рівня. Аналітична діяльність integrated information повинна враховувати ризики порушень інформаційної безпеки, постійно систематично аналізувати проблемну ситуацію, виявляти тенденції, що потребують оперативного реагування та прийняття управлінських рішень [20–21].

Існує декілька способів консолідації інформації для забезпечення безпеки інфраструктури:

1. ISMS (Information Security Management System) є інформаційною системою управління безпекою інформації.

ISMS – це систематичний підхід до управління безпекою інформації в організації. Він базується на міжнародному стандарті ISO 27001 і складається з політики безпеки, процедур, практик та технологій, які спрямовані на захист конфіденційності, цілісності та доступності інформації.

Це набір політик, процедур, процесів та технічних заходів, які призначені для ефективного управління ризиками, пов'язаними з інформаційною безпекою у організації.

ISMS дозволяє організаціям аналізувати, краще розуміти та управляти ризиками у сфері інформаційної безпеки, відповідно до встановлених міжнародних стандартів. Основний етап реалізації ISMS – це визначення політики інформаційної безпеки, включаючи оцінювання ризику, вибір заходів із захисту інформації, розробку процедур безпеки та надання компетентності персоналу.

ISMS забезпечує систематичний підхід до управління ризиками та характеризується постійним моніторингом, оцінкою та вдосконаленням політики інформаційної безпеки. Крім того, впровадження ISMS дозволяє організаціям відповідати вимогам законодавства щодо захисту конфіденційної інформації та даних клієнтів.

ISMS відповідає стандарту ISO/IEC 27001, який є міжнародним стандартом і подає принципи та вимоги для ефективного управління інформаційною безпекою.

Впровадження ISMS допомагає організаціям покращити свою інформаційну безпеку, зменшити ризики та захистити критичну інформацію.

ISMS допомагає організаціям ідентифікувати та управляти ризиками, пов’язаними з інформаційною безпекою, забезпечує розробку та впровадження політик, процедур та контрольних механізмів. Він також включає неперервне вдосконалення системи безпеки і організаційну культуру безпеки.

ISMS є важливим інструментом для забезпечення високого рівня безпеки інформації в організації, а також виконання вимог законодавства та міжнародних стандартів щодо захисту інформації і може містити такі компоненти, як:

– політика інформаційної безпеки;

– процедури інформаційної безпеки;

– технології інформаційної безпеки.

ISMS також включає у себе такі ключові елементи:

– установлення інформаційної безпеки: ISMS допомагає організаціям визначити цінність інформації та встановити механізми для її захисту. Це включає ідентифікацію активів, визначення рівня конфіденційності, цілісності та доступності, а також планування заходів з захисту.

– ризик-орієнтований підхід: ISMS допомагає організаціям визначити ризики, пов’язані з інформаційною безпекою, і розробити стратегії та заходи для їх зниження. Це включає оцінювання ризиків, встановлення контролів безпеки та планування непередбачених ситуацій.

– керівництво та зобов’язання: ISMS вимагає активного участі керівництва організації в управлінні інформаційною безпекою. Це включає призначення відповідальних осіб, визначення політики безпеки та стандартів, а також регулярну оцінку та оновлення системи.

– неперервне вдосконалення: ISMS пропонує цикл постійного вдосконалення, включаючи планування, впровадження, перевірку та дії. Організації повинні постійно оновлювати та вдосконалювати свої політики та процедури безпеки, враховуючи нові загрози та виклики.

– аудит та оцінювання: ISMS включає проведення аудиту та оцінювання ефективності системи. Це включає моніторинг та вимірювання результатів, виявлення потенційних проблем та несправностей, а також коригування та запобігання інцидентам безпеки.

– ISMS є важливим інструментом для будь-якої організації, оскільки забезпечує безпеку конфіденційних даних, захищає від потенційних загроз та сприяє дотриманню регуляторних вимог щодо захисту інформації.

2. SIEM (Security Information and Event Management) є системою, що поєднує у собі можливості збору, аналізу та відображення інформації про події та безпеку комп'ютерної мережі. SIEM використовується для моніторингу, виявлення та аналізу потенційних загроз безпеці, що дозволяє підвищити ефективність реагування на події безпеки.

Основні компоненти SIEM включають:

– збір даних: SIEM збирає дані про події та безпеку з різних джерел, таких як файрволи, системи виявлення вторгнень (IDS/IPS), сервери, бази даних та інші. Ці дані можуть бути зібрані у реальному часі або збережені для подальшого аналізу;

– нормалізація даних: SIEM нормалізує зібрані дані, щоб забезпечити їх однорідність та уніфікований формат; це дозволяє більш ефективно аналізувати та порівнювати дані з різних джерел;

– аналіз та виявлення загроз: SIEM застосовує різні методи аналізу та алгоритми для виявлення потенційних загроз безпеці, таких як вторгнення або аномалії, що можуть свідчити про атаку або порушення безпеки. SIEM використовує різні техніки, такі як правила кореляції подій, аналіз поведінки, машинне навчання та інші, для виявлення загроз та видавання алертів про них;

– журналювання та архівування: SIEM забезпечує зберігання та аналіз журнальних записів подій на тривалості часу, що дозволяє проводити ретроспективний аналіз та розслідування подій, а також забезпечує виконання вимог збереження даних згідно зі стандартами безпеки;

– візуалізація та звітність: SIEM надає можливість візуалізації даних та створення звітів, що допомагають аналітикам та адміністраторам системи швидко розуміти та реагувати на події безпеки.

Застосування SIEM дозволяє організаціям підвищити рівень безпеки, виявляти і запобігати кібератакам, швидше виявляти та відновлюватися від інцидентів безпеки, а також виконувати регуляторні вимоги щодо збереження та аналізу даних безпеки.

SIEM також може бути використана для виявлення вразливостей у системі та вдосконалення процесів безпеки шляхом аналізу подій та інформації про безпеку.

SIEM є важливим інструментом у сфері кібербезпеки, який допомагає організаціям протидіяти загрозам безпеки, виявляти вразливості та отримувати цінну інформацію про стан безпеки своєї комп’ютерної мережі.

3. Використання спільної платформи – це централізована база даних, до якої мають доступ багато організацій і використовуються ними для постачання інформації, обміну інформацією, отримання інформації згідно наданим доступам до системи.

Загалом консолідація інформації для аналізу безпеки фінансової інфраструктури є важливим етапом в управлінні ризиками і забезпеченні безпеки фінансових систем. Вона допомагає виявити потенційні загрози та вразливості і реагувати на них, щоб запобігти можливим інцидентам та захистити фінансову інфраструктуру.

1.4 Методи системного аналізу безпеки об’єктів

Системний аналіз безпеки критичних об’єктів фінансової інфраструктури включає у себе ряд методів, що допомагають ідентифікувати і оцінити ризики, розробити та впровадити заходи безпеки [22–36].

Етапи системного аналізу безпеки об’єктів:

– оцінювання стану безпеки критичного об’єкту: передбачає проведення аналізу існуючих заходів безпеки, виявляються вразливості і загрози;

– розробка заходів безпеки: передбачає розробку заходів, які мінімізують ризики, пов’язані з вразливостями та загрозами;

– впровадження заходів безпеки: передбачає практичне впровадження заходи безпеки;

– контроль ефективності заходів безпеки: передбачає проведення оцінювання ефективності впроваджених заходів безпеки.

Основі методи системного аналізу безпеки об’єктів:

– аналіз загроз;

– аналіз вразливостей;

– аналіз безпеки систем;

– аналіз безпеки процесів;

– аналіз ризиків.

Також можна використовувати й інші методи, такі як:

– SWOT;

– аналіз дерева помилок;

– аналіз сценаріїв.

Аналіз загроз – процес визначення потенційних загроз і проведення оцінювання потенційних загроз безпеці фінансової інфраструктури і включає у себе такі етапи:

– ідентифікація загроз: загрози ідентифікують та класифікують;

– оцінювання загроз: загрози оцінюють за такими критеріями:

- ймовірність реалізації;
- наслідки реалізації;
- критичність.

Аналіз загроз включає у себе технічний аналіз, який дозволяє оцінити технічний стан інфраструктури, таких як сервери, мережі, бази даних тощо, з метою виявлення можливих проблем безпеки:

– проводиться аудит мережевої інфраструктури, перевірка наявності її оновлень і патчів, аналіз конфігурацій, сканування портів, моніторинг мережевого трафіку;

– проводиться аудит серверів і сховищ даних, перевірка наявності оновлень, аналізуються налаштування доступу користувачів, стан програмних брандмауерів і проксі-серверів;

– аналіз програмного забезпечення: цей метод включає виявлення та виправлення дефектів, які можуть бути використані для атаки на систему; це може бути зроблено шляхом аналізу коду, проведення тестів на безпеку та використання методів статичного аналізу;

– аналіз безпеки баз даних: цей метод включає у себе оцінювання безпеки даних, таких як персональна інформація, фінансові дані тощо; це включає забезпечення правильного зберігання, а також захист від несанкціонованого доступу;

– аналізуються інші системи та процеси обміну і обробки даних, що використовуються в фінансовій інфраструктурі, для виявлення можливих вразливостей, які можуть бути використані зловмисниками;

– проведення спеціальних тестів;

– аналіз статистичних даних;

– ретроспективний аналіз інцидентів;

– рекомендації експертів.

Для проведення аналізу загроз можна використати такі методи:

– експертних оцінок: проведення оцінок загроз експертами;

– SWOT: оцінювання сильних та слабких сторін, можливості та загрози об’єкта.

Також, аналіз загроз може включати додаткові аналізи, які доповнюють основні методи системного аналізу безпеки об’єктів фінансової інфраструктури і забезпечують більш глибокий та повний аналіз безпеки:

– аналіз витоків інформації: цей метод включає виявлення можливого витоку чутливої інформації (інсайд); це може бути зроблено шляхом аналізу даних, використання обмежень доступу і шифрування;

– аналіз соціальної інженерії: цей метод визначає потенційні загрози, пов’язані з людським фактором, таких як недостатня свідомість про безпеку, слабкий пароль, недостатня навичка розпізнавання фішингу тощо, з метою отримати несанкціонований доступ до системи. Він включає у себе аналіз соціальних інженерних атак, таких як фішинг, фізичний доступ і шахрайство.

Використання цих методів у поєднанні з системним підходом дозволяє покращити рівень кібербезпеки і забезпечити ефективний захист фінансових систем від потенційних загроз та зловживань.

Аналіз вразливостей – процес виявлення вразливостей, які можуть бути використані зловмисниками для реалізації загроз.

Етапи аналізу вразливостей:

– ідентифікація загроз: загрози ідентифікують та класифікують;

– оцінювання загроз: загрози оцінюють за наступними критеріями:

- ймовірність реалізації;
- наслідки реалізації;
- критичність.

Для проведення аналізу вразливостей можна використати такі методи:

– метод аудиту безпеки: передбачає проведення аудиту безпеки об’єкта для виявлення вразливостей;

– метод тестування безпеки: передбачає проведення тестування безпеки об’єкта для виявлення вразливостей.

Аналіз безпеки систем – процес оцінювання безпеки систем, які використовуються на об’єкті.

Кібербезпека традиційно зосереджена на досягненні конфіденційності, цілісності та доступності.

Однією з відмінностей традиційних систем інформаційних технологій (IT) та автоматизованих систем управління технологічними процесами полягає у тому, що стратегія кібербезпеки традиційних інформаційних технологій спрямована, у першу чергу, на досягнення конфіденційності з необхідними засобами керування доступом для досягнення даної мети. При цьому цілісність інформації займає друге місце по важливості задачі. Доступність у даному випадку буде за пріоритетністю займати останнє місце [9].

Етапи аналізу безпеки систем:

– оцінювання безпеки систем: системи оцінюють за такими критеріями:

- конфіденційність
- цілісність
- доступність

– розробка заходів безпеки для систем: розробляють заходи, які допоможуть мінімізувати ризики, пов’язані з безпекою систем.

Для проведення аналізу безпеки систем можна використати такі методи:

– метод аудиту безпеки: передбачає проведення аудиту безпеки систем для виявлення вразливостей;

– метод тестування безпеки: передбачає проведення тестування безпеки систем для виявлення вразливостей.

Аналіз безпеки процесів – процес оцінювання безпеки процесів, які відбуваються на об’єкті.

Етапи аналізу безпеки процесів:

– оцінювання безпеки процесів: процеси оцінюють за такими критеріями:

- конфіденційність;
- цілісність;
- доступність;

– розробка заходів безпеки для процесів: розробляють заходи, які допоможуть мінімізувати ризики, пов'язані з безпекою процесів.

Для проведення аналізу безпеки процесів можна використати такі методи:

– метод аудиту безпеки: передбачає проведення аудиту безпеки процесів для виявлення вразливостей;

– метод тестування безпеки: передбачає проведення тестування безпеки процесів для виявлення вразливостей.

Аналіз ризиків – процес оцінювання ризиків, пов’язаних з об’єктом, і розробки заходів, які допоможуть мінімізувати ці ризики.

Етапи аналізу ризиків:

– ідентифікація ризиків: ідентифікують та класифікують за видами;

– оцінювання ризиків: ризики оцінюються за такими критеріями:

- ймовірність виникнення;
- наслідки виникнення;
- критичність;

– управління ризиками: на цьому етапі розробляються заходи, які допоможуть мінімізувати ризики.

Для проведення аналізу ризиків можна використати такі методи:

– метод експертних оцінок: передбачає проведення експертних оцінок ризиків;

– метод математичного моделювання: цей метод передбачає використання математичних моделей для оцінки ризиків.

Також, методи оцінюваня ризиків поділяються та 3 основні типи:

1. Методи, які пов’язані з кількісним оцінюванням ризиків (Mehari RiskWatch, ISAMM). Надають можливість оцінити ризики кількісно, мають чисельне значення величин як окремих ризиків так і загальної оцінки ризику, базуються на математичній статистиці, використанні економіко-математичних методів прийняття рішень, теорії ймовірностей.

2. Методи, які пов’язані з якісним оцінюванням рівня ризиків (OCTAVE, EBIOS, FRAP). Надають можливість визначити загрози, що впливають на рівень безпеки і можливі збитки, визначити заходи для зменшення або

уникнення ризику і надають розуміння, на скільки добре в даний момент здійснюється контроль.

3. Методи, які пов’язані з використанням обох вищезазначених метода і надають змішане оцінювання, як якісне, так і кількісне (MAGERIT, CRAMM, MSAT).

SWOT – метод, який дозволяє оцінити сильні та слабкі сторони, можливості та загрози об’єкта.

Сильні сторони об'єкта – це його позитивні характеристики, які можуть допомогти йому протистояти загрозам. Слабкі сторони об’єкта – це його негативні характеристики, які можуть зробити його більш вразливим до загроз. Можливості об’єкта – це зовнішні чинники, які можуть сприяти його безпеці. Загрози об’єкта – це зовнішні чинники, які можуть завдати шкоди його безпеці [18].

Для проведення аналізу SWOT можна використати такі інструменти:

– матриця SWOT: дозволяє представити сильні та слабкі сторони, можливості та загрози об’єкта у таблиці;

– діаграма SWOT: дозволяє представити сильні та слабкі сторони, можливості та загрози об’єкта у вигляді діаграми.

Метод аналізу дерева помилок – метод, який дозволяє виявити потенційні помилки та їх наслідки, передбачає побудову дерева, де ребро дерева представляє потенційну помилку, а вузол дерева – наслідки цієї помилки.

Для проведення аналізу дерева помилок можна використати такі інструменти:

– схематичне зображення дерева помилок: дозволяє швидко зрозуміти взаємозв’язок між помилками та їх наслідками;

– таблиця дерева помилок: дозволяє представити потенційні помилки та їх наслідки у табличній формі.

Метод аналізу сценаріїв – метод, який дозволяє розробити сценарії можливих подій та оцінити їх вплив, передбачає розробку сценаріїв можливих подій, які можуть впливати на безпеку об’єкта.

Сценарії оцінюються за такими критеріями:

– ймовірність виникнення;

– наслідки виникнення;

– критичність.

Для проведення аналізу сценаріїв можна використати такі інструменти:

– сценарій: опис можливої події, яка може впливати на безпеку об’єкта;

– таблиця сценаріїв: дозволяє представити сценарії можливих подій та їх оцінку.

Після отримання результатів дослідження можна переходити до заходів щодо покращення рівня безпеки:

1. Розробка стратегій безпеки: на основі отриманих результатів аналізу формулюються стратегії безпеки, що включають у себе рекомендації та рекомендовані заходи для забезпечення безпеки системи фінансової інфраструктури.

2. Впровадження заходів безпеки: реалізація розроблених стратегій безпеки шляхом впровадження рекомендованих заходів, таких як використання шифрування, встановлення механізмів аутентифікації, вбудовання механізмів контролю доступу тощо.

3. Моніторинг та аудит безпеки: проводиться постійний моніторинг безпеки системи фінансової інфраструктури для виявлення нових загроз та вразливостей. Проводиться аудит системи з метою перевірки дотримання встановлених правил та процедур безпеки.

Використання цих заходів допомагає забезпечити високий рівень безпеки об’єктів фінансової інфраструктури та запобігти можливим загрозам та атакам.

Дотримання встановлених стандартів щодо кібербезпеки і фізичної безпеки на об’єктах фінансової інфраструктури значно збільшує шанси на виявлення потенційних загроз, забезпечення ефективного ризик-менеджменту і захисту фінансових систем від зловживань та кіберподій. Постійне удосконалення методів системного аналізу безпеки є важливим елементом забезпечення безпеки фінансової інфраструктури в умовах постійно зростаючих загроз.

1.5 Аналіз сучасних методів автентифікації користувачів інформаційного ресурсу

Аутентифікація користувачів – це процес підтвердження ідентичності користувача або визначення, що користувач є тим, ким він вдається бути. Цей процес зазвичай виконується перед наданням користувачам доступу до певних ресурсів або послуг, таких як системи комп'ютерної мережі, приватні файли або банківські рахунки.

Аутентифікація виконується для забезпечення конфіденційності, цілісності та доступності інформації або ресурсів і для запобігання несанкціонованому доступу до них. Вона є важливою складовою безпеки і технологій захисту інформації.

Автентифікація користувачів інформаційного ресурсу є важливою складовою безпеки даних, оскільки вона дозволяє перевірити ідентичність користувача перед наданням доступу до ресурсу.

Сучасні методи автентифікації користувачів включають:

1. Логін та пароль: це найбільш поширений метод, який вимагає від користувача введення унікального ідентифікатора (логіна) та пароля. Однак, цей метод має свої недоліки, такі як компрометація пароля або можливість його підбору. Пароль вважається сильним, якщо він складається з комбінації букв верхнього та нижнього регістрів, цифр і спеціальних символів. Однак, паролі можуть бути підірвані шляхом жаргон-атак, відображенням на моніторі або викраденням через кібератаки.

2. Двофакторна (багатофакторна) аутентифікація – посилена аутентифікація, яка вимагає від користувача введення двох незалежних автентифікаційних факторів, таких як пароль та одноразовий код, отриманий через SMS або іншим способом. Це значно збільшує безпеку, оскільки навіть якщо хтось зламає один фактор, він не зможе отримати доступ без іншого фактора.

3. OTP (One-Time Password) або одноразовий пароль – використовується для тимчасової автентифікації користувача. Користувачу надсилається одноразовий

пароль, який він повинен ввести для отримання доступу. Цей пароль може бути надісланий через SMS, електронну пошту або генеруватись спеціальними пристроями або програмами, наприклад, Google Authenticator.

Цей метод може використовуватись як самостійний спосіб автентифікації або, у поєднанні з іншими методами, може виконувати роль другого фактору.

4. Автентифікація через соціальні мережі: цей метод дозволяє користувачам автентифікуватись на інших веб-сайтах або додатках, використовуючи обліковий запис в іншому сервісі (наприклад, автентифікація за допомогою Google або Facebook). Зазвичай, при цьому використовується протокол OAuth, який надає веб-сайту або додатку обмежений доступ до інформації користувача без розкриття його пароля. Це зручний спосіб для користувачів, оскільки вони не повинні створювати новий обліковий запис і запам’ятовувати новий пароль.

5. Біометричні дані: цей метод використовує фізичні характеристики користувача, такі як відбитки пальців, сканер обличчя або розпізнавання голосу для автентифікації. Використання біометричних даних дозволяє створити унікальний і надійний спосіб ідентифікації користувачів. Це дозволяє уникнути проблем, пов’язаних з викраденням або використанням паролів та інших традиційних методів автентифікації, забезпечує високу ступінь безпеки, оскільки ці дані є унікальними для кожної особи.

6. Розпізнавання шаблону набору: цей метод використовується на мобільних пристроях, де користувач визначає своє унікальне руху пальця по екрану, для автентифікації. Це дозволяє зручно та ефективно автентифікуватись на пристрої, оскільки не потрібно запам'ятовувати паролі.

7. FIDO U2F (Universal 2nd Factor) і його наступник FIDO2: це стандарт, розроблений Альянсом FIDO (Fast Identity Online), який забезпечує зручну і безпечну двофакторну аутентифікацію. Користувачі використовують фізичний ключ (наприклад, USB-ключ), який містить криптографічні ключі для автентифікації. Цей спосіб автентифікації гарантує захист від фішингу та атак перехоплення.

8. Сертифікати: цей метод використовує електронні сертифікати, що підтверджують ідентичність користувача. Сертифікати можуть бути видані авторитетом сертифікації, який перевіряє дані користувача та видає йому сертифікат. Користувач може використовувати цей сертифікат для автентифікації на різних ресурсах.

9. Аналіз поведінки користувача: цей метод використовує аналіз поведінки індивідуального користувача, такий як швидкість набору тексту, спосіб наведення курсору тощо, для визначення його ідентичності.

10. Використання синхронних або асинхронних механізмів шифрування, таких як SSL/TLS або SSH. Ці механізми забезпечують конфіденційність і цілісність даних під час передачі між користувачем і системою.

11. Автентифікація на основі IP-адреси – метод, який використовується для перевірки IP-адреси користувача для впізнавання та контролю доступу.

12. Автентифікація на основі пари IP-адреси і MAC-адреси – метод, який використовується для перевірки пари IP-адреси і MAC-адреси користувача для впізнавання та контролю доступу.

13. Фактори заслуг: цей метод використовує відомості та докази про володіння унікальними факторами, які можуть підтвердити ідентичність користувача. Наприклад, користувач може надати докази про наявність конкретних знань, навичок або носити ідентифікатор для підтвердження.

14. Автентифікація на основі візуальних методів – метод, у якому використовуються візуальні елементи для автентифікації, такі як CAPTCHA або вказування точок на певному зображенні.

15. Використання блокчейн технологій для автентифікації. Блокчейн забезпечує безпеку та безперервну доступність даних, а автентифікація на основі блокчейн може використовувати криптографічні методи для визнання ідентичності користувача.

16. Контекстна аутентифікація: цей метод використовує контекстну інформацію, таку як місцезнаходження, час доступу, тип пристрою, для аутентифікації користувача. Наприклад, якщо звичайно користувач займається

діяльністю в одному регіоні, але раптом з’являється запит з іншого регіону, може бути запит на додаткову аутентифікацію.

17. SMS-аутентифікація – це процес підтвердження ідентифікації користувача за допомогою одноразового пароля, який надсилається на його мобільний телефон у вигляді SMS-повідомлення. Цей метод аутентифікації використовується для забезпечення додаткового рівня безпеки при доступі до різних веб-сайтів, додатків або функцій.

Однак, SMS-аутентифікація також має свої обмеження і потенційні ризики. Зокрема, зловмисники можуть перехопити SMS-повідомлення з одноразовим паролем. Також, іноді можуть виникати проблеми з доставкою SMS-повідомлень або затримками в їх отриманні, що може створити незручності для користувачів.

18. Аутентифікація на основі утилітил: цей метод використовується для обробки інформації з пристроїв або програмного забезпечення, які використовуються користувачем, для підтвердження його ідентичності. Наприклад, може вимагатися наявність певного пристрою або програми для входу в систему.

19. Сесійна аутентифікація: цей метод вимагає підтвердження ідентичності користувача кожного разу при початку нової сесії. Користувач має вводити свої дані аутентифікації при кожному вході.

20. Аутентифікація на основі технології блокування: цей метод використовується для розпізнавання унікальних маркерів на фізичних пристроях або мобільних телефонах для аутентифікації користувача.

21. Карти доступ, також відомі як картки ключів є фізичними пристроями, які використовуються для отримання доступу до захищених приміщень або ресурсів. Це можуть бути ідентифікаційні картки, які вміщують у себе електронний чіп або магнітну смужку, яка містить інформацію про дозволений доступ. Карти доступу можуть бути також безконтактними картами, які використовують радіочастоту для комунікації з читачем. Для отримання доступу, користувач приставляє карту до читача або пропускного пункту, який перевіряє її дійсність та наявність прав доступу. Карти доступу широко застосовуються в

офісах, готелях, аеропортах, банках, а також в інших приміщеннях, які потребують контролю доступу.

Багато карт доступу також можуть бути програмованими і керованими за допомогою програмного забезпечення. Це дозволяє адміністраторам встановлювати обмеження, права доступу та графіки роботи. Карти доступу можуть бути використані самостійно або у поєднанні з іншими системами безпеки, такими як системи відеоспостереження або системи адміністрування присутності. Деякі картки доступу також можуть включати біометричні сканери, такі як сканери відбитків пальців чи сканери радужної оболонки ока, для додаткового рівня ідентифікації.

Карти доступу можуть бути безприводними (тобто без батареї) або приводними (тобто з батареєю). Безприводні карти отримують енергію від читача, коли їх приставляють до нього, тоді як приводні карти мають власну внутрішню енергію, що дозволяє їм комунікувати з читачем.

Кожна картка доступу створює запис про своє використання. Це дає можливість вести аудит активності користувачів та виявляти будь-які випадки недозволеного доступу або підозрілу активність.

Карти доступу також можуть бути легко видаляються або деактивовані у разі втрати або крадіжки, що забезпечує збереження безпеки системи. Крім того, використання карт доступу дозволяє уникнути необхідності у фізичних ключах, які можуть бути загублені або скопійовані.

У сучасних системах доступу додаткові функціональні можливості карт доступу можуть включати у себе автоматичну ідентифікацію працівника, реєстрацію часу роботи, контроль пропуску і навіть транзакції платежів.

Карти доступу є повсюдним і надійним засобом контролю доступу, який допомагає забезпечувати безпеку, захищати приватність та ефективно керувати доступом до ресурсів. Вони є важливим елементом у сучасних системах безпеки.

Ці методи можуть бути комбіновані для забезпечення більшої безпеки і зручності для користувачів. Важливо врахувати потреби та вимоги конкретного

інформаційного ресурсу при виборі методу автентифікації, їх порівняння наведено у таблиці 1.2.

Таблиця 1.2.

Порівняння методів автентифікації

Метод автентифікації	Простота впровадження (1–10)	Рівень безпеки	Зручність для користувача	Залежність від додаткових засобів	Поширеність використання
Ідентифікатор та пароль	10	Низький	7	Ні	Висока
Двофакторна аутентифікація	8	Високий	6	Так	Середня
Біометрична аутентифікація	7	Високий	8	Так	Середня
Одноразові паролі	8	Високий	7	Так	Середня
SMS-аутентифікація	9	Середній	6	Так	Середня
Аутентифікація за допомогою соцмереж	9	Середній	8	Так	Середня

Загалом, сучасні методи автентифікації користувачів інформаційного ресурсу стають більш безпечними та зручними, дозволяючи забезпечити доступ тільки авторизованим користувачам і захистити конфіденційну інформацію від несанкціонованого доступу.

Вибір конкретного методу автентифікації повинен залежати від вимог безпеки та зручності використання для конкретного інформаційного ресурсу.

1.6 Висновки та постановка задачі

У розділі було проаналізовано та розглянуто теоретичні аспекти створення консолідованого інформаційного ресурсу з метою аналізу безпеки фінансової інфраструктури. Результати дослідження та аналізу дозволяють зробити такі висновки:

1. Консолідований інформаційний ресурс є необхідним інструментом для ефективного аналізу безпеки фінансової інфраструктури. Він дозволяє збирати, обробляти та аналізувати дані з різних джерел, що дозволяє отримувати більш повну й об’єктивну картину стану безпеки фінансової системи.

2. Створення консолідованого інформаційного ресурсу вимагає використання сучасних технологій та методів обробки та аналізу даних. Це може включати у себе використання штучного інтелекту, машинного навчання, аналітики даних та інших інструментів.

3. Для ефективного аналізу безпеки фінансової інфраструктури необхідно мати доступ до різних видів інформації, включаючи дані про дотримання вимог законодавства у роботі об’єкта критичної інфраструктури, злочинну активність, кібератаки та інші аспекти безпеки. Консолідований інформаційний ресурс дозволяє об’єднати цю інформацію з різних джерел і забезпечити її аналіз у комплексі.

Задачі розділу:

– вивчити і проаналізувати сучасні технології та методи створення консолідованого інформаційного ресурсу для аналізу безпеки фінансової інфраструктури;

– розробити архітектуру та інфраструктуру для створення консолідованого інформаційного ресурсу; включити в неї компоненти для збору, обробки та аналізу даних з різних джерел;

– розробити алгоритми та методи аналізу даних для виявлення потенційних загроз безпеці фінансової інфраструктури;

– провести експерименти та тестування для перевірки ефективності розроблених методів і алгоритмів;

– розробити рекомендації щодо впровадження консолідованого інформаційного ресурсу в практику для аналізу безпеки фінансової інфраструктури; оцінити позитивний вплив цього ресурсу на безпеку фінансової системи та прийняття рішень з її підвищення;

– виявити проблеми та виклики, які можуть виникнути; здійснити аналіз можливих обмежень та обговорити можливі шляхи їх подолання;

– розробити стратегію і план дій для впровадження консолідованого інформаційного ресурсу в організацію аналізу безпеки фінансової інфраструктури; визначити етапи реалізації проекту, розподіл завдань та відповідальностей між учасниками;

– оцінити ефективність консолідованого інформаційного ресурсу під час його експлуатації; зібрати дані, провести аналіз та визначити показники успішності, такі як час відповіді, точність прогнозування загроз, кількість виявлених атак, а, також, атак, які вдалось запобігти та інші;

– зробити висновки про ефективність та користь консолідованого інформаційного ресурсу для підвищення безпеки фінансової інфраструктури; розробити рекомендації для наступного етапу розвитку та покращення ресурсу.

РОЗДІЛ ІІ. СТВОРЕННЯ ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ АНАЛІЗУ БЕЗПЕКИ ФІНАНСОВОЇ ІНФРАСТРУКТУРИ

2.1 Особливості створення інформаційного ресурсу аналізу безпеки фінансової інфраструктури

Фінансова інфраструктура – це сукупність установ, систем, послуг і технологій, які забезпечують функціонування фінансової системи в цілому. Ця інфраструктура створюється для підтримки фінансових транзакцій, обміну інформацією та ефективного функціонування різних фінансових ринків [37].

У світовій фінансовій літературі існують принаймні чотири ключові теорії щодо фінансової інфраструктури, які відрізняються поглядами на розвиток конкретних інститутів у фінансовому секторі. Значущість цих теорій визначається у контексті їх впливу на економічний ріст. Основні теорії розвитку включають у себе:

1. Теорії розвитку фінансових посередників;
2. Теорії розвитку фінансових ринків;
3. Теорії розвитку фінансових послуг;
4. Теорії розвитку законодавчої бази.

Фінансова інфраструктура – це оболонка, що оточує ринок, і пронизує весь спектр взаємин, що виникають всередині ринку. Його можна визначити як сукупність елементів (інститутів, інституцій, організацій, систем), які забезпечують і створюють умови для нормального, прозорого і безперебійного багаторівневого функціонування економіки при динамічному розвитку, русі і розподілі потоків капіталу між секторами, суб’єктами і об’єктами.

Основною метою основних гравців фінансової екосистеми є задоволення потреб кінцевого споживача, суб’єкта української економіки, якому в ході своєї діяльності необхідно використовувати різні фінансові продукти для досягнення своїх цілей. Саме кінцеві користувачі фінансових послуг привертають увагу всіх учасників фінансової екосистеми, оскільки створення умов для ефективної роботи

господарюючих суб’єктів є головним завданням всього фінансового сектора. З цією метою основні гравці екосистеми взаємодіють один з одним і створюють відповідні сервіси та продукти для споживачів. Успіх всієї екосистеми залежить від злагодженої та взаємовигідної роботи учасників, заснованої на відкритості та повазі інтересів учасників [38].

Потреби всіх економічних суб’єктів повинні задовольнятися шляхом надання відповідних фінансових послуг учасниками фінансової екосистеми, що є обов'язком чотирьох основних груп.:

1. Постачальник фінансових послуг – це компанія або державна установа, яка надає фінансові продукти та послуги безпосередньо кінцевим користувачам.

2. Інфраструктура та технології – це компанії та державні установи, які надають продукти, послуги та рішення постачальникам фінансових послуг та іншим учасникам фінансового сектору та додають цінності пропозиції споживачам фінансових послуг.

3. Регулювання і менеджмент, як правило, є державними органами, які створюють правила взаємодії учасників екосистеми і стежать за дотриманням цих правил.

4. Експертиза – це учасник ринку і державна установа, чиї послуги і рішення створюють основу для професійного розвитку учасників екосистеми.

Склад фінансової інфраструктури у різних аспектах представлений на рисунку 2.1, який відображає поточні та майбутні потреби представників усіх груп екосистеми, є як споживачем фінансових послуг, так і великим гравцем, що бере участь у створенні цих послуг, а також сприяє реалізації місії компанії. фінансовий сектор України.

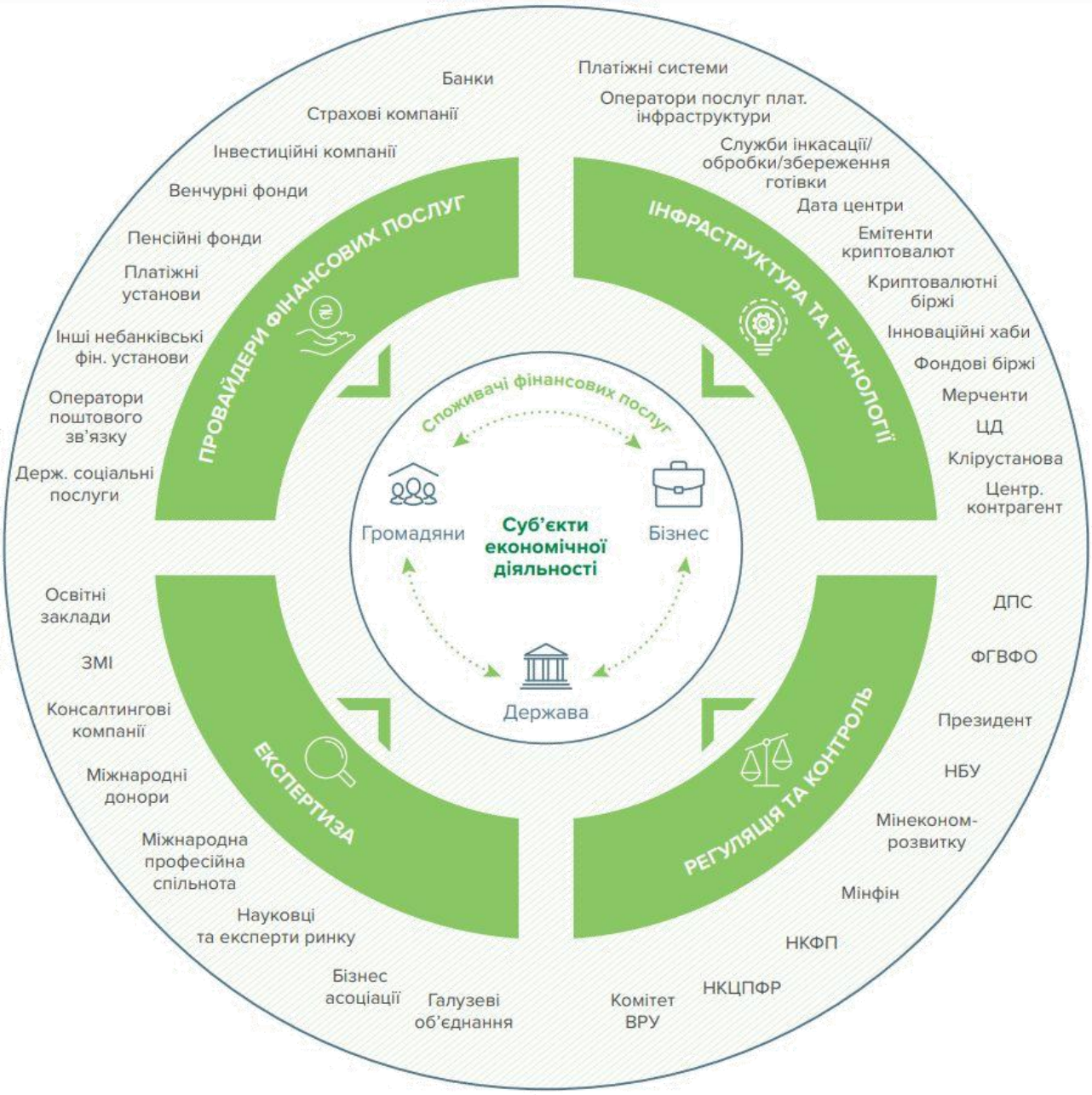


Рисунок 2.1. Склад фінансової інфраструктури у різних аспектах.

Також, на рисунку 2.2. відображено основні завдання фінансового сектору України: дорожню карту, стратегічні цілі і напрямки, місію і візію на майбутнє.

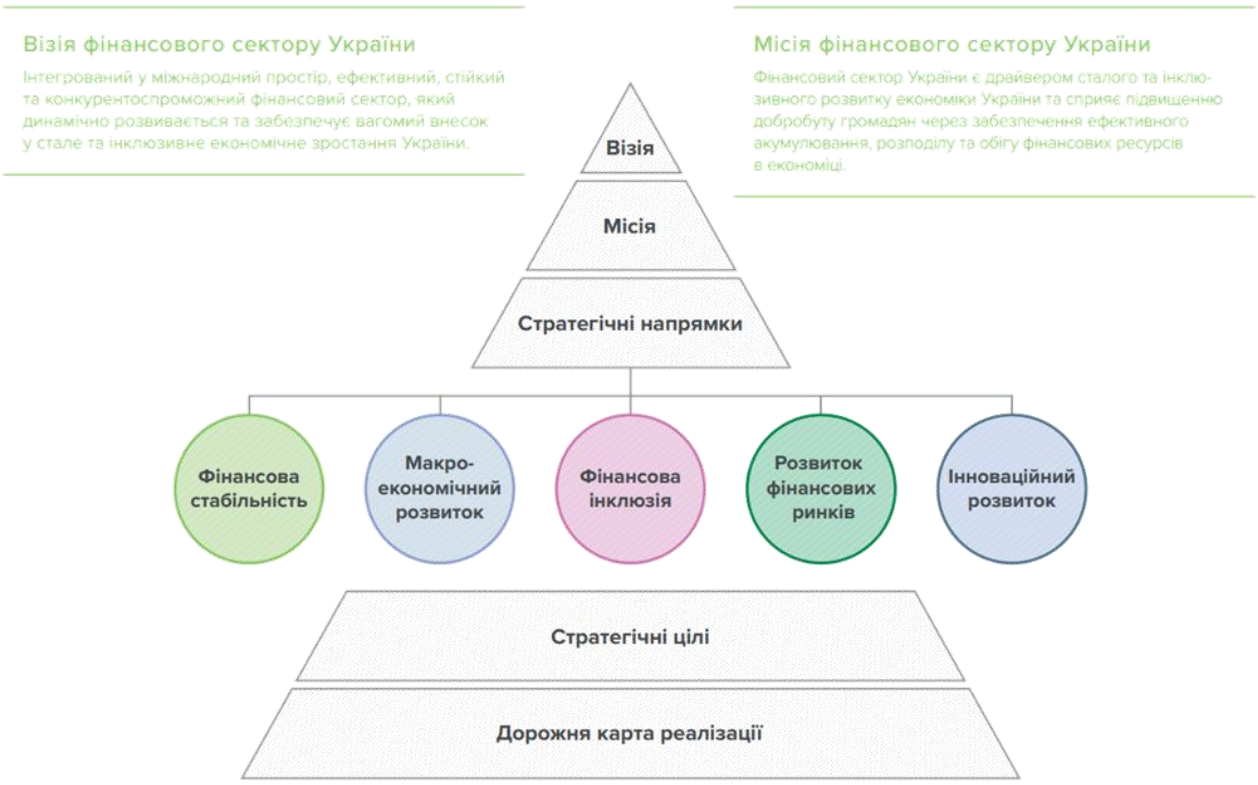


Рисунок 2.2. Цілі, візія і місія фінансового сектору України

Дотримання вимог стандартів ISO забезпечує надійну безпеку об’єктів фінансової інфраструктури і систем шляхом встановлення вимог та рекомендацій щодо управління ризиками, безпеки інформації. Однією з найважливіших вимог є відповідність стандартам ISO/IEC 27001:2015 (ISO/IEC 27001:2013, Cor 1:2014, IDT), ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT), ISO/IEC 27010:2018 (ISO/IEC 27010:2015, IDT), що допомагає фінансовим установам забезпечувати безпеку своїх інфраструктур, зменшувати ризики і покращує якість та надійність фінансових послуг.

Впровадження цих стандартів забезпечує:

1. Цілісність: фінансова інфраструктура повинна бути захищена від несанкціонованого доступу, зміни або знищення даних. Наявність механізмів контролю доступу та автентифікації користувачів, а також резервне копіювання даних.

2. Конфіденційність: інформація, що обробляється, повинна бути захищена від несанкціонованого доступу. Використання шифрування та інших методів захисту даних може бути ефективним способом забезпечити конфіденційність.

3. Доступність: фінансова інфраструктура повинна бути доступною для користувачів у будь-який час. Механізми масштабування та відновлення допоможуть забезпечити неперервну доступність.

Дотримання фінансовими установами вимог цих стандартів ISO є головним критерієм оцінювання рівня їх кібезахисту.

Забезпечення безпеки фінансової інфраструктури вимагає координації між усіма цими критеріями та застосування відповідних політик та процедур.

Аналіз безпеки фінансової інфраструктури має ключове значення для запобігання небажаним подіям. Він допомагає установам розібратися з потенційними загрозами та виробити ефективні стратегії безпеки для мінімізації ризиків.

Створення консолідованого інформаційного ресурсу має деякі особливості, які варто враховувати:

1. Визначення мети та цілей: перед початком створення консолідованого інформаційного ресурсу необхідно чітко встановити його мету та цілі. Наприклад, це може бути збір інформації з різних джерел для подальшого аналізу або створення централізованого доступу до інформації для користувачів.

2. Вибір технологій: важливо обрати правильні технології для створення інформаційного ресурсу. Це може бути веб-сайт, база даних, електронна бібліотека або інші типи програмного забезпечення. Вибір технологій залежить від потреб і вимог користувачів, доступних бюджетних можливостей та технічних обмежень.

3. Збір та обробка інформації: необхідно зібрати інформацію з різних джерел та обробити її, щоб вона була доступна для користувачів консолідованого ресурсу. Це може включати ручний внесок даних, автоматичний збір інформації за допомогою алгоритмів або роботів, а також обробку даних для забезпечення їхньої якості і структурованості.

4. Структурування інформації: важливо створити структуру для інформаційного ресурсу, яка дозволяє зручно організовувати та шукати інформацію. Це може включати створення розділів, тематичних категорій, тегів або інших засобів класифікації інформації.

5. Доступ до інформації: консолідований інформаційний ресурс повинен мати зручний спосіб доступу до інформації. Це може бути здійснено за допомогою пошукової системи, індексу, фільтрів або методу навігації по різним категоріям.

6. Забезпечення безпеки і захисту інформації: створюючи консолідований інформаційний ресурс, важливо враховувати питання безпеки і захисту інформації. Це означає захист від несанкціонованого доступу, втрати даних, а також резервне копіювання і забезпечення цілісності інформації.

7. Розширення та підтримка: консолідований інформаційний ресурс має бути гнучким і легкодоступним для розширення новою інформацією та оновленням існуючої. Також необхідно забезпечити постійну підтримку ресурсу, у тому числі виправлення помилок, враховувати потреби користувачів, оновлення інтерфейсу та функцій.

8. Визначення аудиторії та користувачів: перед створенням консолідованого інформаційного ресурсу важливо чітко визначити цільову аудиторію та потреби користувачів. Це допоможе врахувати їхні вимоги та забезпечити відповідний функціонал та зручний інтерфейс ресурсу.

9. Оновлення та підтримка контенту: важливо постійно оновлювати інформаційний ресурс і підтримувати актуальність контенту. Це може включати оновлення існуючої інформації, додавання нової, видалення застарілої та перевірку достовірності джерел. Також варто забезпечити можливість для користувачів вносити свої внески та оновлення.

10. Аналітика та звітність: створення консолідованого інформаційного ресурсу включає також встановлення системи аналітики для збору даних про користувачів, їх поведінку та використання інформації. Це допомагає зрозуміти, як ефективно використовується ресурс та як зробити його ще кращим, а також

забезпечує можливість створення звітів для оцінювання результатів і досягнення поставлених цілей.

Аналіз безпеки фінансової інфраструктури включає дослідження та оцінювання заходів, які приймаються для захисту фінансових установ від різних видів загроз.

Створення консолідованого інформаційного ресурсу – це складний процес, який вимагає детального планування, організації та визначення потреб та вимог користувачів, грамотного вибору технологій та методів структурування та обробки інформації. Врахування особливостей, які були описані вище, сприятиме успішному створенню і ефективному функціонуванню консолідованого інформаційного ресурсу.

2.2 Розробка бази даних консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури методом сутність-зв’язок

Розробка консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури методом сутність-зв’язок передбачає створення бази даних, яка буде зберігати інформацію про різні сутності, пов’язані з безпекою фінансової інфраструктури, а також зв’язки між цими сутностями.

До основних етапів створення захищеного консолідованого інформаційного ресурсу належать [39-49]:

– проектування ER-моделі консолідованого інформаційного ресурсу;

– побудова бази даних;

– нормалізація бази даних;

– розроблення інтерфейсу;

– захист інформації у бази даних;

– застосування створеного консолідованого інформаційного ресурсу для отримання звітів аналізу безпеки.

Розглянемо кожен етап окремо.

Проектування ER-моделі консолідованого інформаційного ресурсу.

Щоб створити базу даних, необхідно врахувати усі особливості фінансової індустрії. Щоб правильно створити базу даних, потрібно розробити ER-модель, засновану на принципі «взаємозв’язків сутності».

Модель сутність-зв’язок – це набір понять, що використовуються для опису логічної структури бази даних.

Базис понять семантичного моделювання загалом містить:

– визначення реалізованого об’єкта;

– визначення об’єкта;

– типу;

– визначення зв’язку між об’єктами;

– визначення властивості об’єкта;

– визначення ідентифікує властивості об’єкта.

Для моделі «сутність–зв’язок» базовими є поняття:

– сутність;

– зв’язок;

– атрибут.

Модель відносин сутностей заснована на графічному підході. Графічні інструменти використовуються для представлення різних аспектів структури даних, таких як об’єкти, властивості об’єктів, зв’язки між об’єктами та властивості посилань.). Будь-який фрагмент області, що цікавить, може бути представлений як набір сутностей, між якими існує кілька наборів зв’язків.

Сутність – це клас подібних об’єктів, і ця інформація повинна враховуватися у моделі. Кожна сутність повинна мати ім’я, представлене іменником однини.

Атрибут сутності – це іменована характеристика, яка є властивістю сутності. Назва атрибута має бути виражено іменником в однині (його можна охарактеризувати прикметниками).

Ключ сутності – це неповний набір атрибутів, значення яких у сукупності унікальні для кожного екземпляра сутності. Недолік надійності полягає в тому, що видалення атрибута з ключа порушує його унікальність.

З’єднання – це свого роду з’єднання між 2 сутностями. Одна сутність може бути пов’язана з іншою сутністю або з самою собою. З’єднання дозволяє знаходити інші сутності, пов’язані з 1 сутністю.

Процес розробки бази даних спрямований на створення структурованої системи, яка враховує важливі аспекти аналізу безпеки фінансової критичної інфраструктури, забезпечуючи високу якість зберігання та обробки інформації для підтримки прийняття рішень та вчасної реакції на потенційні загрози.

При проектуванні цієї бази даних важливо буде встановити правильні залежності між сутностями і зв’язками, а також забезпечити цілісність і консистентність даних. Для цього можна використовувати різні методи, такі як нормалізація, використання первинних та зовнішніх ключів, установка обмежень тощо.

Основні сутності фінансової інфраструктури:

1. User – користувач системи;
2. Financial Institution – фінансова установа: банк, страхова компанія, інвестиційний фонд, біржа та інші регульовані установи, які займаються обробкою, зберіганням та передаванням фінансової інформації і коштів;
3. FinancialInstitution Type – тип фінансових установ;
4. ObjectKI – об’єкт критичної інфраструктури фінансової установи і його системи критичної інформаційної інфраструктури: системи та мережі – технологічні інфраструктури, такі як платіжні системи та інші цифрові платформи, які забезпечують передавання фінансових операцій та обробку фінансової інформації;
5. Implementation Level – рівень впровадження заходів кіберзахисту;
6. Contact – контакти;
7. Criticality Categories – категорії критичності об’єктів;
8. Region – містить інформацію про область розміщення;
9. Settlement – містить інформацію про місто розміщення;
10. Operator – організація, відповідальна за забезпечення захисту;
11. Audit – результат аналізу безпеки;

Визначимо зв’язки між сутностями:

User здійснює Audit;

Financial_institution – має – Financial institution Type;

Financial_institution – має – Region;

Financial_institution – має – Area;

Financial_institution – має – Settlement;

Financial_institution – має – Operator;

ObjectKI – належить – Financial_institution;

ObjectKI – має – Categories_of_criticality;

ObjectKI – має – Region;

ObjectKI – має – Settlement;

Settlement – поділяє – Region;

FinancialInstitution містить ObjectKI.

Визначаємо атрибути обраних сутностей та ключі для кожної із сутностей:

Financial_institution:

name – назва установи

edrpou – ідентифікаційний код юридичної особи в ЄДРПОУ (унікальне)

street – вулиця

house – будинок

дата реєстрації

ObjectKI:

name – назва об’єкта

street – вулиця

house – будинок

Визначаємо ключі сутностей:

Financial_institution_Type (<financial_institution_type_id>,

financial_institution_type_name)

Region (<region_id>, region_name)

User (<User id>, first_name, last_name, email, password, ipn);

Audit (<Audit id>, audit name, user id, objectKI id, audit date, audit score);

FinancialInstitution (<FinancialInstitution id>, financial institution name, financial institution description, financial institution technical specification);

ObjectKI (<ObjectKI id>, object name, object type, object location, financial institution id);

Визначаємо ступінь зв’язку та класу належності сутностей «User» та «Audit» (рис. 2.3).

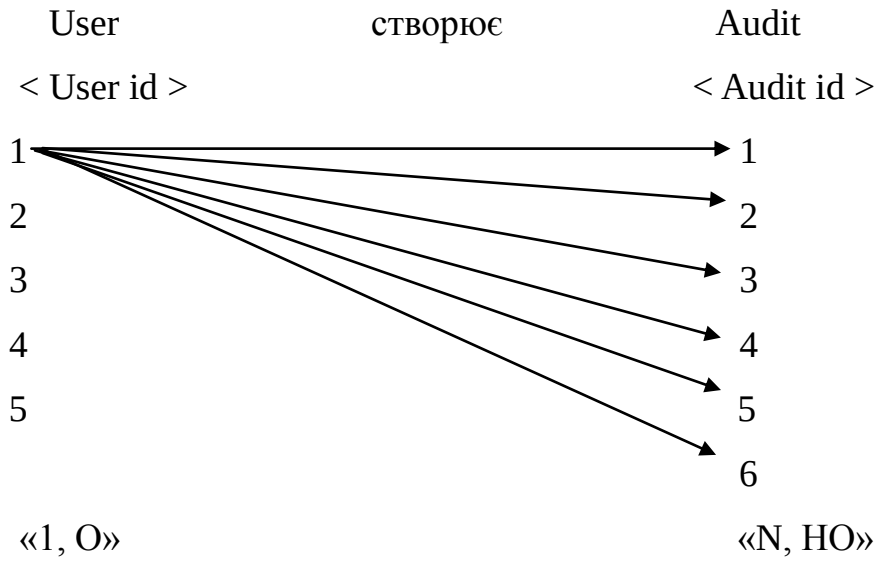


Рисунок 2.3. Аналіз зв’язку сутностей «Users» та «Audit»

Визначаємо ступінь зв`язку та класу належності сутностей «Audit» та «ObjectKI» (рис. 2.4):

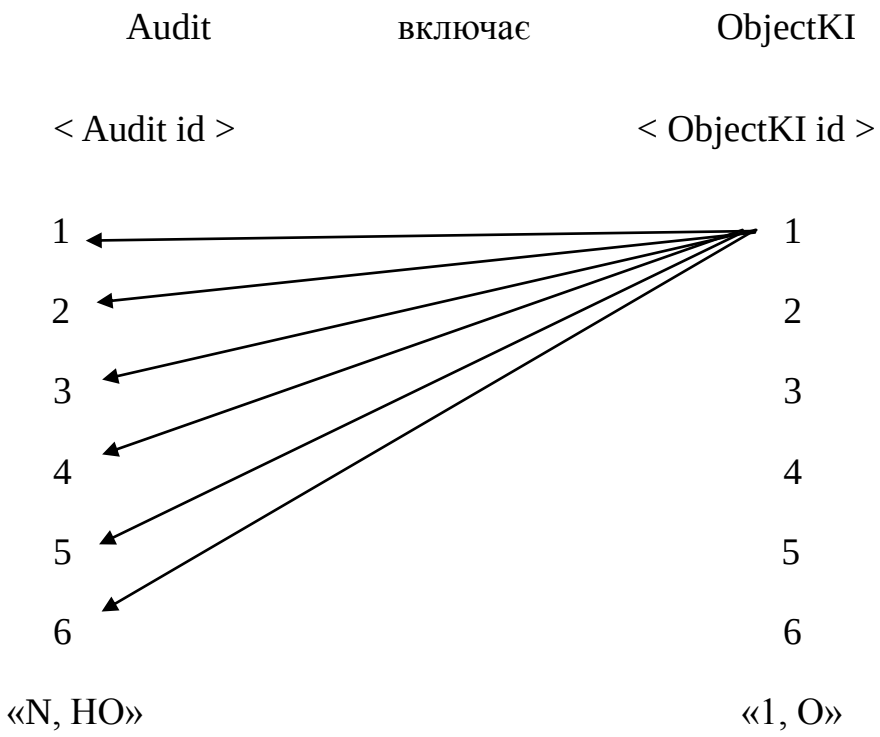


Рисунок 2.4. Аналіз зв’язку сутностей «Audit» та «ObjectKI»

Визначаємо ступінь зв`язку та класу належності сутностей «FinancialInstitution» та «ObjectKI» (рис. 2.5).

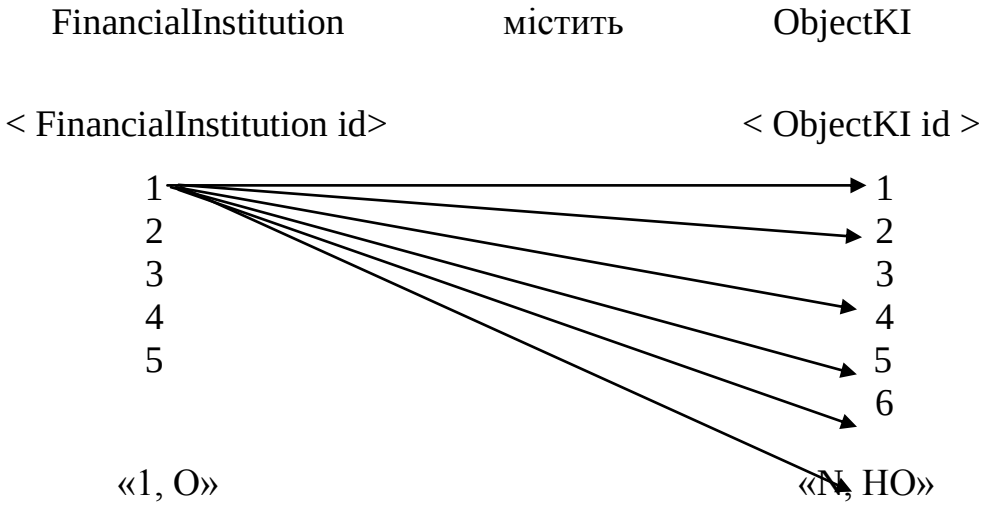


Рисунок 2.5. Аналіз зв’язку сутностей «FinancialInstitution» та «ObjectKI»

Визначення ступеня зв’язку та класу належності сутностей «ObjectKI» та «Operator» (рис. 2.6).:

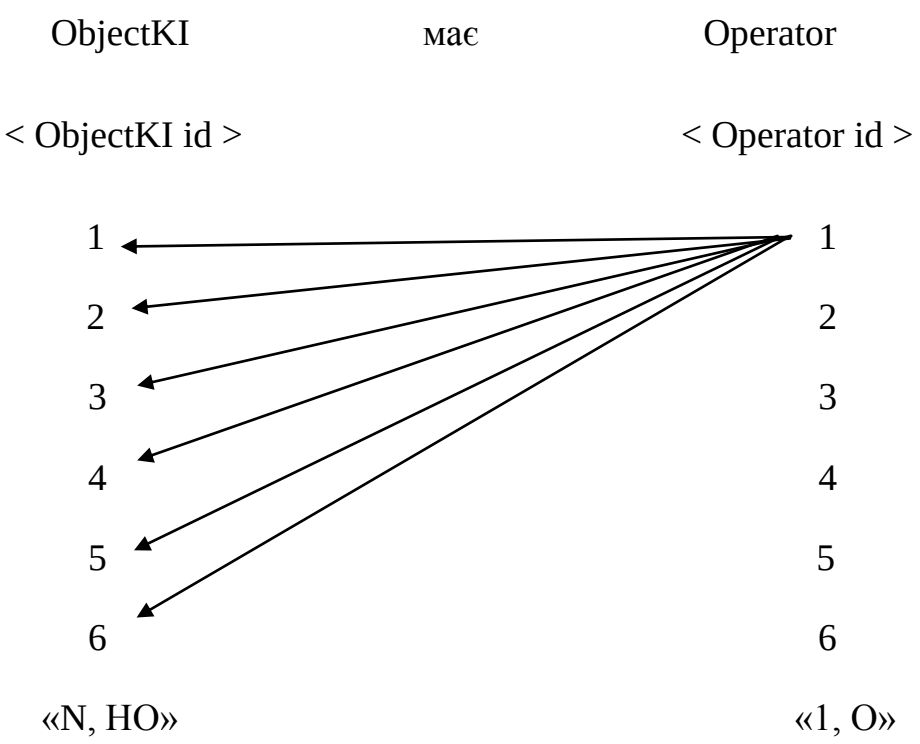


Рисунок 2.6. Аналіз зв’язку сутностей «ObjectKI» та «Operator»

Проектування ER-моделі.

Проектування ER-моделі бази даних – це процес створення абстрактної моделі бази даних, що використовує концепції сутність–зв’язок (ER) для представлення інформації та взаємозв’язків між різними об’єктами домену. ER-модель дозволяє описати структуру даних, визначити як дані будуть зберігатися та взаємодіяти між собою.

В результаті проектування отримаємо ER-модель, яку зображену на рисунку 2.7:

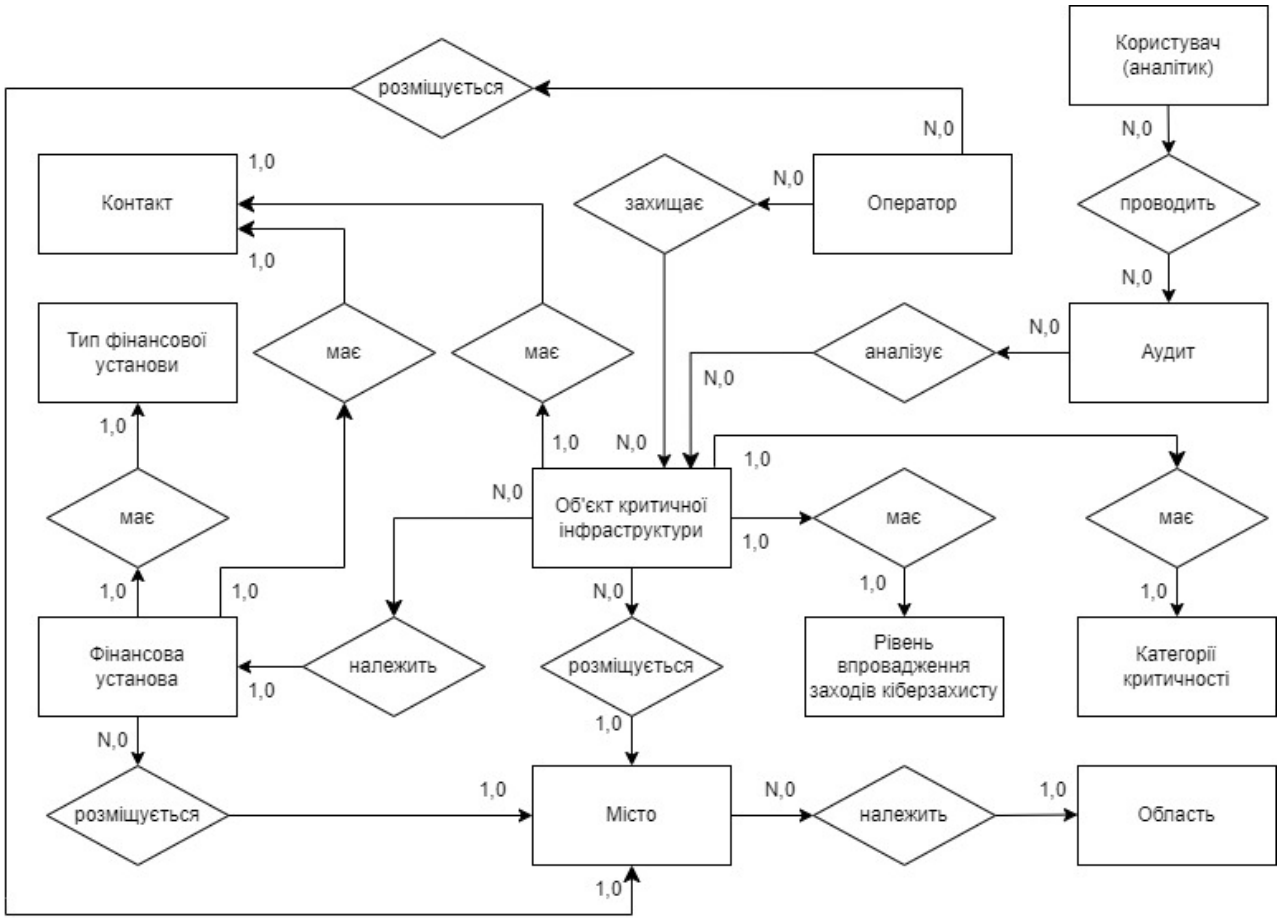


Рисунок 2.7. ER-модель бази даних

Виходячи з сутностей та їх атрибутів, отриманих вище, та усіх взаємозв'язків між сутностями у моделі ER, ми приступаємо до проектування таблиці бази даних для консолідованого інформаційного ресурсу, де атрибути діють як таблиці бази даних. Після створення таблиць їх необхідно заповнити даними. Дані в цих таблицях будуть атрибутами сутностей у кожній відповідній таблиці (рис. 2.8).

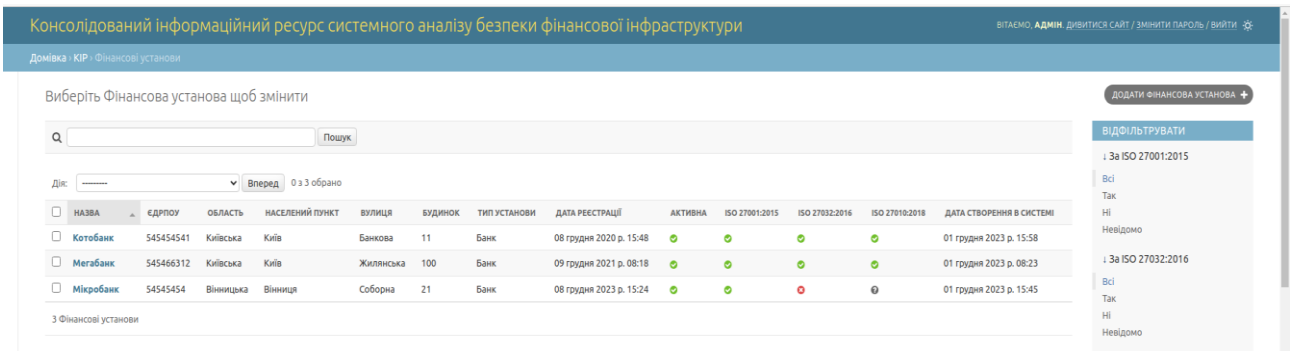


Рисунок 2.8. Вигляд таблиці Фінансові установи

Наступним кроком в реалізації бази даних є встановлення зв’язків між таблицями даних відповідно до їх первинних та вторинних ключів за допомогою UM-діаграми класів, як вказано на рис. 2.9.

2.3 Отримання кінцевих відношень бази даних за методом нормалізації відношень

Нормалізація – це процес заміни існуючої структури реляційної бази даних іншою, в якій відношення мають простий та вірний формат [50-51]. У теорії реляційних баз даних, процес нормалізації включає кілька послідовних нормальних форм, розроблених різними вченими:

– Перша, друга і третя нормальні форми (1НФ, 2НФ, 3НФ), що були винайдені Е.Ф. Коддом.

– Нормальна форма Бойса-Кодда (НФБК).

– Четверта нормальна форма (4НФ).

– П'ята нормальна форма або нормальна форма проекції–з’єднання (5НФ або НФПЗ), розроблені Р. Фейджиним.

Реляційне відношення перебуває у тій чи іншій нормальній формі, якщо задані на ньому функціональні залежності задовольняють певним умовам.

Процес переходу від початкового стану бази даних до нормалізованого включає кілька етапів. Перший етап полягає у приведенні відношення до першої нормальної форми, для чого необхідно відповідати таким умовам:

1. відсутність повторень атрибутів і кортежів.

2. відсутність впорядкування атрибутів і кортежів.

3. елементарність значень атрибутів у кортежах відношення.

4. усі кортежі відношення повинні мати однакову структуру.

5. імена атрибутів повинні бути різними, і значення кожного атрибуту повинні мати однаковий тип.

Перша нормальна форма.

Реляційне відношення вважається першою нормальною формою (1НФ), якщо всі його атрибути мають атомарні (прості) домени, що означає, що значення у кожній комірці таблиці неможливо поділити з точки зору будь-яких можливих використань.

Другий крок. Перехід до другої нормальної форми.

Нехай є відношення R з атрибутами A та B. Відношення R вважається в другій нормальній формі (2НФ), якщо атрибут B функціонально залежить від атрибуту A, і кожне значення R[A] відповідає точно одному значенню R[B]. Інакше кажучи, для будь-якого кортежу відношення R кожному значенню з множини атрибутів A відповідає лише одне значення з множини атрибутів B.

Також, друга нормальна форма може бути визначена як відношення, яке знаходиться у першій нормальній формі і в якому всі неключові атрибути повністю залежать від первинного ключа.

Отже, висновок може бути сформульований так: якщо первинний ключ є простим, то відношення автоматично вважається другою нормальною формою (2НФ).

Третій крок. Перехід до третьої нормальної форми. Транзитивна залежність виникає, коли неключовий атрибут залежить від іншого неключового атрибута, що, у свою чергу, залежить від ключового атрибута. У відношенні R(A*, B, C), де атрибут C залежить від атрибута B, який, у свою чергу, залежить від ключового атрибута A*, транзитивно залежить від A*.

Для усунення транзитивних залежностей використовується декомпозиція. В результаті отримуємо два нові відношення: R1(A*, B) і R2(B*, C), де атрибути розділені таким чином, щоб уникнути транзитивних залежностей.

Третя нормальна форма. Реляційне відношення вважається третьою нормальною формою (3НФ), якщо воно вже перебуває у другій нормальній формі і відсутні транзитивні залежності між непервинними атрибутами та можливими ключами. Іншими словами, усі непервинні атрибути функціонально незалежні один від одного у межах відношення.

Важливо відзначити, що відношення, що знаходиться у 3НФ, не може містити розрахункових полів.

Нормальна форма Бойса-Кодда (НФБК).

Вимоги нормальної форми Бойса-Кодда аналогічні вимогам 3НФ, тільки єдиний ключ у кожному відношенні є простим – складається лише з одного атрибуту.

Четвертий крок. Перехід до четвертої нормальної форми.

Багатозначна залежність представляє собою конкретний вид функціональної залежності, де атрибут B має багато значень для одного і того ж значення атрибута A. Наприклад, у випадку атрибутів "група: код студента=1:∞", де одній групі відповідає багато студентів, ми маємо справу з багатозначною залежністю.

Треба відзначити поняття тривіальної та нетривіальної багатозначної залежності. Залежності типу A – >>B і B – >>A вважаються тривіальними, тоді як залежність типу A – >>B і B ≠ >>A вважається нетривіальною.

Четверта нормальна форма (4НФ) вимагає, щоб у відношенні, яке вже перебуває у третій нормальній формі, будь-яка багатозначна залежність, визначена на множині атрибутів, була лише тривіальною або нетривіальною залежністю, для якої ліва частина є ключем.

У відношенні R(A*, B, C), атрибут A багатозначно визначає атрибут B, якщо B залежить тільки від A при всіх можливих комбінаціях з іншими атрибутами відношення. Якщо відношення містить багатозначні залежності, такі як A – >>B і A – >>C, то його слід розкласти на два інші відношення R1(A, B) і R2(A, C).

П'ята нормальна форма.

Реляційне відношення вважається п'ятою нормальною формою (5НФ), якщо воно вже знаходиться у четвертій нормальній формі і при подальшій декомпозиції отримані проекції включають у себе принаймні один потенційний ключ та хоча б один неключовий атрибут з початкового відношення. Для виявлення багатозначних залежностей потрібен глибокий семантичний аналіз атрибутів.

На практиці, четверта та п'ята нормальні форми використовуються при створенні складних баз даних. Цей процес нормалізації дозволяє усувати

різноманітні залежності між атрибутами, такі як неповні функціональні, транзитивні та нетривіальні багатозначні залежності. Це унеможливлює дублювання даних та запобігає виникненню аномалій при виконанні операцій вставлення, оновлення та вилучення даних.

В результаті, отримаємо UML-діаграму класів, що представлена на рис.2.9.

2.4 Забезпечення захисту створеного консолідованого інформаційного ресурсу

При дослідженні існуючих методів атак на інформаційні ресурси і захисту від них необхідно спочатку проаналізувати, які види захисту вже існують і надаються розробнику його фреймворком. Якщо наданого захисту недостатньо або необхідно його посилити, тоді виникає необхідність задіювання сторонніх бібліотек або самостійної розробки додаткового захисту.

В роботі виконано налаштування наданих фреймворком Django захистів і розроблено додатковий захист інформаційного ресурсу.

Виконано налаштування таких видів захисту інформаційного ресурсу:

1. Захист від міжсайтових сценаріїв XSS (Cross site scripting).

XSS-атаки дозволяють користувачеві впроваджувати сценарії на стороні клієнта в браузери інших користувачів. Зазвичай це досягається шляхом зберігання шкідливих сценаріїв у базі даних, де вони будуть отримані та відображені іншим користувачам, або шляхом спонукання користувачів клацати посилання, яке призведе до виконання JavaScript зловмисника у браузері користувача. Однак атаки XSS можуть виникати з будь-якого ненадійного джерела даних, наприклад файлів cookie або веб-служб, якщо дані недостатньо оброблені перед додаванням на сторінку. Використання шаблонів Django захищає вас від більшості атак XSS.

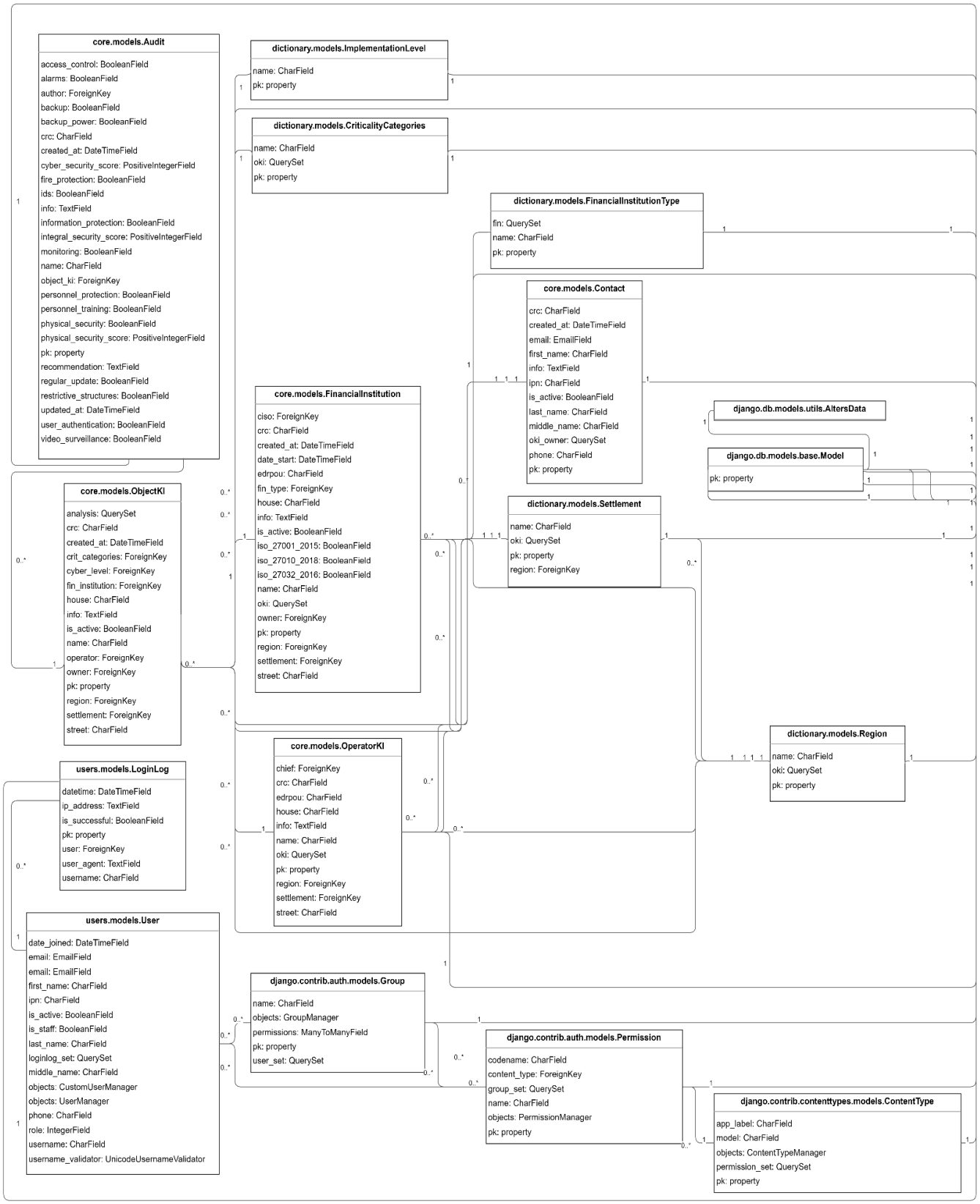


Рисунок 2.9. UML діаграма класів

2. Захист від підробки міжсайтового запиту CSRF (Cross-site request forgery).

Атака CSRF дозволяє зловмиснику використовувати облікові дані іншого користувача для виконання дії без відома або згоди цього користувача. Django має вбудований захист від більшості типів атак CSRF, якщо він увімкнений і використовується за потреби. Захист CSRF працює шляхом перевірки секретності кожного запиту POST. Це заважає зловмиснику «відтворювати» форму post на веб-сайті та дозволяти іншим користувачам несвідомо надсилати форму. Зловмисник повинен знати секрети, які залежать від користувача (використовуючи файли cookie).

3. Захист від SQL-ін’єкцій (SQL injection).

SQL-ін’єкція – це форма атаки, яка дозволяє зловмиснику виконувати довільний SQL-код у системі бази даних. Це може призвести до неправомірного видалення записів або розголошення конфіденційної інформації. Django захищає свої набори запитів від SQL-ін’єкцій, оскільки запити формуються з використанням параметризації, де SQL-код і параметри запиту визначаються окремо. Параметри екрануються базовим драйвером бази даних, оскільки вони можуть бути введені користувачем і, таким чином, становити потенційну загрозу безпеці. Django також дозволяє розробникам використовувати необроблені SQL-запити, але варто це робити обережно, завжди дотримуючись належних заходів безпеки і уникати передавання користувачем контрольованих параметрів.

4. Захист від клікджекінгу (Clickjacking).

Клікджекінг — це тип атаки, коли шкідливий сайт загортає інший сайт у фрейм. Ця атака може призвести до того, що нічого не підозрює користувача обманом змусить виконати ненавмисні дії на цільовому сайті. Django містить захист від клікджекінгу у формі, який у підтримуваному браузері може запобігти відображенню сайту у фреймі. Можна вимкнути захист для кожного перегляду або налаштувати точне значення заголовка, що надсилається X-Frame-Options middleware

5. Перевірка заголовка хосту (Host header check).

У деяких випадках Django використовує Hostзаголовок, наданий клієнтом, для створення URL-адрес. Хоча ці значення дезінфікуються, щоб запобігти атакам міжсайтового сценарію, фальшиве Hostзначення можна використовувати для підробки міжсайтових запитів, атак з отруєнням кешу та отруєння посилань у електронних листах. Оскільки навіть на перший погляд безпечні конфігурації веб-сервера сприйнятливі до підроблених Host-заголовків, Django перевіряє Hostзаголовки на відповідність ALLOWED_HOSTS.

6. Політика реферрерів (HTTP referrer).

Браузери використовують Referrer заголовок як спосіб надсилання інформації на сайт про те, як користувачі туди потрапили. Установивши політику реферрера, ви можете допомогти захистити конфіденційність своїх користувачів, обмеживши, за яких обставин Referrer встановлюється заголовок.

7. Політика відкриття між джерелами (Cross-origin opener policy).

Заголовок політики відкриття між джерелами (COOP) дозволяє браузерам ізолювати вікно верхнього рівня від інших документів, розміщуючи їх в іншу контекстну групу, щоб вони не могли безпосередньо взаємодіяти з вікном верхнього рівня. Якщо документ, захищений COOP, відкриває спливаюче вікно різного походження, window.opener властивість спливаючого вікна буде null. COOP захищає від перехресних атак.

8. Безпека сесії.

Подібно до обмежень CSRF, які вимагають розгортання сайту таким чином, щоб ненадійні користувачі не мали доступу до субдоменів, django.contrib.sessions також є обмеження.

9. SSL/HTTPS.

На сайті з міркувань безпеки завжди необхідно налаштувати роботу за протоколом HTTPS. Без цього зловмисні користувачі мережі можуть перехопити облікові дані автентифікації або будь-яку іншу інформацію, що передається між клієнтом і сервером, а в деяких випадках – активні мережеві зловмисники – можуть змінити дані, які надсилаються в будь-якому напрямку.

Посилено захист консолідованого інформаційного ресурсу за допомогою таких засобів:

1. Доступ користувача до системи відбувається шляхом введення логіна і пароля з підтвердженням коду двофакторні автентифікації.
2. Користувачі із різними ролями мають на сайті різні шляхи для входу в систему і різні доступи згідно своїй ролі у системі;
3. Записи у таблицях бази даних мають додаткове поле з контрольною сумою, яке захищає від можливої спроби несанкціонованої модифікації.
4. Розділення доступу до таблиць даних на рівні як ролі користувача так і індивідуальних дозволів користувача дозволяє убезпечити дані від редагування або перегляду без відповідного дозволу.
5. Створення журналу дій користувача ресурсу при зміні або видаленні даних.
6. Створення журналу спроб входу із фіксуванням IP-адреси відвідувача і інших його характеристик.

2.5 Висновки до розділу

Фінансова інфраструктура є важливою сутністю для функціонування фінансових ринків і забезпечення сприятливого середовища для фінансових операцій. У той же час, безпека фінансової інфраструктури піддається різного роду загрозам і ризикам, які можуть вплинути на її стабільність та надійність.

У даному розділі було проведено проектування бази даних консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури і визначення наборів сутностей, які представляють предметну область.

Також було посилено захист консолідованого інформаційного ресурсу за допомогою набору засобів і технологій.

РОЗДІЛ ІІІ. ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ ТА СИСТЕМНИЙ АНАЛІЗ БЕЗПЕКИ ФІНАНСОВОЇ ІНФРАСТРУКТУРИ

3.1 Обґрунтування вибору СУБД

Переваги вибору СУБД PostgreSQL для розробки консолідованого інформаційного ресурсу включають:

1. Висока надійність: PostgreSQL має механізми для забезпечення цілостності даних, роботи з транзакціями та відновлення після збоїв. Це дозволяє забезпечити безперебійну роботу консолідованого інформаційного ресурсу.

2. Підтримка багатьох схем: PostgreSQL дозволяє використовувати різні схеми в одній базі даних. Це дозволяє зберігати дані різних додатків у відокремлених схемах, що забезпечує можливість ефективної організації та обслуговування консолідованого ресурсу.

3. Розширена функціональність: PostgreSQL має багатий набір вбудованих функцій та можливостей, таких як підтримка географічних даних, робота з JSON, повнотекстовий пошук, робота з XML та інше. Це дозволяє зберігати та обробляти різні типи даних у консолідованому русурсі.

4. Масштабованість: PostgreSQL здатний обробляти великі обсяги даних та навантаження, дозволяючи ефективно масштабувати консолідований ресурс при необхідності. Він також підтримує реплікацію, що дозволяє створювати резервні копії та забезпечувати відмовостійкість системи.

5. Відкритий код та активна спільнота: PostgreSQL є вільно розповсюджуваною СУБД з активною спільнотою розробників. Це дозволяє швидко виявляти та виправляти помилки, а також надавати актуальні оновлення та підтримку.

6. Широкі можливості настроювання: PostgreSQL надає розширені можливості налаштування для оптимізації продуктивності бази даних. В ньому можна настроїти параметри даних, кешування, оптимізації запитів та інші

параметри, щоб максимально використовувати потужності вашого обладнання та задовольняти вимоги проекту.

7. Підтримка реплікації та кластеризації: PostgreSQL має вбудовану підтримку реплікації, що дозволяє створювати примірники бази даних для забезпечення високої доступності та збереження даних. В ньому можна використовувати різні розв’язки для кластеризації PostgreSQL для розподілу навантаження та забезпечення масштабованості.

8. Безкоштовність та відкритий код: PostgreSQL є вільно розповсюджуємою СУБД з відкритим кодом. Це означає, що ви можете використовувати його безкоштовно та змінювати його відповідно до ваших потреб. Крім того, відкритий код забезпечує доступ до внутрішніх механізмів бази даних, що дозволяє вам глибоко налаштувати та розширити функціональність СУБД.

9. Підтримка ANSI SQL та різних мов програмування: PostgreSQL виконує стандарти ANSI SQL, що дозволяє вам легко мігрувати ваші існуючі додатки на СУБД PostgreSQL. Він також підтримує різні мови програмування, такі як Python, Java, PHP, C++, що дозволяє вам реалізувати додатки з використанням вашої улюбленої мови програмування.

10. Велика активна спільнота та документація: PostgreSQL має велику та активну спільноту розробників, яка надає підтримку, відповіді на питання та допомогу вирішенню проблем. Крім цього, PostgreSQL має докладну документацію та численні ресурси, що допомагає швидко освоїти та використати усі можливості цього СУБД.

11. Висока продуктивність: PostgreSQL володіє оптимізованим двигуном для виконання складних запитів та операцій з базою даних. Він підтримує індекси, оптимізацію запитів та механізми кешування, що робить його ефективним для роботи з великими обсягами даних та високим навантаженням.

12. Багатоплатформовість: PostgreSQL доступний для різних операційних систем, включаючи Windows, macOS і різні дистрибутиви Linux. Це дає свободу вибору операційної системи, що найкраще підходить для розроблюваного проекту.

13. Розширюваність: PostgreSQL дозволяє створювати власні функційність та розширення, використовуючи мову програмування PL/pgSQL або інші мови, які підтримуються. Це дозволяє розширити можливості бази даних під свої потреби та вимоги проекту.

14. Легка інтеграція з іншими інструментами: PostgreSQL має багато драйверів та інтеграцій з різними інструментами розробки, такими як ORM-бібліотеки, BI-системи, ETL-рішення та інші. Це дозволяє легко інтегрувати базу даних з іншими системами та використовувати потужність інших інструментів для розробки нашого консолідованого інформаційного ресурсу.

15. Підтримка стандартів: PostgreSQL дотримується стандартів SQL і ACID (атомарності, консистентності, ізольованості і довіри) для забезпечення надійності та цілісності даних. Це робить його сумісним з іншими базами даних та забезпечує переносимість даних між різними системами.

16. Захист даних: PostgreSQL надає різні механізми для захисту даних, включаючи налаштовувані рівні прав доступу, шифрування та аудиторію. Це дозволяє нам контролювати доступ до даних та забезпечувати їх конфіденційність та цілісність.

Вибір СУБД PostgreSQL для розробки консолідованого інформаційного ресурсу має безліч переваг, які роблять його привабливим вибором для проектів будь-якого розміру та складності. Він поєднує високу надійність, широкі можливості настроювання та розширення, захист даних

Отже, вибір СУБД PostgreSQL для розробки консолідованого інформаційного ресурсу може забезпечити надійну, гнучку та продуктивну платформу для збереження та обробки даних.

3.2 Обґрунтування вибору мови програмування

Переваги вибору мови програмування Python для розробки консолідованого інформаційного ресурсу:

1. Простота вивчення: Python відомий своїм простим і лаконічним синтаксисом, що робить його легким для вивчення навіть для початківців.

2. Велика спільнота: Python має велику і активну спільноту розробників, яка завжди готова надати підтримку і відповіді на питання.

3. Багато бібліотек: В Python є багато сторонніх бібліотек, які спрощують розробку консолідованого інформаційного ресурсу, такі як бібліотеки для роботи з регулярними виразами, обробки даних, веб-скрапінгу тощо.

4. Висока продуктивність: Python має високу продуктивність і швидкодію, завдяки широкому використанню вбудованих бібліотек, оптимізаційним технікам та можливості паралельного виконання коду.

5. Платформонезалежність: Python може працювати на різних операційних системах, таких як Windows, macOS, Linux, забезпечуючи широкі можливості та зручність у використанні.

6. Інтеграція з іншими мовами: Python може легко інтегруватися з кодом, написаним на інших мовах програмування, таких як C, C++, Java, що робить його досить гнучким і універсальним для різних задач.

7. Великі компанії використовують Python: Python добре підтримується і використовується такими великими компаніями, як Google, Facebook, Instagram, Dropbox, Spotify, Netflix та інші, що свідчить про його ефективність та можливості.

8. Багата документація: Python має велику кількість документації, яка пояснює синтаксис, функції та модулі, що дозволяє швидко знайти необхідну інформацію та розв’язати проблеми.

9. Підтримка об’єктно-орієнтованого програмування (ООП): Python підтримує ООП, що дозволяє розробникам створювати класи, об’єкти та зв’язки між ними, що полегшує організацію та управління кодом.

10. Велика кількість розширень: Python має велику кількість розширень (extensions) і модулів для вирішення різних задач. Наприклад, бібліотеки для роботи з базами даних, генерації звітів, парсингу XML та інших форматів, що дозволяє розширити базовий функціонал.

11. Підтримка мультиплатформеності і мультипроцесорності: Python має багатоплатформенну підтримку, що дозволяє запускати код на різних операційних

системах. Крім того, він також підтримує мультипроцесорність, що дозволяє прискорити обчислення за допомогою паралельного виконання коду.

12. Широкі можливості веб-розробки: Python має багато фреймворків для веб-розробки, таких як Django і Flask, які полегшують створення веб-додатків і API. Це дозволяє швидко розробляти інформаційний ресурс зі зручним і інтуїтивно зрозумілим інтерфейсом.

13. Широкий спектр застосувань: Python використовується в різних галузях, включаючи науку, фінанси, машинне навчання, великі дані, аналіз даних, інтернет-розробку, геодезію та багато інших. Це дозволяє розробникам розширити свій потенціал і розвиватися в різних напрямках.

14. Сумісність з іншими мовами: Python може взаємодіяти з кодом, написаним на інших мовах програмування, таких як Java або C++, що дає можливість використовувати бібліотеки та інструменти, написані на різних мовах.

15. Широкі можливості тестування: Python має багато різних фреймворків для тестування, таких як PyTest і unittest, що дозволяють швидко і ефективно тестувати інформаційний ресурс на різних рівнях, включаючи одиницеве тестування, функціональне тестування та інтеграційне тестування.

16. Підтримка розробки на різних платформах: Python підтримує розробку на різних платформах, включаючи настільні комп’ютери, сервери і мобільні пристрої, що дозволяє створювати інформаційні ресурси для різних цільових аудиторій.

17. Широкі можливості візуалізації даних: Python має багато бібліотек для візуалізації даних, таких як Matplotlib і Seaborn, які дозволяють створювати графіки, діаграми і інші візуальні елементи, що полегшує аналіз інформації і сприяє зрозумілості даних.

18. Інтегрована інтерпретація: Python має інтерактивну інтерпретацію, що дозволяє виконувати код на льоту та експериментувати з різними функціями та можливостями, що полегшує розробку та налагодження інформаційного ресурсу.

Загалом, вибір мови програмування Python для розробки консолідованого інформаційного ресурсу може забезпечити швидкий розвиток проєкту, простоту

розробки та підтримку, а також широкі можливості і інтеграцію з іншими технологіями.

3.3 Практична реалізація бази даних інформаційного ресурсу

Консолідований інформаційний ресурс аналізу безпеки фінансової критичної інфраструктури для організації та зберіганні інформації про користувачів, результати аналізів, фінансових організацій та їх об’єктів і заходів безпеки може використати такі розроблені таблиці:

– «User» – містить дані про користувачів системи, такі як логін, хеш пароля, ІПН, ім'я, прізвище, email і роль;

– «FinancialInstitution» – дані про фінансові установи: назва, ЄДРПОУ, область, місто, вулиця, будинок, пов’язаного CISO та власника, тип установи, примітки;

– «FinancialInstitutionType» – дані по типам фінансових установ;

– «ObjectKI» – міститть інформацію про окремі критичні об'єкти, включаючи назву, область, місто, вулицю, будинок, категорію критичності, пов’язаних фінустанови, CISO та власника;

– «ImplementationLevel» – містить дані про рівні впровадження заходів кіберзахисту на об’єкті критичної інфраструктури;

– «Contact» – дані про контактних осіб: ПІБ, ІПН, email, телефон і примітки;

– «CriticalityCategories» – дані по категоріям критичності об’єктів;

– «Region» – дані по назвам областей;

– «Settlement» – містить інформацію про назву міста і пов’язаною з ним областю;

– «Audit» – зберігає результати проведених аналізів безпеки: назву, дату проведення, опис, результати, аналітика та пов'язаний об’єкт критичної інфраструктури;

– «Operator» – містить інформацію про оператора, такі як назва організації, яка забезпечує захист об’єкту, її місцезнаходження, ЄДРПОУ, контакти керівника і власника.

Також в інших таблицях представлені технічні сутності, такі як:

– Журнал дій користувачів системи;

– Журнал спроб входу в систему;

– Пристрої TOTP користувачів (підтримка двофакторної автентифікації);

– Тип контенту (загальний інтерфейс високого рівня для роботи з моделями даних);

– Групи користувачів;

– Дозволи груп;

– Дозволи користувачів;

– Ролі користувачів (реалізовано як внутрішня сутність сутності користувача), наявні 2 ролі «Адміністратор» і «Аналітик», передбачає можливість додавання нових ролей з налаштуванням групових і особистих дозволів).

Детальна схема бази даних консолідованого інформаційного ресурсу аналізу безпеки фінансової критичної інфраструктури представлена на рисунках 3.1 та 3.2.

3.4 Розробка програмних модулів забезпечення захисту інформаційного ресурсу

Розробка програмних модулів забезпечення захисту інформаційного ресурсу є важливою складовою процесу створення безпечних інформаційних систем. Вони допомагають забезпечити високий рівень захисту, впровадити ефективні механізми доступу та забезпечити безпеку інформаційного ресурсу.

Цей процес має бути виконаний принципово, з урахуванням вимог безпеки і специфіки конкретного інформаційного ресурсу. Ретельне проектування, розробка та впровадження модулів забезпечення безпеки гарантують захист конфіденційності, цілісності та доступності інформаційного ресурсу.

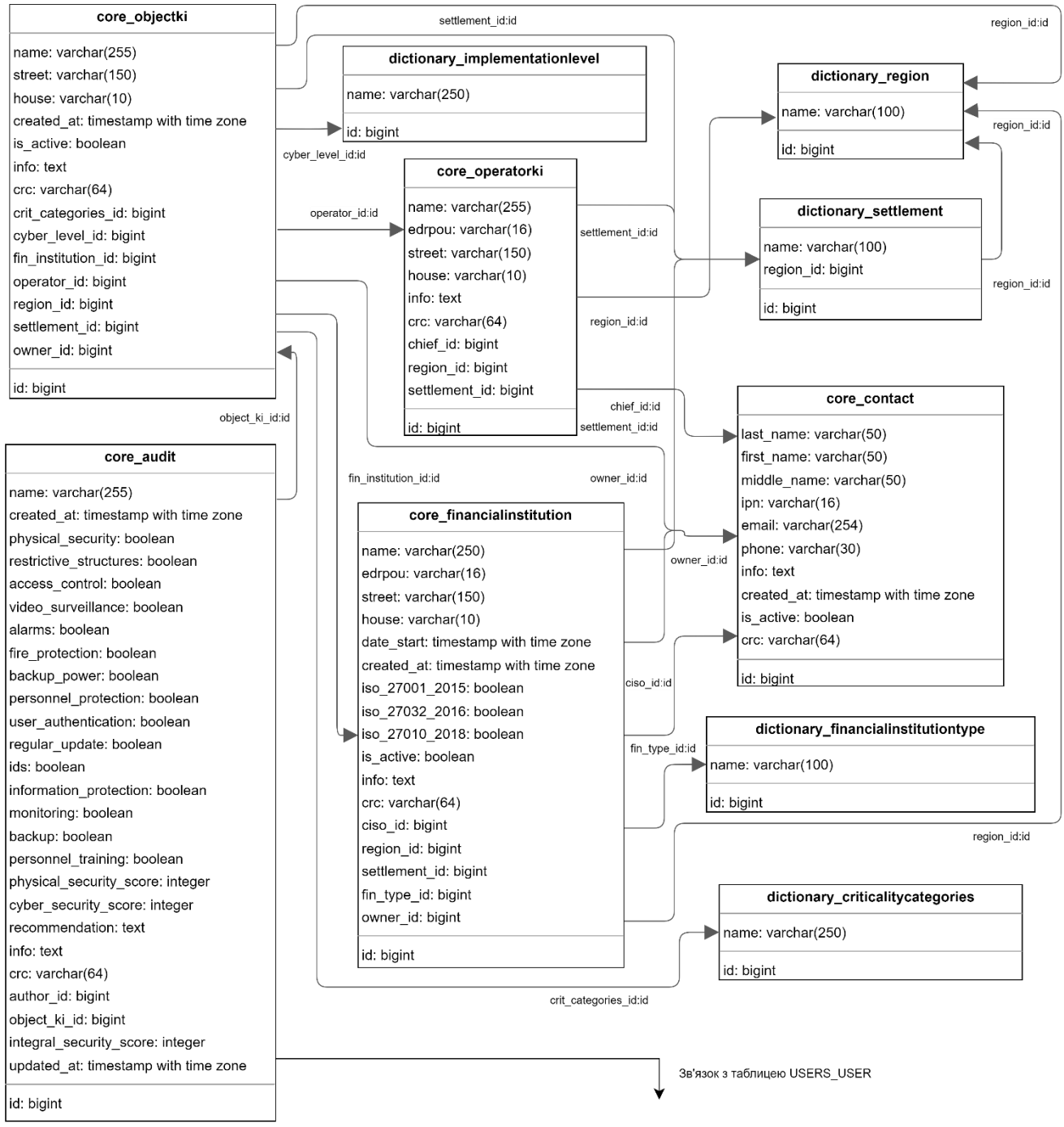


Рисунок 3.1. Схема бази даних, частина 1.

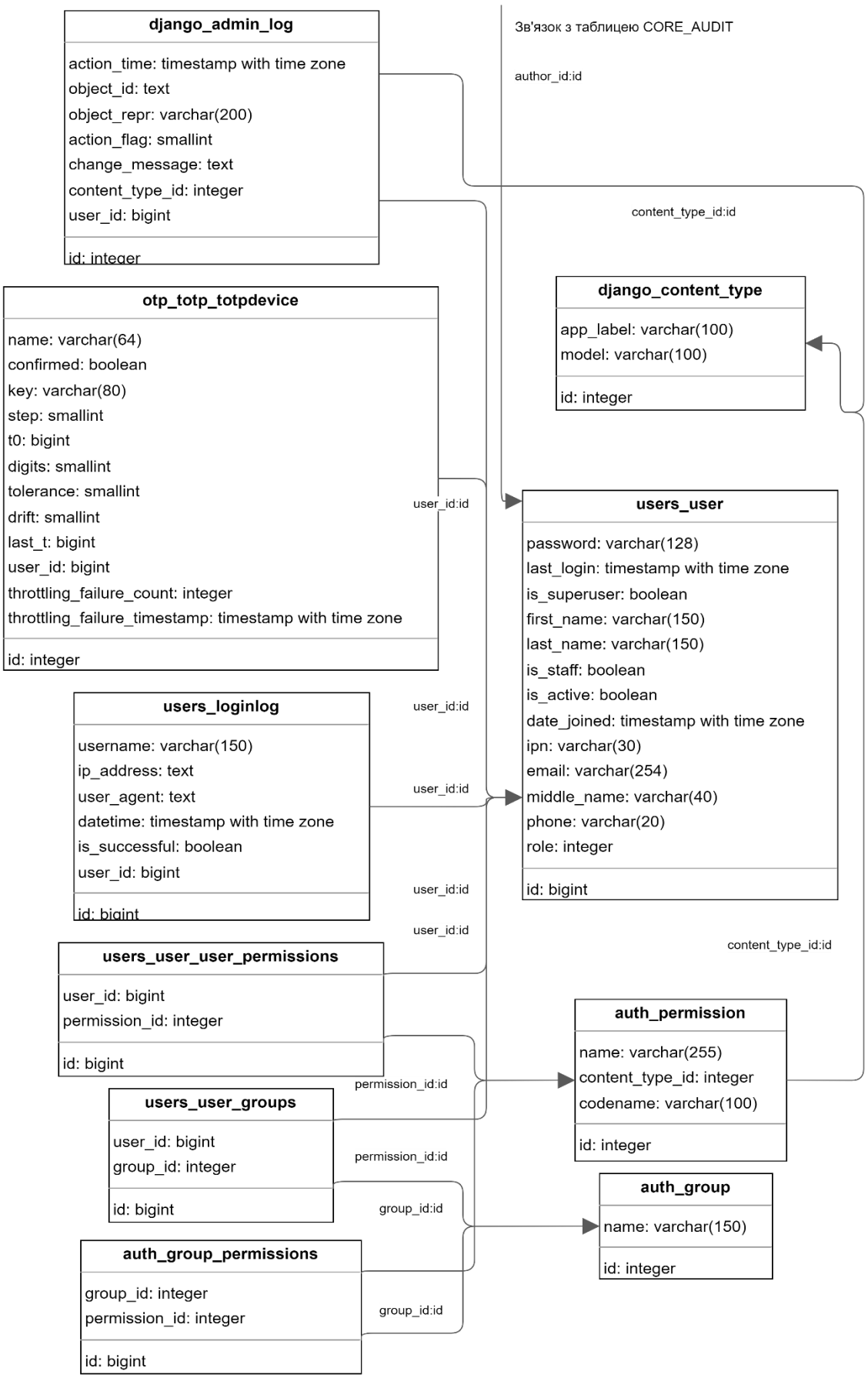


Рисунок 3.2. Схема бази даних, частина 2.

Крім того, розробка програмних модулів забезпечення безпеки має бути постійним процесом, оскільки загрози і вразливості можуть змінюватись з часом. Тому, після впровадження модулів, важливо проводити регулярні оновлення, аналізувати нові загрози та впроваджувати відповідні заходи безпеки.

Розробка програмних модулів забезпечення безпеки інформаційного ресурсу вимагає глибоких знань і експертизи в галузі кібербезпеки, а також знання принципів розробки програмного забезпечення. Тому, важливою складовою розробки програмних модулів забезпечення безпеки є співпраця з експертами з безпеки, включаючи команду аналітиків, етичних хакерів та інших фахівців з кібербезпеки, щоб отримати додаткову перевірку і освітлення вразливостей і ризиків або мати в команді професіоналів, які володіють відповідними навичками і досвідом.

Всі ці кроки, поєднані разом, допоможуть забезпечити надійний і ефективний захист інформаційного ресурсу, а також зменшити ризик його порушення. Розробка програмного забезпечення забезпечення безпеки є постійним і розвиваючимся процесом, який потребує постійного вдосконалення та адаптації до сучасних загроз і вимог безпеки.

Розроблено додатковий захист, який протидіє такому явищу, як намагання інсайдером виконати несанкціонованої модифікації даних у базі даних внаслідок можливості прямого доступу до неї (в обхід передбаченого ресурсом інтерфейсу).

У всіх основних таблицях до їх записів додано поле CRC, яке представляє собою контрольну суму всіх інших полів цього запису і вираховується як швидкий хеш фіксованої довжини за допомогою стандартної бібліотеки Python. Якщо значення будь якого поля запису зазнає несанкціонованих змін, контрольна сума вже не співпаде і цей модифікований запис буде виявлено при перевірці.

Система складається з таких частин:

1. Модуль управління користувачами і їх ролями, забезпечує процес аутентифікації користувача при вході в систему (логін і пароль) та підтвердження другого фактору, а, також, первинне налаштування другого фактору для нового

користувача. Забезпечує управлінням доступами користувачів до окремих таблиць чи дій в залежності від їх ролей, членства в групах або особистих дозволів.

2. Модуль управління даними фінансових установ і їх об’єктів критичної інфраструктури, забезпечення наявності операцій CRUD (create read update delete, 4 основні функції управління даними «створення», «читання», «оновлення» і «вилучення») для додаванням інформації і її збереженням в БД, а, також, формування і відображення звітів.

3. Модуль управління даними довідників (CRUD), таких як категорії критичності, області, міста та інші.

3.5 Системний аналіз безпеки фінансової інфраструктури регіону на основі реалізованих програмних засобів

При вході на сайт необхідно автентифікуватись (рис.3.3):

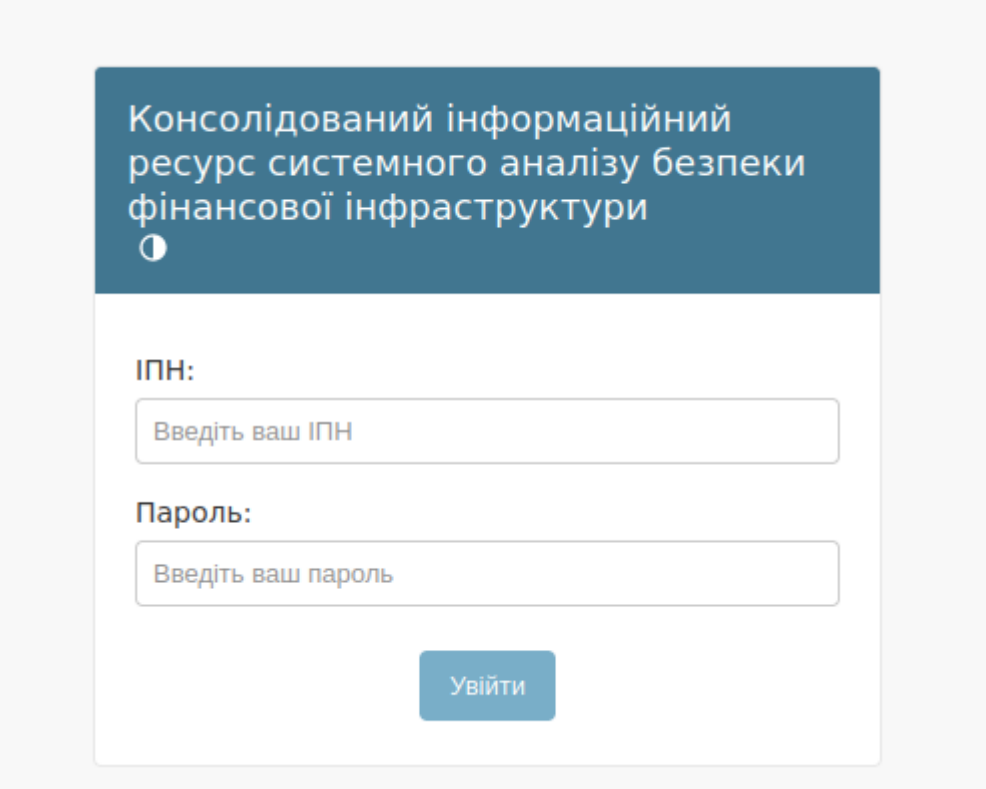


Рисунок 3.3. Вікно введення логіна (ІПН) і пароля.

Якщо користувач заходить вперше, йому буде запропоновано створити пристрій другого фактору (рис.3.4):

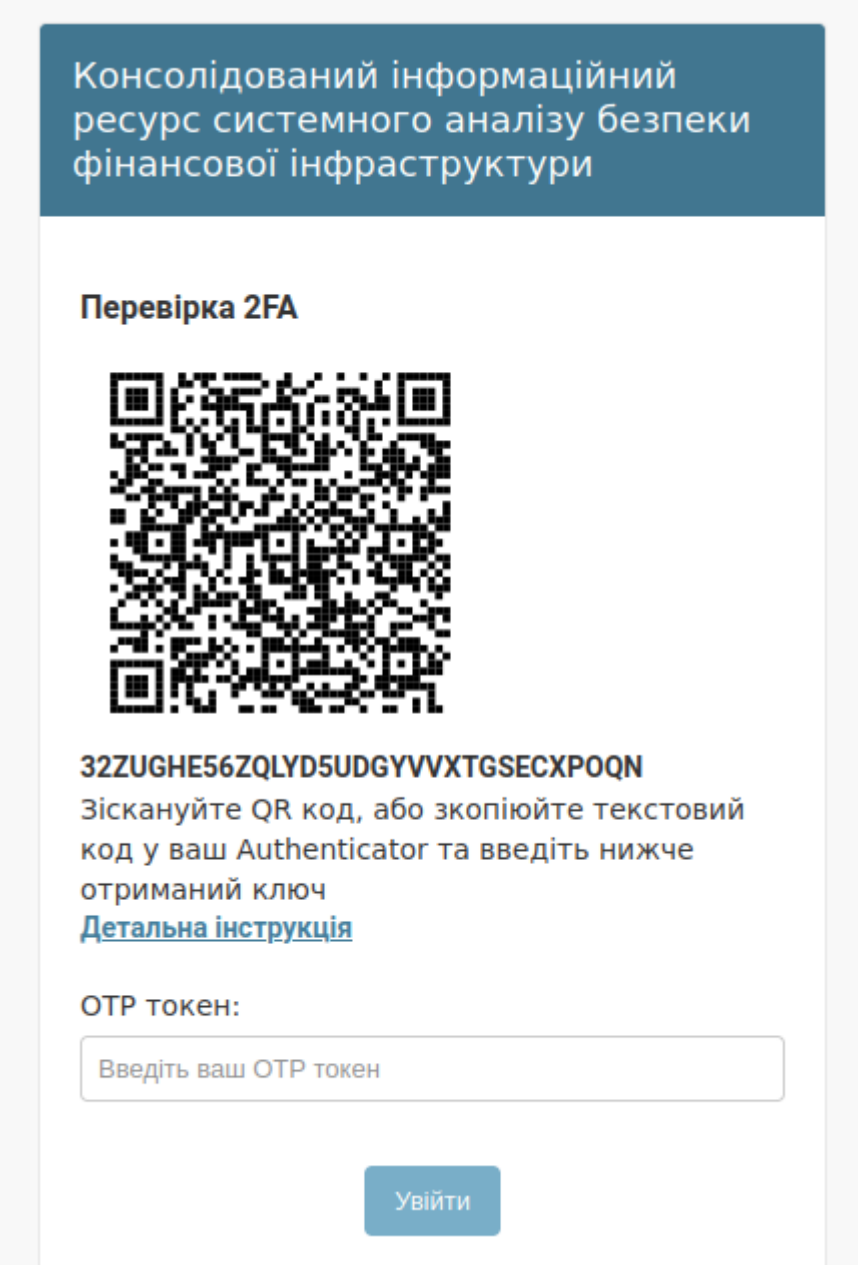


Рисунок 3.4. Вікно створення пристрою другого фактору.

Після налаштувань 2FA і введення відповідного коду користувач автоматично переводиться на головне вікно свого кабінету.

При наступних входах у систему вікна налаштувань 2FA не буде, користувач після логіна/пароля в наступному вікні буде вводити код зі свого пристрою.

Якщо пристрій 2FA втрачено, адміністратор може видалити його із таблиці пристроїв, і тоді користувач зможе зайти як в перший раз і створити новий пристрій 2FA.

Для роботи адміністратора і аналітика побудований зручний інтерфейс, заснований на таблицях, що дозволяє легко фільтрувати записи за вибраним критерієм, сортувати дані у таблиці по стовпцям, виконувати текстовий пошук в записах таблиці, робити передбачені дії як над одним записом таблиці, так і над групою обраних. Кожен користувач має свій кабінет і бачить в ньому тільки ті таблиці, які йому дозволено доступом.

Головна сторінка адміністратора (рис. 3.5).

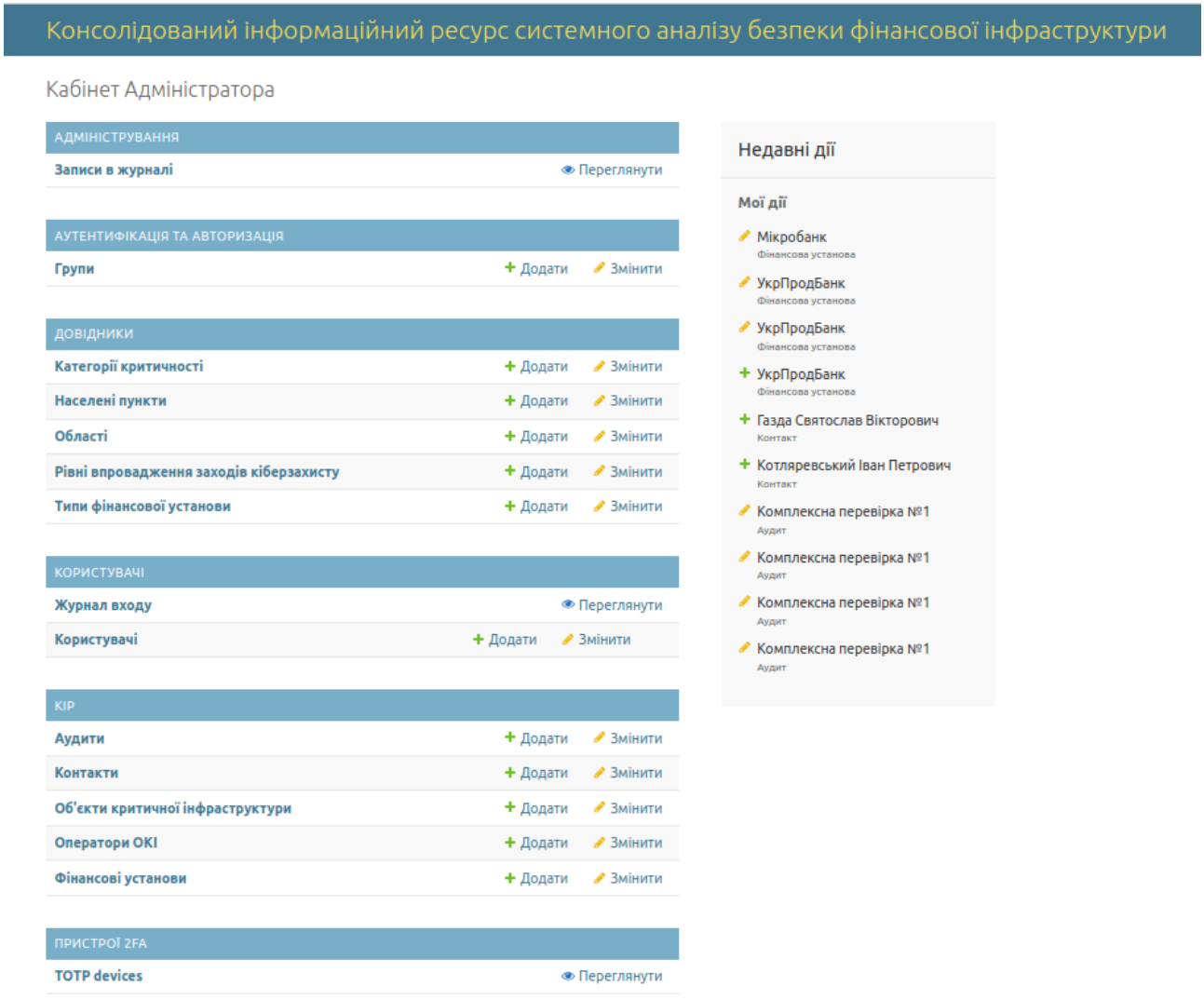


Рисунок 3.5. Головна сторінка адміністратора ресурсу

Користувачі інших ролей зможуть бачити тільки ті таблиці, на які є дозвіл. Головна сторінка кабінету Аналітика має такий вигляд (рис. 3.6):

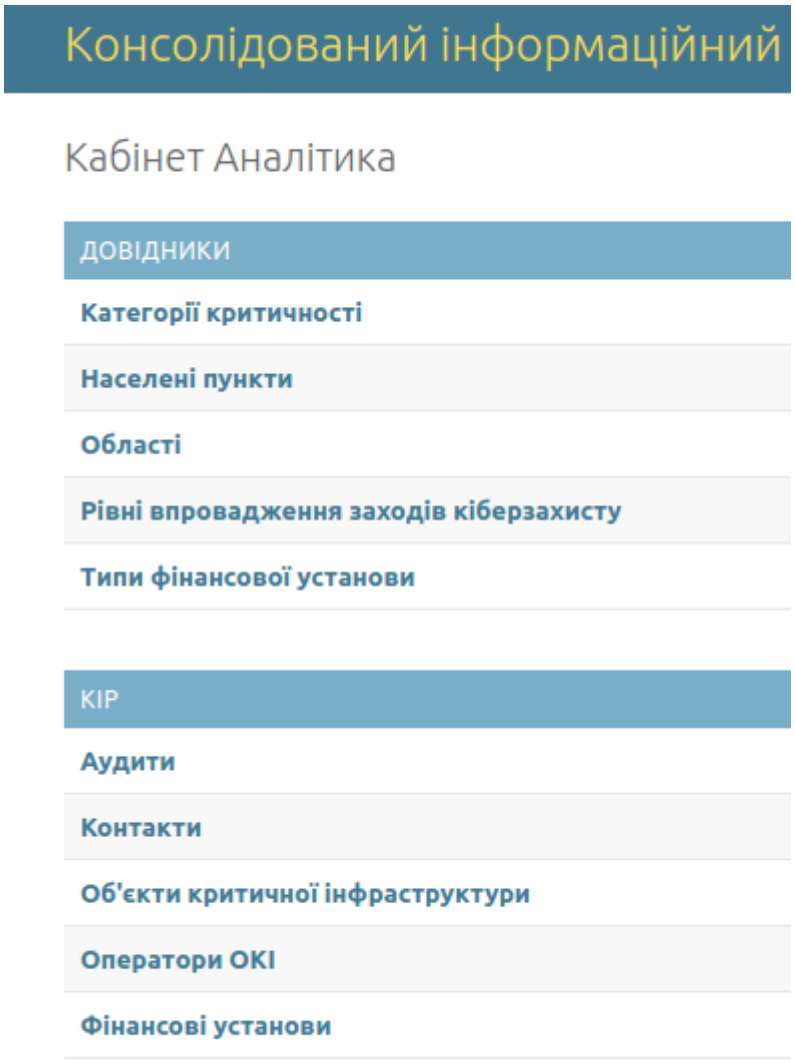


Рисунок 3.6. Головна сторінка кабінету Аналітика

У кожному кабінеті праворуч зверху розташовані елементи керування, які дозволяють користувачу змінити пароль, вийти із системи і перемикнути сайт на темну тему (рис.3.7):

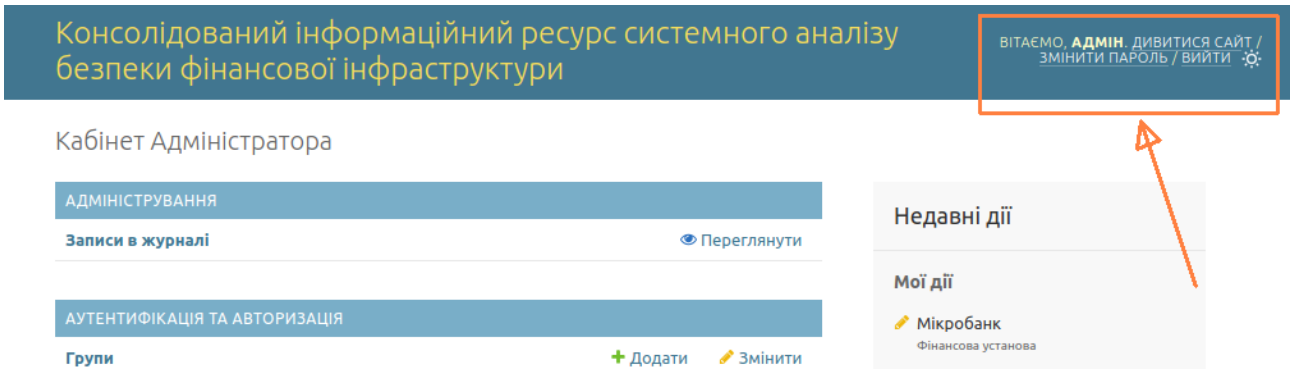


Рисунок 3.7. Елементи управління

Вигляд таблиці «Фінансові установи» (рис 3.8):

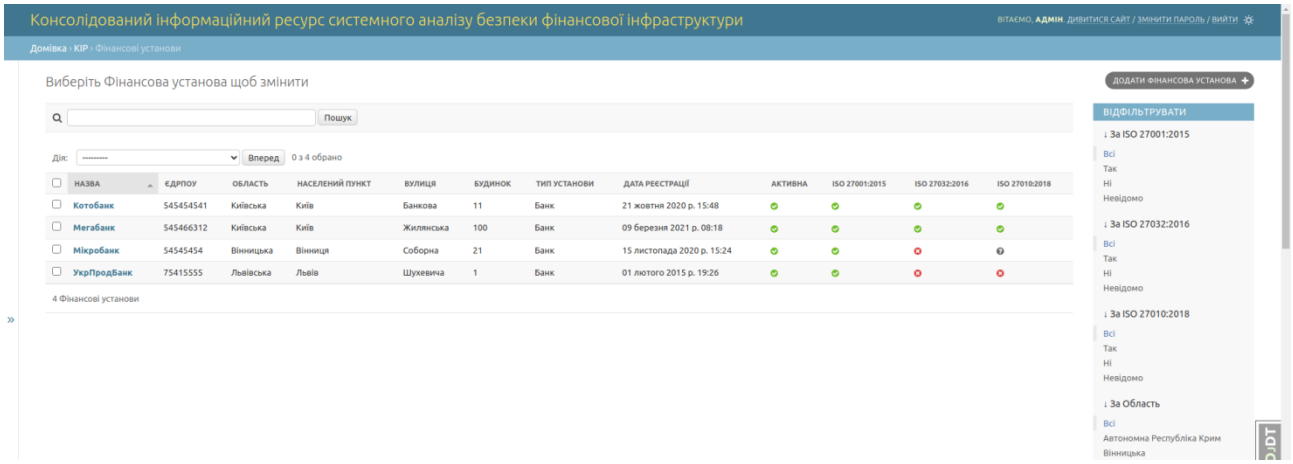


Рисунок 3.8. Фінансові установи

При редагуванні запису для зручності доступні віджети «Спадаючий список», «Дата і час» (рис.3.9):

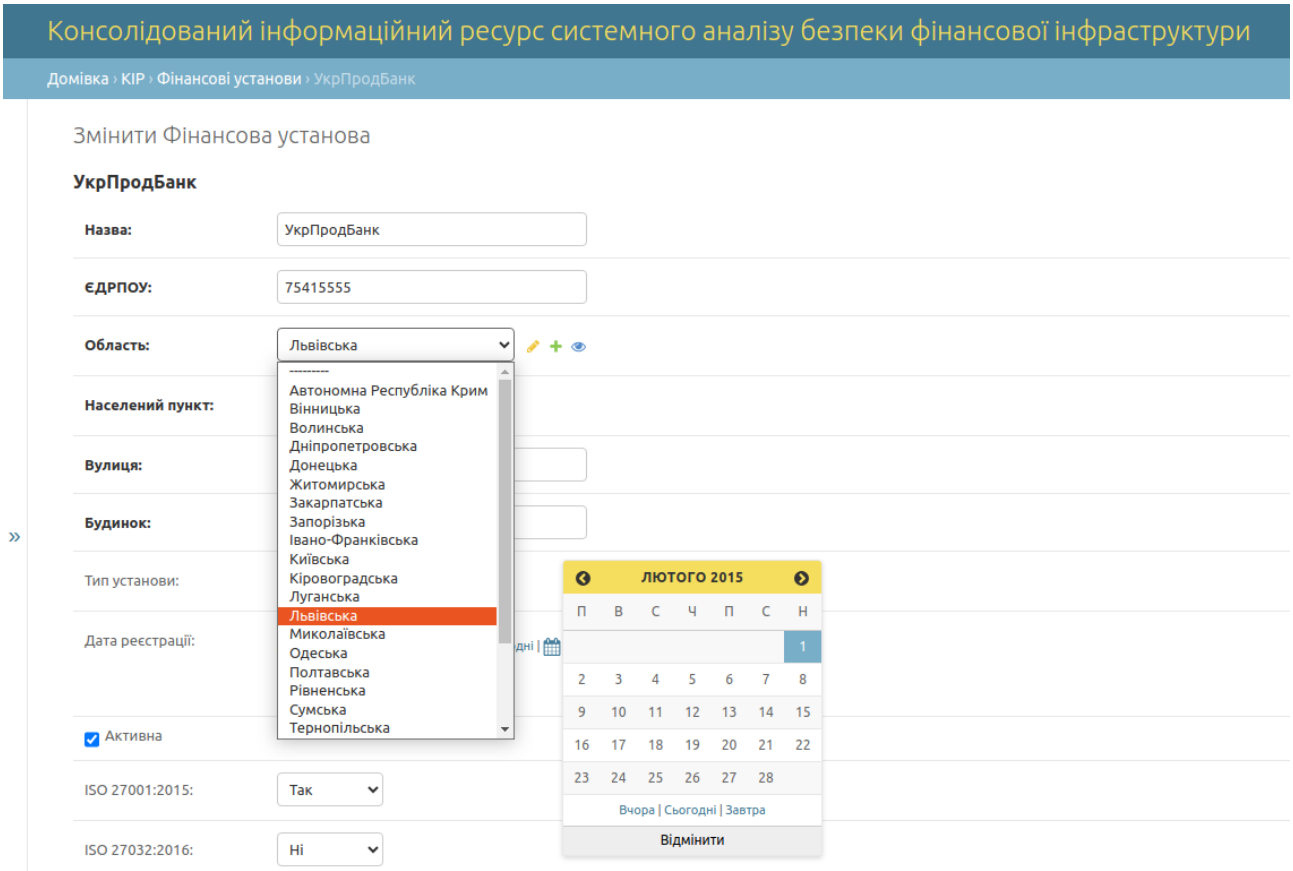


Рисунок 3.9. Редагування запису фінансової установи

Для зручності заповнення додана можливість створення елементів вибору в модальних вікнах, не покидаючи основне вікно, щоб не переходити кожного разу до відповідних таблиць Оператори і Контакти для створення відповідних записів (рис.3.10):

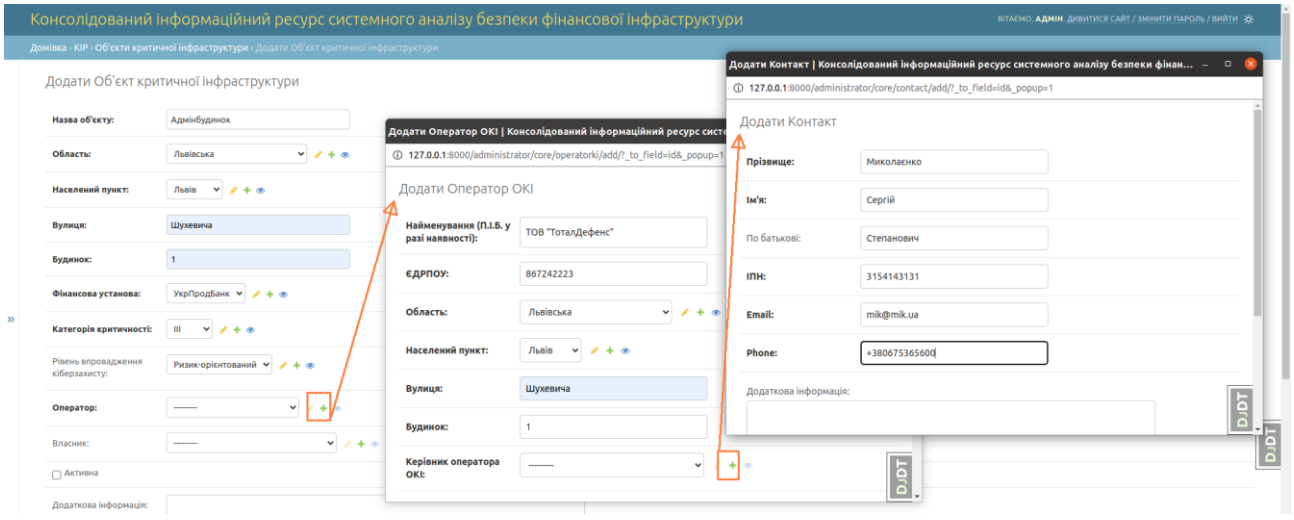


Рисунок 3.10. Редагування запису фінансової установи

Якщо користувач не заповнив обов’язкові поля форми і намагається зберегти запис, то форма надасть йому відповідне повідомлення з вказанням місця помилки (рис.3.11):

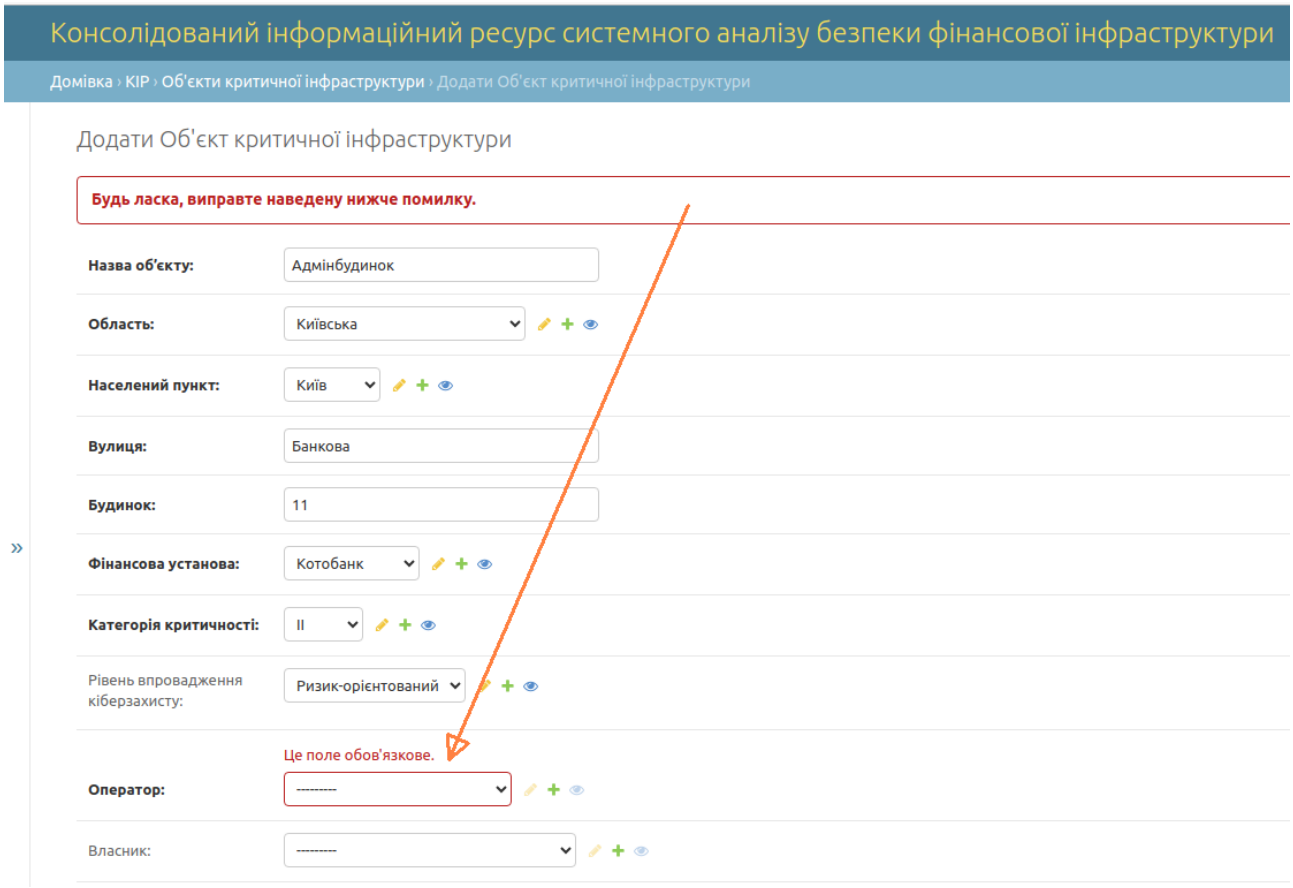


Рисунок 3.11. Повідомлення форми про помилку

В результаті операцій створення, збереження або видалення запису, користувачу надсилається відповідне повідомлення статусу операції (рис.3.12):

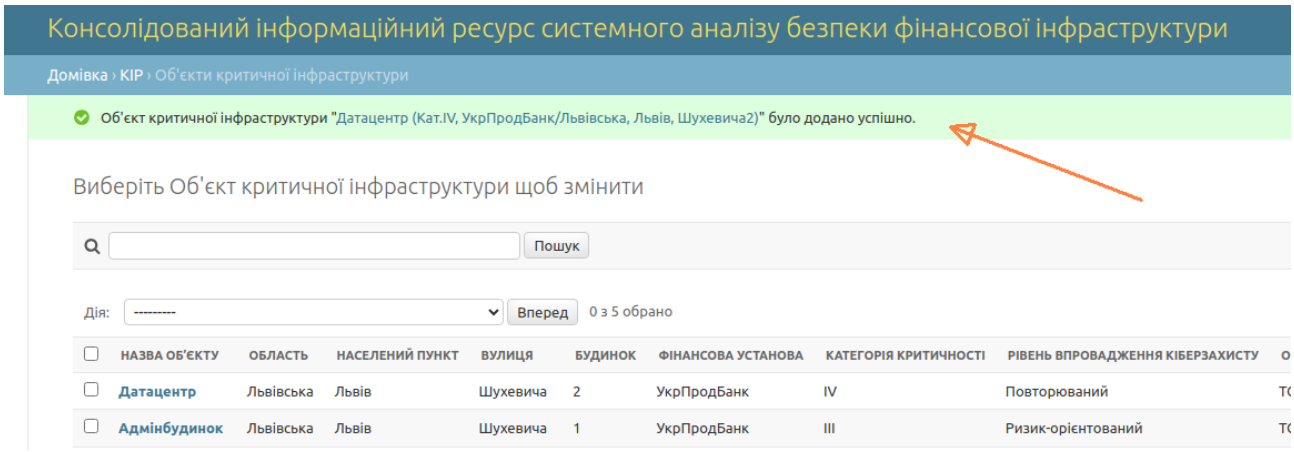


Рисунок 3.12. Повідомлення статусу операції

Підтримка двоспрямованого сортування записів у таблиці за вказаним стовпцем (рис.3.13):

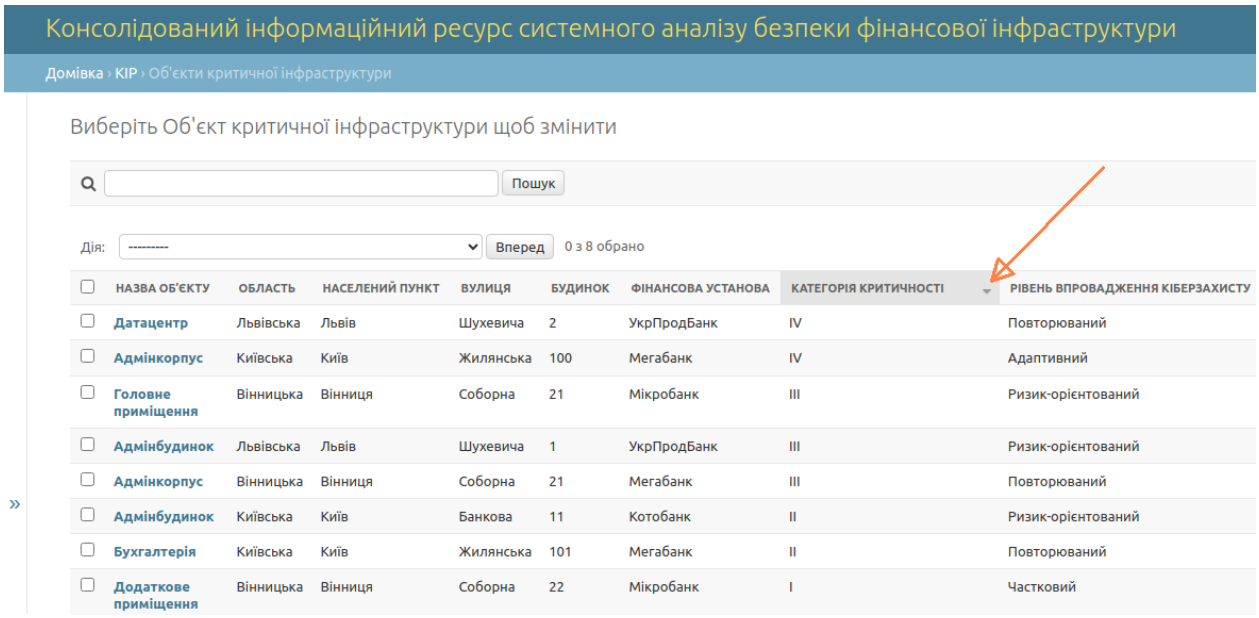


Рисунок 3.13. Підтримка двоспрямованого сортування

Аналітик створює новий Аудит і заповнює форму оцінювання стану систем об’єкту критичної інфраструктури (рис.3.14):

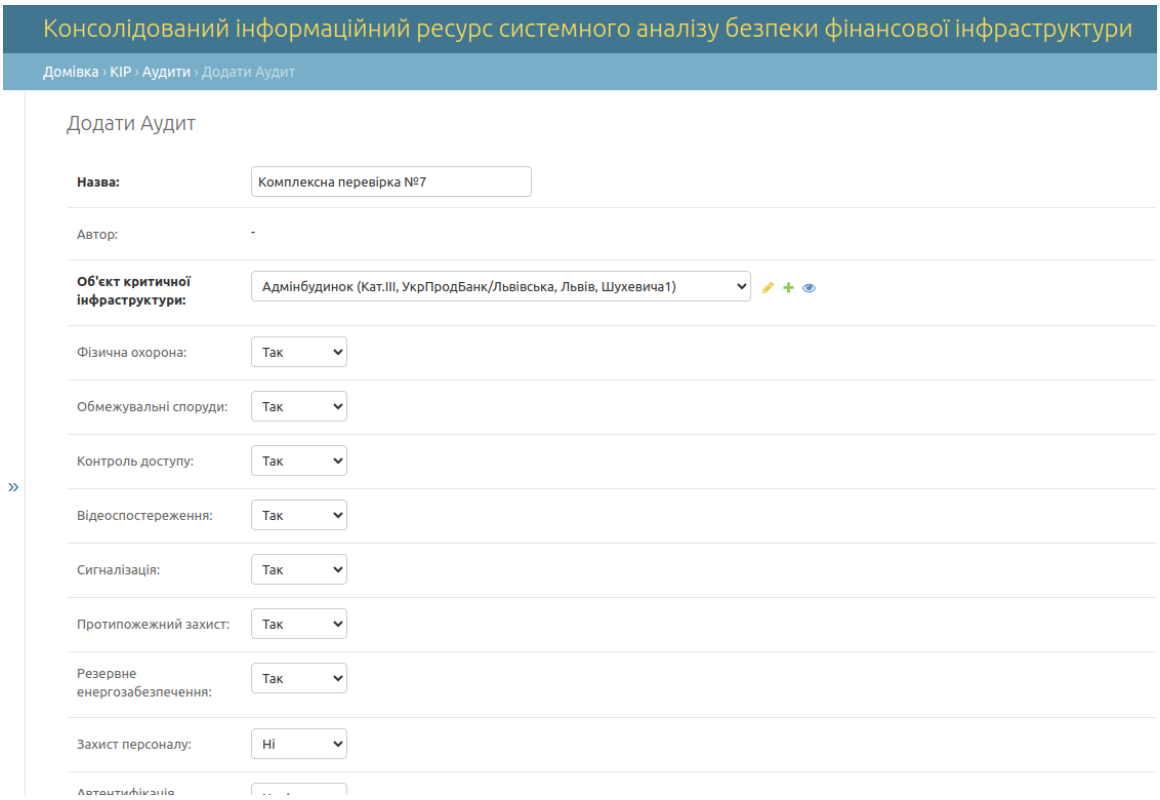


Рисунок 3.14. Створення Аудиту

Створені такі звіти за різними критеріями (рис.3.15-3.):

Рисунок 3.15. Рейтинг об’єктів за категоріями критичності

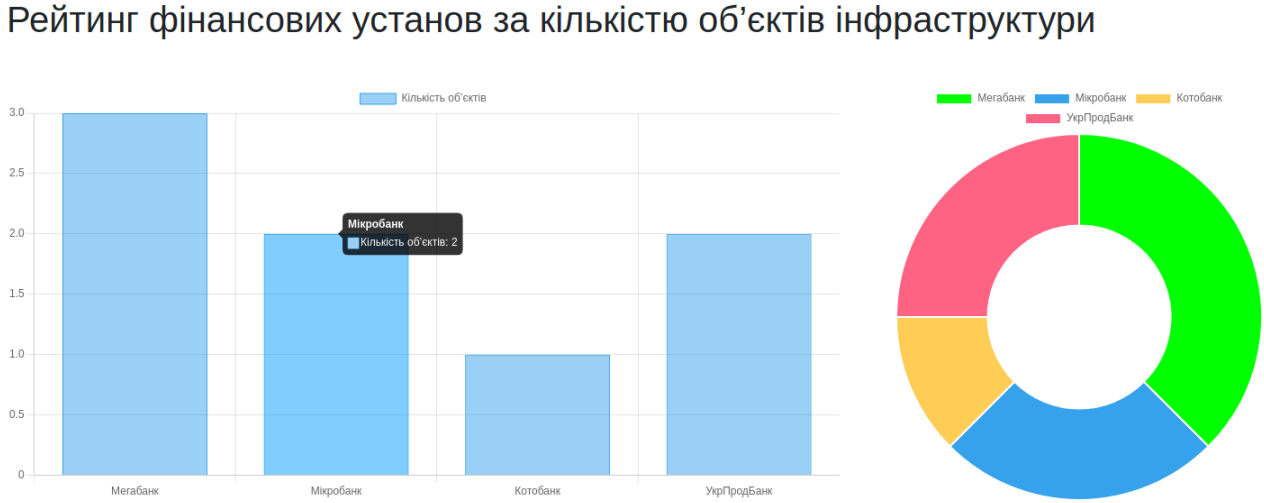


Рисунок 3.16. Рейтинг фінансових установ за кількістю об’єктів

Рисунок 3.17. Рейтинг областей за кількістю об’єктів

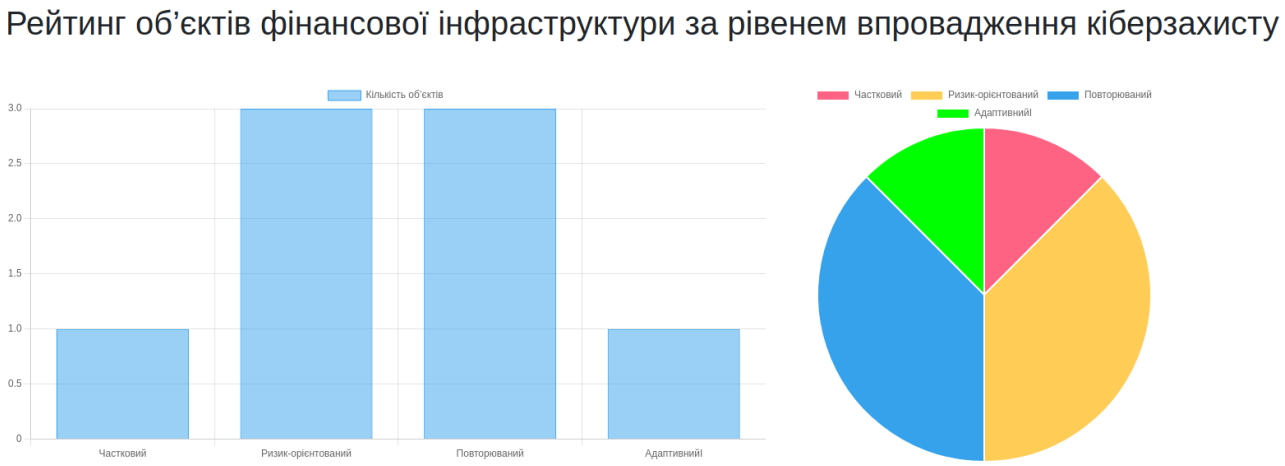


Рисунок 3.18. Рейтинг об’єктів фінансової інфраструктури за рівнем впровадження кіберзахисту

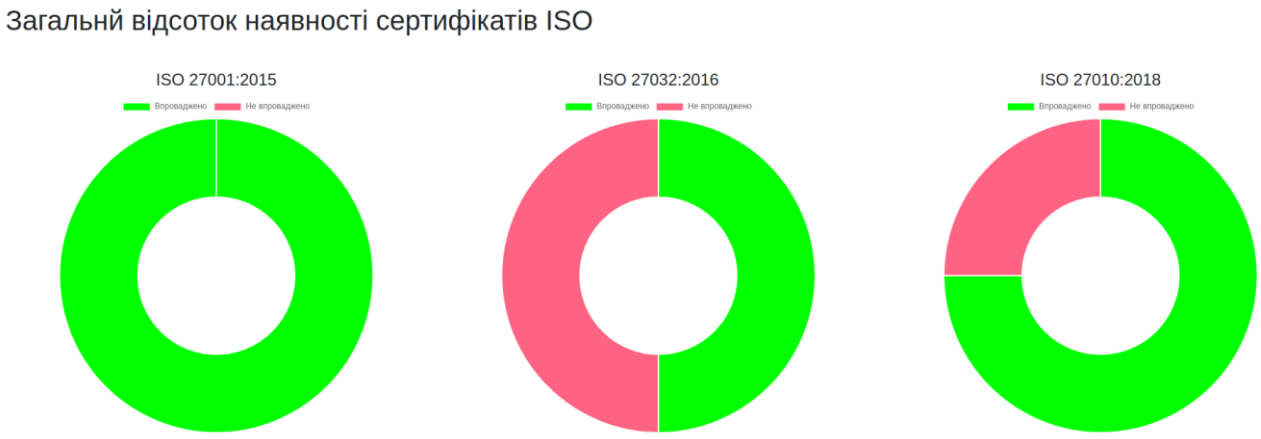


Рисунок 3.19. Загальний відсоток наявності сертифікатів ISO

Рисунок 3.20. Динаміка безпеки об'єкту за результатами його аудитів

3.6 Висновки до розділу

У цьому розділі було розроблено систему керування консолідованим інформаційним ресурсом аналізу безпеки фінансової інфраструктури регіону.

Також, реалізовано функціонал CRUD, тобто чотири основні функції управління даними «створення, читання, оновлення і вилучення» до кожної відповідної таблиці бази даних.

Також створено таблиці та бази даних, на основі якої був реалізовано управління користувачами ресурсу.

Створено звіти для підвищення ефективності роботи та подальшого аналізу.

Дослідження показало, що консолідований інформаційний ресурс був успішно реалізований. Цей ресурс забезпечує збір, обробку і представлення інформації з різних джерел в одному місці.

Це дозволяє виконувати швидкий доступ до різноманітних даних, що сприяє полегшенню прийняття рішень та підтримці аналітичної роботи.

Консолідований інформаційний ресурс допомагає уникнути дублювання даних і забезпечує їх єдиний джерело правди. Це дозволяє забезпечити доступ до актуальних і точних даних для всіх користувачів.

Також виявлено, що цей ресурс зменшує витрати на обробку і зберігання даних, оскільки дозволяє зберігати усю інформацію в одному місці замість багатьох різних систем і здійснювати консолідацію даних.

Отже, реалізація консолідованого інформаційного ресурсу є вигідною і ефективною стратегією для організацій, які потребують забезпечення швидкого та точного доступу до даних.

Консолідований інформаційний ресурс сприяє полегшенню співпраці та обміну даними і дозволяє забезпечити єдиний доступ до даних для усіх користувачів, незалежно від їхньої локації чи функціональних обов’язків. Це полегшує комунікацію та співпрацю між різними користувачами ресурсу та забезпечує більше єднання у роботі.

Крім того, консолідований інформаційний ресурс також допомагає забезпечити безпеку даних. Збереження усієї інформації в одній системі дозволяє зручно керувати правами доступу різних користувачів. Це зменшує ризик втрати чи несанкціонованого доступу до даних та забезпечує дотримання стандартів безпеки.

Нарешті, консолідований інформаційний ресурс може сприяти покращенню ефективності та продуктивності роботи. Швидкий доступ до інформації, її легка обробка та аналіз дозволяють користувачам швидше приймати рішення та виконувати свої завдання.

Висновки з дослідження показують, що реалізація консолідованого інформаційного ресурсу виявляється ефективним та вигідним рішенням для аналізу безпеки критичних об’єктів фінансової установи. Він сприяє максимальному використанню та оптимізації різноманітності даних, забезпечує полегшення співпраці та забезпечує безпеку даних, що, у свою чергу, приводить до покращення ефективності та продуктивності роботи і прийнятті кращих управлінських рішень.

РОЗДІЛ IV. ЕКОНОМІЧНА ЧАСТИНА

Економічна частина науково-дослідної розробки є важливою складовою процесу створення нового продукту або технології.

Головною метою економічної частини науково-дослідної розробки є оцінка комерційного потенціалу проекту. Це означає вивчення економічних аспектів розробки таких як ринкові можливості і аналіз конкуренції, вартість розробки та впровадження, оцінка потенційних доходів та витрат, прогнозування точок беззбитковості та рентабельності та інші фактори, які впливають на успіх проекту. Врахування економічних аспектів також дозволяє розробити стратегію його впровадження на ринку, що є важливою складовою успіху .

Магістерська кваліфікаційна робота за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок, тобто коли відбувається комерціалізація науково-технічної розробки. Оскільки результатами розробки можуть користуватися інші споживачі, отримуючи при цьому певний економічний ефект, напрямок є пріоритетним. Для цього необхідно знайти потенційного інвестора і переконати його в економічній доцільності реалізації цього проекту.

Необхідно виконати наступні етапи робіт:

1. Проведення комерційного аудиту науково-технічної розробки, а саме, встановлення її науково-технічного рівня та комерційного потенціалу.

2. Розрахунок витрат для здійснення науково-технічної розробки.

3. Розрахунок економічної ефективності науково-технічної розробки і провести обґрунтування економічної доцільності комерціалізації потенційним інвесторам.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Рекомендується здійснювати оцінювання науково-технічного рівня розробки та її комерційного потенціалу із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними у табл. 4.1 [52].

Таблиця 4.1.

Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка:

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних умовах
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі влас-тивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів

Продовження табл. 4.1

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуютьс я у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь- які регламентні обмеження на виробництво та реалізацію продукту

Дані результатів оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно внести до таблиці.

Таблиця 4.2. Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	4	4	4
2. Ринкові переваги (наявність аналогів)	4	4	4
3. Ринкові переваги (ціна продукту)	4	3	4
4. Ринкові переваги (технічні властивості)	4	4	4
5. Ринкові переваги (експлуатаційні витрати)	3	3	3
6. Ринкові перспективи (розмір ринку)	4	4	3
7. Ринкові перспективи (конкуренція)	4	4	4
8. Практична здійсненність (наявність фахівців)	3	4	4
9. Практична здійсненність (наявність фінансів)	3	4	4
10. Практична здійсненність (необхідність нових матеріалів)	4	4	4
11. Практична здійсненність (термін реалізації)	4	4	4
12. Практична здійсненність (розробка документів)	3	3	3
Сума балів	44	45	45
Середньоарифметична сума балів $СБ_c$	44,6		

Зробимо висновки щодо науково-технічного рівня і рівня комерційного потенціалу розробки за результатами розрахунків, наведених в таблиці 4.2, і використаємо рекомендації, наведені в табл. 4.3 [52].

Таблиця 4.3. Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» становить 44,6 бала, і відповідно до таблиці 4.3, свідчить про комерційну важливість проведення даних досліджень, тобто рівень комерційного потенціалу розробки високий.

4.2 Оцінювання рівня новизни розробки

Оцінювання рівня новизни розробки є важливим етапом у процесі розробки будь-якого продукту чи послуги. Це визначає наскільки унікальним та інноваційним є розроблений продукт відносно вже існуючих рішень на ринку.

Новизна виражається в здатності розробки вирішити певну проблему або виконати конкретну функцію, що є відсутньою у наявних продуктах. Оцінка новизни допомагає визначити потенціал ринкового успіху продукту, його конкурентні переваги та можливість проникнення на нові ринки. Тому необхідне проведення визначення рівня новизни розробки, отриманої в результаті досліджень за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону».

Найбільш актуальним є визначення рівня і ступеня інтегральної новизни, оскільки її рівень визначає ступінь однакового позитивного сприйняття новизни розробки як виробником, так і споживачем, а отже і ринком в цілому, а це, у свою чергу, є гарантією того, що новинка знайде своє місце на ринку,

користуватиметься попитом у споживачів і забезпечить відшкодування витрат, зазнаних виробником під час розроблення та виробництва [53].

Рівень новизни нового продукту розраховується експертним методом шляхом протиставлення нового продукту та його аналогів, що присутні в даний час на ринку, з використанням чинників, що визначають її значення, за системою «краще-гірше». Рівень новизни встановлюється відносно рівня аналога, або досить близького до аналога продукту.

Для визначення *i*-го виду новизни застосовуються чинники, які впливають на її рівень. Кожен чинник *i*-го виду новизни розраховується в балах - чим більша кількість набраних балів, тим більший рівень новизни. Для оцінювання рівня новизни використаємо експертів, які встановлюють бали відповідним чинникам. Бал відповідності вноситься в діапазоні від -5 (значно гірше аналога) до +5 (значно краще аналога). Результати оцінювання науково-технічного рівня та комерційного потенціалу розробки зведемо до відповідного листа оцінювання рівня новизни експертами (таблиця 4.4).

Таблиця 4.4. Лист оцінювання рівня новизни експертами

Види та чинники		Бали та експерти		
		Експерт 1	Експерт 2	Експерт 3
1		*2*	*3*	*4*
Споживча новизна	Питома вага 0,225	Максимальний бал $Б_{i\ MAX}$		25
1. Зміна поведінкових звичок споживача		5	5	4
2. Ступінь задоволення потреб і запитів		5	4	4
3. Спосіб задоволення потреби		3	3	4
4. Формування нової потреби		1	1	2
5. Формування нового споживача		0	0	0
Середній бал експертів $Б_{i\ отр}$		14		

Продовження таблиці 4.4

1		*2*	*3*	*4*
Товарна новизна	Питома вага 0,217	Максимальний бал $Б_{i\ MAX}$		30
1. Параметричні зміни показників продукції				
1.1. Якісні		3	4	3
1.2. Технічні		4	4	3
1.3. Економічні		3	3	3
1.4. Сервісні		4	4	4
2. Якість продукції по відношенню до конкурентів		3	3	3
3. Функціональні зміни		3	3	3
Середній бал експертів $Б_{i\ отр}$		20		
Виробнича новизна	Питома вага 0,042	Максимальний бал $Б_{i\ MAX}$		25
1. Рівень унікальності товару для підприємства		5	5	5
2. Рівень унікальності для галузі		3	4	3
3. Рівень унікальності товару для країни		1	1	1
4. Зміна виробничої системи		4	4	4
5. Відносно існуючого асортименту		2	2	2
Середній бал експертів $Б_{i\ отр}$		15		
Прогресивна новизна	Питома вага 0,179	Максимальний бал $Б_{i\ MAX}$		25
1. Зміна технології виготовлення		4	4	4
2. Рівень застосування нових компонентів і матеріалів		1	2	1
3. Зміна технологічного принципу дії виробу		1	2	1
4. Зміна конструктивного виконання		3	2	3
5. Рівень застосування інновацій		2	2	2
Середній бал експертів $Б_{i\ отр}$		11		

Продовження таблиці 4.4

1		*2*	*3*	*4*
Ринкова новизна	Питома вага 0,12	Максимальний бал $Б_{i\ MAX}$		20
1. Новий виріб на новому ринку		0	0	0
2. Новий виріб на відомому ринку		2	2	2
3. Модернізований виріб		2	2	2
4. Нова модель		1	2	2
Середній бал експертів $Б_{i\ отр}$		6		
Екологічна новизна	Питома вага 0,035	Максимальний бал $Б_{i\ MAX}$		20
1. Рівень екологічної чистоти технології виробництва		5	5	5
2. Рівень впровадження мало- та безвідходних технологій		5	5	5
3. Рівень екологічно небезпечних режимів експлуатації продукції		5	5	5
4. Рівень забруднення навколишнього середовища		5	5	5
Середній бал експертів $Б_{i\ отр}$		20		
Соціальна новизна	Питома вага 0,036	Максимальний бал $Б_{i\ MAX}$		20
1. Використання нового товару приводить до покращення стану здоров’я нації		0	0	0
2. Використання нового товару приводить до зростання доходів населення		0	0	0
3. Виробництво нового товару приводить до збільшення (зменшення) кількості робочих місць на підприємстві		4	5	4
4. Виробництво нового товару приводить до підвищення кваліфікації персоналу		3	3	3
Середній бал експертів $Б_{i\ отр}$		7		

Продовження таблиці 4.4

1		*2*	*3*	*4*
Маркетингова новизна	Питома вага 0,146	Максимальний бал $Б_{i\,MAX}$		20
1. Нові методи маркетингових досліджень		0	0	0
2. Вживання нових стратегій сегментації ринку		3	3	3
3. Вибір нової маркетингової стратегії обхвату і розвитку цільового сегмента		2	3	2
4. Побудова нових каналів збуту		2	2	2
Середній бал експертів $Б_{i\,отр}$		7		

Значення *i*-го виду новизни розраховується за формулою [53]:

$$I_i = \frac{Б_{i\,отр}}{Б_{i\,MAX}}, \tag{4.1}$$

де $Б_{i\,отр}$ – отримана кількість балів за шкалою оцінок чинників, що визначають *i*-й вид новизни;

$Б_{i\,MAX}$ – максимальна кількість балів, що може бути отримана за *i*-м видом новизни.

Загальний рівень інтегральної новизни розраховується як додаток отриманого значення *i*-го виду новизни і її вагомості. Вагомість *i*-го виду новизни визначаємо експертним методом, за формулою [53]:

$$N_{інт} = \sum_{i}^{n} W_i \cdot I_i, \tag{4.2}$$

де $N_{інт}$ – рівень інтегральної (сукупної) новизни;

W_i – вагомість (питома вага) *i*-го виду новизни;

n – загальна кількість видів новизни.

$$N_{інт} = (0,225 \cdot 14/25)+(0,217 \cdot 20/30)+(0,042 \cdot 15/25)+(0,179 \cdot 11/25)+(0,12 \cdot 6/20)+$$
$$(0,035 \cdot 20/20)+(0,036 \cdot 7/20)+(0,146 \cdot 7/20) = 0,516.$$

Отримане значення інтегрального рівня новизни зіставляємо зі шкалою, що наведена в табл. 4.5 [53].

Таблиця 4.5. Рівні новизни нового товару та їхня характеристика

Рівні новизни товару	Значення інтег-ральної новизни	Характеристика товару	Вид нового товару
Найвища	1,00	Абсолютно новий товар	Новий товар, що наділений ознаками інноваційності (інноваційний товар)
Висока	0,8…0,99	Товар, який не має аналогів	
Значуща	0,6…0,79	Принципова зміна споживчих властивостей товару	
Достатня	0,4…0,59	Принципова технологічна модифікація товару	
Незначна	0,2…0,39	Кардинальна зміна параметрів	Новий товар
Помилкова	0,00…0,19	Малоістотна модифікація	

Відповідно до таблиці 4.5, отримане значення інтегральної новизни: 0,516. Це показує, що розробка відповідає таким рівням:

– рівень новизни товару – достатня новизна;

– характеристика – принципова технологічна модифікація товару;

– вид розробки – новий товар, що наділений ознаками інноваційності (інноваційний товар).

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Згрупуємо за відповідними статтями витрати, які пов'язані з проведенням науково-дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» під час планування, обліку і калькулювання собівартості.

4.3.1 Витрати на оплату праці

До статті «Витрати на оплату праці» відносяться витрати на виплату основної та додаткової заробітної плати працівникам, які безпосередньо приймають участь у виконанні конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці. Такими працівникам можуть бути керівники відділів, наукові, інженерно-технічні працівники, конструктори, технологи, лаборанти, а, також інші працівники, які не дослідниками.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуються у відповідності до посадових окладів працівників, за формулою [52]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.3)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дні;

T_p – середнє число робочих днів в місяці, T_p=24 дні.

$$З_о = 19000{,}00 \cdot 60 / 24 = 47500{,}00 \text{ грн.}$$

Проведені розрахунки вносяться до таблиці 4.6.

Таблиця 4.6. Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	19000	791,67	60	47500
Інженер-розробник програмного забезпечення	16500	687,5	56	38500
Науковий співробітник дослідження проблем програмного забезпечення	13000	541,67	10	5416,67
Всього				91416,67

Основна заробітна плата робітників.

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» розраховується за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \,, \tag{4.4}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \,, \tag{4.5}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду [52];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 24 дні;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700,00 \cdot 1,10 \cdot 1,65 / (24 \cdot 8) = 63,34$ грн.

$З_{р1} = 63,34 \cdot 6,00 = 380,02$ грн.

Таблиця 4.7. Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Установка електронно-обчислювального обладнання	6	2	1,1	63,34	380,02
Підготовка робочого місця дослідника	2,4	2	1,1	63,34	152,01
Інсталяція програмного забезпечення	2,2	5	1,7	97,88	215,34
Всього					747,36

Додаткова заробітна плата дослідників та робітників.

Додаткова заробітна плата розраховується як 10-12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.6)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймаємо 10%.

$З_{дод}$ = (91416,67+ 747,36) · 10 / 100% = 9216,40 грн.

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховується як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.7)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = ((91416,67+ 747,36+ 9216,40) · 22 / 100% = 22303,69 грн.

4.3.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону».

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj}, \quad (4.8)$$

де $Н_j$ – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 ... 1,15*);

$В_j$ – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$М_1 = 2,00 \cdot 200,00 \cdot 1,1 - 0,000 \cdot 0,00 = 440,0$ грн.

Проведені розрахунки зведемо до таблиці 4.8.

Таблиця 4.8. Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за од, грн	Норма витрат, од	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Офісний папір, уп	200	2	0	0	440
Папір для записів, уп	110	1	0	0	121
Органайзер офісний,шт	210	2	0	0	462
Канцелярське приладдя (набір офісного працівника), шт	175	2	0	0	385
Картридж для принтера	1100	1	0	0	1210
Диск оптичний CD-RW	15	3	0	0	49,5
Flesh-пам'ять 16 GB	130	1	0	0	143
Тека для паперів	82	2	0	0	180,4
Всього					3490,63

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» відсутні.

4.3.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування, яке необхідне для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування та встановлення. В дослідній роботі «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» витрати на спец устаткування відсутні.

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та, за потреби, придбання спеціальних програмних засобів і програмного забезпечення, які необхідні для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансова вартість програмного забезпечення розраховується за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.9)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 5420,00 \cdot 1 \cdot 1,12 = 6070,4$ *грн.*

Отримані результати вносяться до таблиці 4.9.

Таблиця 4.9. Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
ОС Windows 11	1	5420	6070,4
Прикладний пакет Microsoft Office 2019	1	5230	5857,6
Система розробки PyCharm	1	11100	12432,0
Всього			24360,0

4.3.7 Амортизація обладнання, програмних засобів та приміщень

Для спрощення, амортизаційні відрахування по кожному виду обладнання та програмному забезпеченню, розраховуються з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.10)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (24370{,}00 \cdot 2) / (2 \cdot 12) = 2030{,}83$ *грн.*

Проведені розрахунки вносяться до таблиці 4.10.

Таблиця 4.10. Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Персональний комп'ютер	24370	2	2	2030,83
Робоче місце дослідника	7880	5	2	262,67
Оргтехніка	8675	4	2	361,46
ОС Windows 11	5450	2	2	451,67
Прикладний пакет Microsoft Office 2019	3795	2	2	435,83
Всього				3542,46

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на електричну енергію (B_e) розраховуються за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.11)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 7,50$ грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,3 \cdot 452,0 \cdot 7,50 \cdot 0,95 / 0,97 = 996,03$ *грн.*

Проведені розрахунки вносяться до таблиці 4.11.

Таблиця 4.11. Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Персональний комп’ютер	0,3	452	996,03
Робоче місце дослідника	0,15	452	498,02
Оргтехніка	0,45	10	33,05
Всього			1527,1

4.3.9 Службові відрядження

Службові відрядження є важливим елементом економічної діяльності підприємств та організацій і передбачають виконання певних обов'язків та завдань, пов'язаних з роботою, поза територією постійного місцезнаходження працівника.

До статті «Службові відрядження» дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань, а також витрати на відрядження на наукові конференції, наради, які пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховується як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \qquad (4.12)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$B_{св}$ = (91416,67+ 747,36) · 20 / 100% = 18432,81 грн.

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуються як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.13)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$B_{сп}$ = (91416,67+ 747,36) · 30 / 100% = 27649,21 грн.

4.3.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (91416,67+ 747,36) · 50 / 100% = 46082,01 грн.

4.3.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}\ , \qquad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 120%.

$B_{нзв}$ *= (91416,67+ 747,36) · 120 / 100% = 110596,83 грн.*

Витрати на проведення науково-дослідної роботи на тему «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}\,. \qquad (4.17)$$

$B_{заг}$*=91416,67+747,36+9216,40+22303,69+3490,63+0,00+0,0+24360+3542,46+*
+1527,10+18432,81+27649,21+46082,01+110596,83= 359365,17 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \qquad (4.16)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,9.

ЗВ = 359365,17/ 0,9 = 399294,63 грн.

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

ΔN – збільшення кількості споживачів продукту, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, проектних груп	500	700	800	500

N – кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки, приймемо 100 проектних груп;

$Ц_б$ – вартість програмного продукту у році до впровадження результатів розробки, приймемо 20000,00 грн;

$\pm\Delta Ц_о$ – зміна вартості програмного продукту від впровадження результатів науково-технічної розробки, приймемо 1000,00 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [52]:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.17)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту. Приймемо ρ =38%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1$ =(1000,00·100+21000,00·500)·0,83·0,38·(1-0,18/100%)= 3337222,17 грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2$ =(1000,00·100+21000,00·(500+700))·0,83·0,38·(1-0,18/100%)= 7965256,68грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3$ =(1000,00·100,00+21000,00·(500+700+800))·0,83·0,38·(1-0,18/100%)= 13254438,99 грн.

Збільшення чистого прибутку 4-го року:

$\Delta П_4$ =(1000,00·100,00+21000,00·(500+700+800+500))·0,83·0,38·(1-0,18/100%)= 16560177,93 грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.18)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,25;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = 3337222,17 /(1+0,25)^1 + 7965256,68 /(1+0,25)^2 + 13254438,99 /(1+0,25)^3 + \\ + 16560177,93 /(1+0,25)^4 = 82934939,33 \text{ грн.}$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \qquad (4.19)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 399294,63 грн.

$PV = k_{інв} \cdot ЗВ = 2 \cdot 399294,63 = 798589,26$ грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \qquad (4.20)$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 82934939,33 грн;

PV – теперішня вартість початкових інвестицій, 798589,26 грн.

$E_{абс} = ПП - PV$ = 82934939,33 - 798589,26 = 82136 350,07 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Тж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (4.21)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 12612807,79 грн;

PV – теперішня вартість початкових інвестицій, 798589,26 грн;

$T_{ж}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$$E_в = \sqrt[Тж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+82136350,07 /798589,26)^{1/4} = 2,19.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.22)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,11;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,2.

$\tau_{мін}$ = 0,11+0,2 = 0,31 < 2,19 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.23}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 2,19 = 0,46 року.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

4.5 Висновки до розділу

Згідно проведених досліджень розробки за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону» рівень комерційного потенціалу становить 44,6 бала, що свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки високий).

Також термін окупності становить 0,46 року, що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже, можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону».

ВИСНОВКИ

У даній магістерській кваліфікаційній роботі було проведено дослідження та розробку захищеного консолідованого інформаційного ресурсу системного аналізу безпеки фінансової інфраструктури регіону.

Дана тема є надзвичайно актуальною. Забезпечення безпеки критичної фінансової інфраструктури дуже важливе у сучасному світі тому, що є життєво необхідним для функціонування суспільства. Будь-яке порушення може мати серйозні наслідки для економіки та фінансової системи країни.

Швидкий розвиток технологій і зростання кількості кібератак вимагає вдосконалення заходів для захисту, тому створення консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури відповідає викликам та потребам галузі, оскільки він допоможе проводити моніторинг та аудит безпеки фінансової інфраструктури і дозволяє мати цілісний погляд на її безпеку.

Дослідження спрямовано на аналіз сучасних підходів та методів аналізу безпеки об’єктів фінансової інфраструктури, особливостей фінансового сектору, методів оцінювання стану безпеки об’єктів, вивчення основних проблем та загроз таких об’єктів, а також покращення безпеки завдяки створенню консолідованого інформаційного ресурсу.

Досліджено методи збору даних для системного аналізу та їх опрацювання, сформульовані висновки на основі проведеного аналізу та визначені ключові завдання для подальших етапів дослідження.

У другому розділі розглянуто створення захищеного консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури регіону, розглянуто вимоги до створення консолідованого інформаційного ресурсу, розроблено архітектуру та функціонал для аналізу безпеки фінансової інфраструктури, виконано розробку бази даних, використовуючи метод сутність-зв’язок, визначено сутності та їх взаємозв’язки для упорядкування інформації про стан безпеки фінансової інфраструктури.

У третьому розділі розроблено алгоритми обробки та аналізу інформації про безпеку об’єктів фінансової інфраструктури, здійснено реалізацію бази даних та формування звітів. Також виконано реалізацію можливості системного аналізу безпеки, на основі впроваджених програмних рішень проаналізовано системну безпеку фінансової інфраструктури регіону.

Четвертий розділ роботи включає проведення аналізу економічної доцільності розробки та її впровадження, розраховані економічні показники, які підтверджують високий комерційний потенціал розробленого продукту.

Магістерська робота досягла своєї основної мети, представлена розробка захищеного консолідованого інформаційного ресурсу для системного аналізу безпеки фінансової інфраструктури регіону дозволяє аналізувати і покращувати безпеку критично важливих об’єктів, а, також має можливості для подальшого вдосконалення ресурсу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова КМУ від 23.08.2016 р. № 563 . Офіційний вісник України. 2016. №69.

2. Про основні засади забезпечення кібербезпеки України» Закон України від 05.10.2017 № 2163-VIII

3. Про критичну інфраструктуру Закон України від 16.11.2021 № 1882-IX {Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}

4. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури: Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України, №601 від 06.10.2021.

5. Постанова КМ України «Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури» (№ 518 від 19.09.2019 р.),

6. Постанова КМ України «Порядок формування переліку об’єктів критичної інформаційної інфраструктури» (№ 943 від 09.10.2020 р.).

7. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об’єктів критичної інфраструктури в банківській системі України".

8. Закон України "Про основні засади забезпечення кібербезпеки України" та з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021.

9. С. Гончар, "Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури", Моделювання та інформаційні технології, Вип. 80, С. 27-32, 2017.

10. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави", Захист інформації, Т. 19, № 3, С. 214-222, 2017.

11. A. Leandros, K. Ki-Hyung, J. Helge, "Cruz Cyber security of critical infrastructures", ICT Express, №4, pp. 42-45, 2018.

12. Д. Бірюков, С. Кондратов, О. Суходоля, Зелена книга з питань захисту критичної інфраструктури в Україні, К., 2016, 176 с.

13. В. Козюра, В. Хорошко, "Заходи протидії прихованої передачі інформації в локальних мережах. Актуальні проблеми управління інформаційною безпекою держави", зб. тез наук. доп. наук.-практ. конф., Київ : Нац. акад. СБУ, С. 91-93, 2018.

14. В. Малащенко, "Теоретичні підходи до проблем та сучасних способів захисту від «інсайдерів»", Ефективність державного управління, Вип. 29, 2011.

15. Кісь Я. П. Методи документування консолідованої інформації: навч. посібник /Я. П.Кісь, Р. О.Голощук– Львів: Львівська політехніка, 2010. – 238 с. – ISBN 966-553-995-7

16. Кунанець Н. Е. Вступ до фаху «Консолідована інформація» / Н. Е. Кунанець, В. В. Пасічник. – Львів: Львівська політехніка, 2013. – 196 с. ISBN 978-966-553-975-9

17. Розробка схеми консолідації інформації на великому підприємстві. Н.О. Нещадим Наукові праці НУХТ № 40

18. Калитич Г.І. Консолідація інформації, знань і мудрості як проектування і основа гармонійного поступу України / Г.І. Калити / / НТІ, 2008 № 1

19. Кунанець Н. Е., Пасічник В. В. Вступ до спеціальності «Консолідована інформація». Навчальний посібник — Львів: «Львівська політехніка», 2010. (Серія «Консолідована інформація». Випуск 1). — 196 с

20. А. О.Азарова, А. А.Шиян,С. П.Мурза, А. В.Кудлик, Т. С.Костюк, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу ринку надання послуг медичними лабораторіями в Україні», ВісникХНУ. Технічнінауки, No 6 (279),с. 105-109, 2019.

21. A.Azarova, A. Shiyan, Y.Mironova, L. Shturma, «The development of secured consolidated infor-mation resource of activity analysis of the poultry industry in Ukraine»,Technology audit and produc-tion reserves,No 6/2 (50), pp. 14–18, 2019.

22. С. Гончар, Г. Леоненко, "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури", Information technology and security, Vol. 4, issue 2 (7), С. 262-268, 2016.

23. В. Мохор, С. Гончар, О. Дибач, "Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури", Ядерна та радіаційна безпека, Вип. 2, С. 4-8, 2019.

24. B. Kosko, "Fuzzy Cognitive Maps", International Journal of Man-Machine Studies, Vol. 24, No. 1, pp. 65-75, 1986.

25. О. М. Степанова, А. А. Волков, «Оцінка інформаційних ризиків в умовах розвитку інформаційної системи підприємства», Вісник східноукраїнського національного університету імені В. Даля, №10 (240), с.106-110, 2017.

26. І. С. Добринін, Н. О. Мальцева, «Вдосконалення методики факторного аналізу інформаційних ризиків», Системи обробки інформації, Вип.3 (149), с.146-150, 2017.

27. О. Г. Корченко, С. В. Казмірчук, «Метод оцінювання ризиків інформаційної безпеки на основі відкритих баз даних уразливостей», Безпека інформації, т.22, №2, с.214-224, 2016.

28. Ю. М. Ткач, С.В. Казмірчук та ін., «Застосування методу експертних оцінок до оцінювання інформаційних ризиків вищого навчального закладу», Захист інформації, т.19, №2, с.137-142, 2017.

29. Салієва О.В. Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп’ютерної мережі / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 21, №4, 2019. – С. 28–39.

30. Салієва О.В. Когнітивна модель для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №2, 2020. – С. 64–73.

31. Салієва О.В. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №1, 2020. – С. 42–49.

32. Салієва О.В. Визначення допустимої інтенсивності зниження рівня захищеності об’єкта критичної інфраструктури ранжуванням загроз / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №2, 2020. – С. 63–76.

33. Салієва О.В. Динамічний часовий аналіз впливу факторів загроз на рівень захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Захист інформації. – Т. 22, №3, 2020. – С. 47–55.

34. Салієва О.В. Симпліціальний аналіз структури когнітивної моделі для дослідження рівня захищеності об’єкта критичної інфраструктури / О.В. Салієва, Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 22, №3, 2020. – С. 59–65.

35. Салієва О.В. Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об’єкту критичної інфраструктури за результатами когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Вісник Черкаського державного технологічного університету. – №3, 2020. – С. 74–83.

36. Салієва О.В. Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту інформації / О.В. Салієва, Ю.Є. Яремчук // Вісник Вінницького політехнічного інституту. – №5, 2020. – С. 47–54.

37. О.А. Боднар, Дисципліна «Фінансова інфраструктура». Курс лекцій, Миколаївський національний аграрний університет,

38. СТРАТЕГІЯ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ ДО 2025 РОКУ, Міністерство Фінансів України
https://mof.gov.ua/storage/files/Strategija_financovogo_sectoru_ua.pdf

39. Корнієнко С. К. Системи баз даних: організація та проектування: Навчальний посібник / С. К. Корнієнко. – Запоріжжя : ЗНТУ, 2006. – С. 252.

40. А. О. Азарова, А. А. Шиян, і Л. О. Нікіфорова, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу діяльності морських портів України», ІТКІ, вип. 48, вип. 2, с. 27–36, Вер 2020.

41. А. О. Азарова, А. А. Шиян, С. П. Мурза, А. В. Кудлик, Т. С. Костюк, «Розроблення захищеного консолідованого інформаційного ресурсу аналізу ринку надання послуг медичними лабораторіями в Україні», Вісник ХНУ. Технічні науки, No 6 (279),с. 105-109, 2019.

42. A.Azarova, A. Shiyan, Y.Mironova, L. Shturma, «The development of secured consolidated information resource of activity analysis of the poultry industry in Ukraine»,Technology audit and produc-tion reserves,No 6/2 (50), pp. 14–18, 2019.

43. A.Silberschatz, H. F.Korth, S.Sudarshan, Database system concepts. New York, USA: McGraw-Hill, 2011,1349.

44. В. М. Богуш, О. А. Довидьков, В. Г. Кривуца, Теоретичні основи захищених інформаційних технологій. К., Україна: ДУІКТ, 2010,454с.

45. Гайна Г.А. Основи проектування баз даних: Навчальний посібник / Г.А. Гайна. − К. : КНУБА, 2005. – 204 с.

46. Гайджарги В. І. Основи проектування та використання баз даних: навчальний посібник / В.І. Гайджарги, О.А. Дацюк. – К.: ІВЦ «Видавництво «Політехніка», 2004. – 256 с

47. Гайна Г.А. Організація баз даних і знань. Мови баз даних: Конспект лекцій.−К.:КНУБА, 2002. − 64 с.

48. Гайна Г.А., Попович Н.Л. Організація баз даних і знань. Організація реляційних баз даних: Конспект лекцій.−К.:КНУБА, 2000. − 76 с

49. Бази даних: проектування та реалізація/ Г. С. Погромська, Н.А. Махровська. – Місто: Видавництво, 2019. – 183 с

50. Харів Н. О. Х 20 Бази даних та інформаційні системи: навчльний посібник / Н. О. Харів. – Рівне : НУВГП, 2018. – 127 с.

51. Пасічник В. В., Резніченко В. А. Організація баз даних та знань. – К.: Видавнича група BHV, 2006. – 384 с.: іл

52. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с.

53. Кавецький В. В. Економічне обґрунтування інноваційних рішень: практикум / В. В. Кавецький, В. О. Козловський, І. В. Причепа. Вінниця : ВНТУ, 2016. 113 с

54. Павленко Б.В. Підвищення стійкості методу захисту забезпечення автентичності растрових зображень доказової бази від несанкціонованого доступу / Б.В. Павленко, Д.П. Присяжний, В.В. Карпінець, Я.Ю. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 20, №4, 2018. – С. 85–99.

55. Карпінець В.В. Підвищення стійкості цифрових водяних знаків до геометричних перетворень шляхом визначення особливих точок зображення / В.В. Карпінець, П.В. Павловський, О.В. Салієва, Я.Ю. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 2(36), 2018. – С. 27–36.

56. Приймак А.В. Дослідження можливості використання алгоритму циклічного надлишкового коду для підвищення стійкості криптосхеми ECIES / А.В. Приймак, О.В. Салієва, Я.Ю. Яремчук // Вісник Хмельницького національного університету. –№1, 2019. – С. 155–161.

57. Приймак А.В. Метод автоматизованого пошуку несанкціонованого майнінгу криптовалюти у контейнерах серверних ОС / А.В. Приймак, В.В. Карпінець, Я.Ю. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 2(36), 2020. – С. 16–24.

58. Шиян А.А., Нікіфорова Л.О., Дьогтєва І.О., Яремчук Я.Ю. Модель управління протидією інформаційним атакам в кіберпросторі // Реєстрація, зберігання і обробка даних. – Т. 23, №2, 2021. – С. 62–71.

59. Салієва О.В., Яремчук Я.Ю. Порівняння моделей інформаційної безпеки за характеристиками суб’єктів // Збірник матеріалів 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI сторіччі». Том 9. Міжнародна конференція «Управління знаннями та конкурентна розвідка». – Харків, 2019. – С. 67–68.

60. Яремчук Я.Ю. Дослідження можливості підвищення стійкості протоколу аутентифікації WPA-PSK // Матеріали XLVIII науково-технічної конференції

підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2019) [Електронне мережне наукове видання] : збірник доповідей. – Вінниця : ВНТУ, 2018. – С. 2455–2456.

61. Приймак А. В., Яремчук Я.Ю. Метод захисту від несанкціонованого майнінгу криптовалюти на основі виявлення підозрілих процесів в контейнерах серверних операційних систем // Метеріали VI-ої Міжнародної науково-практичної конференції «Перспективні напрями захисту інформації». – Одеса, 2020. – С. 76–78.

62. Шиян А.А. Перспективи використання методів розмежування доступу в інформаційному протиборстві / А. А. Шиян, М. Л. Тюльпін, Я. Ю. Яремчук // Матеріали XII Міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій» (ITSec-2023), м. Ужгород, 2–4 травня 2023 р. – К.: НАУ, 2023. – С. 120–122.

63. Шиян А.А. Метод формування системи захисту від інформаційно-психологічних атак у соціальних мережах / А. А. Шиян, Я. Ю. Яремчук, В. В. Саврацький // Матеріали IX Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем», Львів, 25–26 травня 2023 р. – 2023. – С. 43–44.

64. Грицак А.В. Підвищення стійкості віртуальних серверів до DDOS-атак на основі масштабування обчислювальних ресурсів кластера / А. В. Грицак, Я. Ю. Яремчук, В. М. Білоус // Матеріали VI Міжнародної науково-практичної конференції «Інформаційна безпека та комп’ютерні технології»: тези доповідей, 20-21 квітня 2023 р. – Кропивницький: ЦНТУ, 2023. – С. 83–84.

65. Яремчук Я. Ю. Системний аналіз безпеки фінансової інфраструктури регіону на основі захищеного консолідованого інформаційного ресурсу [Електронний ресурс] / Я. Ю. Яремчук, Ю. Є. Яремчук // Міжнародна науково-практична інтернет-конференція «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)»: тези доповідей, Вінниця, 2023 р. – Електрон. текст. дані. – 2023. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19733/16338.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції "Управління інформаційною безпекою" кафедри МБІС
д.т.н., професор
_____ Юрій ЯРЕМЧУК
"20" вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ
до магістерської кваліфікаційної роботи на тему:
Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону
08-72.МКР.009.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи
к.т.н, доц.
_____ Карпінець В.В._____

Вінниця – 2023 р.

1. Найменування та область застосування

Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону

2.Підстава для розробки

Розробка виконується на основі наказу ректора ВНТУ від 18 вересня 2023 року № 247

3. Мета та призначення розробки

3.1 Мета розробки: розробка захищеного консолідованого інформаційного ресурсу системного аналізу безпеки фінансової інфраструктури регіону

3.2 Призначення: консолідація та системний аналіз безпеки фінансової інфраструктури та захист цих даних.

4. Джерела розробки

4.1. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // Сучасний захист інформації. – 2016. №4.– С. 47-51.

4.2. Бурячок В.Л. Політика інформаційної безпеки: підручник. / В.Л.Бурячок, Р.В.Грищук, В.О.Хорошко / За заг. ред. докт. техн. наук, проф. В.О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

4.3. Єсін В.І. Безпека інформаційних систем і технологій / В.І.Єсін, О.О. Кузнецов, Л.С. Сорока. – Харків: ХНУ імені В.Н. Каразіна, 2013. – 632 с.

4.4. ZakariaOmar, ZangooeiToomaj, MohdAfiziMohdShukran. Enhancing Mixing Recognition-Based and Recall-Based Approach in Graphical Password Scheme. IJACT, Vol. 4, No. 15, pp. 189-197, 2012.

5. Вимоги до програми

5.1 Вимоги до функціональних характеристик:

5.1.1 Програмний засіб повинен мати зручний, легкий у використанні інтерфейс користувача;

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків;

5.1.3 Програмний засіб повинен виконувати процес автентифікації користувачів у системі.

5.2 Вимоги до надійності:

5.2.1 Програмний засіб повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень;

5.2.2 Бази даних повинні бути налаштовані на автоматичне створення резервних копій;

5.2.3 Програмний засіб повинен виконувати свої функції.

5.3 Вимоги до складу і параметрів технічних засобів:

– процесор – Pentium 1500 МГц і подібні до них;

– оперативна пам’ять – не менше 512 Mb;

– середовище функціонування – операційна система сімейство Windows;

– вимоги до техніки безпеки при роботі з програмою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп’ютерною технікою.

6. Вимоги до програмної документації

6.1 Обов'язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.4.

7. Вимоги до технічного захисту інформації

7.1 Необхідно забезпечити захист розроблюваного програмного засобу від несанкціонованого використання.

7.2 Неможливість отримання доступу незареєстрованих користувачів до інформаційних ресурсів.

8. Техніко-економічні показники

8.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

8.2 Має бути реалізований таким чином, щоб підходити для використання широкого загалу.

9. Стадії та етапи розробки

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи		Примітка
1.	Визначення напрямку магістерської роботи, формулювання теми	20.09.2023	31.09.2023	
2.	Аналіз предметної області обраної теми	01.10.2023	15.10.2023	
3.	Розробка роботи	16.10.2023	26.10.2023	
4.	Написання магістерської роботи на основі розробленої теми	27.10.2023	15.11.2023	
5.	Передзахист магістерської кваліфікаційної роботи	16.11.2023	24.11.2023	
6.	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	27.11.2023	04.12.2023	
7.	Захист магістерської кваліфікаційної роботи	11.12.2023	17.12.2023	

10. Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- програмний додаток;
- презентація;
- відзив керівника роботи;
- відзив опонента.

Технічне завдання до виконання прийняв _____ Яремчук Я.Ю.

Додаток Б. Лістинги програм

users/models.py – модель Користувача

```
from django.contrib.auth.models import AbstractUser, BaseUserManager
from django.db import models
from django.conf import settings

class CustomUserManager(BaseUserManager):

    use_in_migrations = True

    def _create_user(self, ipn, password, **extra_fields):
        if not ipn:
            raise ValueError('Необхідно вказати Індивідуальний податковий номер')
        ipn = ipn.strip()
        user = self.model(ipn=ipn, **extra_fields)
        user.set_password(password)
        user.save(using=self._db)
        return user

    def create_user(self, ipn, password=None, **extra_fields):
        extra_fields.setdefault('is_staff', False)
        extra_fields.setdefault('is_superuser', False)
        return self._create_user(ipn, password, **extra_fields)

    def create_superuser(self, ipn, password, **extra_fields):
        extra_fields.setdefault('is_staff', True)
        extra_fields.setdefault('is_superuser', True)
        extra_fields.setdefault('role', User.Role.ADMINISTRATOR)

        if extra_fields.get('is_staff') is not True:
            raise ValueError('Superuser must have is_staff=True.')
        if extra_fields.get('is_superuser') is not True:
            raise ValueError('Superuser must have is_superuser=True.')
        if extra_fields.get('role') is not User.Role.ADMINISTRATOR:
            raise ValueError('Superuser must have ADMINISTRATOR role.')
        return self._create_user(ipn, password, **extra_fields)

def random_string(
        length,
        allowed_chars="-+_$&abcdefghjkmnpqrstuvwxyz-
+_$&23456789ABCDEFGHJKLMNPQRSTUVWXYZ-+_$&23456789-+_$&",
):
    return BaseUserManager().make_random_password(length, allowed_chars)

class User(AbstractUser):
    class Role(models.IntegerChoices):
        NO_ROLE = 0, 'Відсутня'
        ADMINISTRATOR = 1, 'Адміністратор'
```

```
        OPERATOR = 2, 'Оператор'
        ANALYST = 3, 'Аналітик'

    username = None
    USERNAME_FIELD = 'ipn'
    REQUIRED_FIELDS = ['last_name', 'first_name', 'email']

    ipn = models.CharField('ІПН', max_length=30, unique=True)
    email = models.EmailField('Email адреса', default='', blank=True)
    middle_name = models.CharField('По-батькові', max_length=40, default='', blank=True)
    phone = models.CharField('Контактний телефон', max_length=20, default='', blank=True)
    role = models.IntegerField('Роль', choices=Role.choices, default=Role.NO_ROLE, blank=True,
db_index=True)

    objects = CustomUserManager()

    class Meta:
        indexes = [
            models.Index(fields=['last_name', ]),
        ]
        verbose_name = 'Користувач'
        verbose_name_plural = 'Користувачі'

    def __str__(self):
        return f'{self.full_name} ({self.ipn})'

    @property
    def full_name(self):
        return f'{self.last_name} {self.first_name} {self.middle_name}'.strip()

    def get_full_name(self):
        return self.full_name

    @property
    def is_operator(self):
        return self.role == self.Role.OPERATOR

    @property
    def is_analyst(self):
        return self.role == self.Role.ANALYST

    @property
    def is_administrator(self):
        return self.is_superuser and self.role == self.Role.ADMINISTRATOR

    @property
    def is_otp_member(self):
        return self.role in [self.Role.ADMINISTRATOR, self.Role.OPERATOR, self.Role.ANALYST]

    @property
    def role_admin_path(self):
        role_str = self.Role._value2member_map_[self.role].name
```

```
        return settings.ROLE_ADMIN_PATH.get(role_str)

    @property
    def make_rnd_psw(self):
        return random_string(length=12)

class LoginLog(models.Model):
    username = models.CharField("Логін", max_length=150, blank=True)
    user = models.ForeignKey(User, models.SET_NULL, verbose_name='Користувач', blank=True,
null=True)
    ip_address = models.TextField('IP адреса', blank=True)
    user_agent = models.TextField('User-Agent', blank=True)
    datetime = models.DateTimeField('Дата та час', auto_now_add=True)
    is_successful = models.BooleanField('Чи успішно')

    def __str__(self):
        return f'Вхід: {self.username}'

    class Meta:
        verbose_name = 'Вхід'
        verbose_name_plural = 'Журнал входу'
        ordering = ['-id']

    @classmethod
    def create(cls, request) -> 'LoginLog':
        username = request.POST.get('username')
        if len(username) > 100:
            username = username[:100] + '...'
        log = LoginLog(
            username=username,
            is_successful=request.user.is_authenticated,
            user_agent=request.headers.get('User-Agent', ''),
        )
        if request.user.is_authenticated:
            log.user = request.user
        log.ip_address = cls.get_ip_from_request(request)
        log.save()
        return log

    @staticmethod
    def get_ip_from_request(request):
        x_forwarded_for = request.META.get('HTTP_X_FORWARDED_FOR', '')
        if x_forwarded_for:
            return x_forwarded_for.split(',')[0].strip()
        return request.META.get('REMOTE_ADDR', '')
```

dictionary/models.py – моделі довідників

```
from django.db import models
from django.contrib.auth import get_user_model
```

```
User = get_user_model()

class Region(models.Model):
    name = models.CharField('Область', max_length=100, unique=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Область'
        verbose_name_plural = 'Області'

class Settlement(models.Model):
    name = models.CharField('Населений пункт', max_length=100)
    region = models.ForeignKey(Region, on_delete=models.CASCADE, related_name='settlement', verbose_name='Область')

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Населений пункт'
        verbose_name_plural = 'Населені пункти'

class FinancialInstitutionType(models.Model):
    name = models.CharField('Назва', max_length=100, default='', blank=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Тип фінансової установи'
        verbose_name_plural = 'Типи фінансової установи'

class CriticalityCategories(models.Model):
    name = models.CharField('Назва', max_length=250, default='', blank=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['id']
        verbose_name = 'Категорія критичності'
        verbose_name_plural = 'Категорії критичності'

class ImplementationLevel(models.Model):
    name = models.CharField('Назва', max_length=250, default='', blank=True)
```

```
    def __str__(self):
        return self.name

    class Meta:
        ordering = ['id']
        verbose_name = 'Рівень впровадження заходів кіберзахисту'
        verbose_name_plural = 'Рівні впровадження заходів кіберзахисту'
```

core/models.py – моделі інших основних сутностей

```
from django.db import models
from django.contrib.auth import get_user_model

from dictionary.models import (
    Region,
    Settlement,
    FinancialInstitutionType,
    CriticalityCategories,
    ImplementationLevel,
)

User = get_user_model()

class Contact(models.Model):
    last_name = models.CharField("Прізвище", max_length=50)
    first_name = models.CharField("Ім'я", max_length=50)
    middle_name = models.CharField("По батькові", max_length=50, blank=True, default='')
    ipn = models.CharField('ІПН', max_length=16, unique=True)
    email = models.EmailField('Email')
    phone = models.CharField('Phone', max_length=30)
    info = models.TextField('Додаткова інформація', blank=True, default='')
    created_at = models.DateTimeField('Дата створення в системі', auto_now_add=True)
    is_active = models.BooleanField('Активний', blank=True, default=False)
    crc = models.CharField('CRC', max_length=64, blank=True, null=True)

    def __str__(self):
        return f'{self.last_name} {self.first_name} {self.middle_name}'.strip()

    class Meta:
        ordering = ['last_name']
        verbose_name = 'Контакт'
        verbose_name_plural = 'Контакти'

class FinancialInstitution(models.Model):
    name = models.CharField('Назва', max_length=250)
    edrpou = models.CharField('ЄДРПОУ', max_length=16)
    region = models.ForeignKey(Region, on_delete=models.DO_NOTHING, related_name='fin',
verbose_name='Область')
    settlement = models.ForeignKey(Settlement, on_delete=models.DO_NOTHING,
related_name='fin', verbose_name='Населений пункт')
```

```
    street = models.CharField('Вулиця', max_length=150)
    house = models.CharField('Будинок', max_length=10)
    fin_type = models.ForeignKey(FinancialInstitutionType, on_delete=models.DO_NOTHING,
related_name='fin', verbose_name='Тип установи', blank=True, default=False)
    date_start = models.DateTimeField('Дата реєстрації', blank=True, default=None)
    created_at = models.DateTimeField('Дата створення в системі', auto_now_add=True)
    iso_27001_2015 = models.BooleanField(null=True, blank=True, verbose_name='ISO 27001:2015')
    iso_27032_2016 = models.BooleanField(null=True, blank=True, verbose_name='ISO 27032:2016')
    iso_27010_2018 = models.BooleanField(null=True, blank=True, verbose_name='ISO 27010:2018')
    is_active = models.BooleanField('Активна', blank=True, default=False)
    ciso = models.ForeignKey(Contact, on_delete=models.DO_NOTHING, related_name='fin_ciso',
                    verbose_name='Керівник ІТ-безпеки')
    owner = models.ForeignKey(Contact, on_delete=models.DO_NOTHING,
related_name='fin_owner', verbose_name='Власник', blank=True, default=False)
    info = models.TextField('Додаткова інформація', blank=True, default='')
    crc = models.CharField('CRC', max_length=64, blank=True, null=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['name']
        verbose_name = 'Фінансова установа'
        verbose_name_plural = 'Фінансові установи'

class OperatorKI(models.Model):
    name = models.CharField('Найменування (П.І.Б. у разі наявності)', max_length=255)
    edrpou = models.CharField('ЄДРПОУ', max_length=16)
    region = models.ForeignKey(Region, on_delete=models.DO_NOTHING, related_name='operator',
verbose_name='Область')
    settlement = models.ForeignKey(Settlement, on_delete=models.DO_NOTHING,
related_name='operator', verbose_name='Населений пункт')
    street = models.CharField('Вулиця', max_length=150)
    house = models.CharField('Будинок', max_length=10)
    chief = models.ForeignKey(Contact, on_delete=models.DO_NOTHING, related_name='operator',
verbose_name='Керівник оператора ОКІ')
    info = models.TextField('Додаткова інформація', blank=True, default='')
    crc = models.CharField('CRC', max_length=64, blank=True, null=True)

    def __str__(self):
        return self.name

    class Meta:
        verbose_name = "Оператор ОКІ"
        verbose_name_plural = "Оператори ОКІ"

class ObjectKI(models.Model):
    name = models.CharField('Назва об’єкту', max_length=255)
    region = models.ForeignKey(Region, on_delete=models.DO_NOTHING, related_name='oki',
verbose_name='Область')
    settlement = models.ForeignKey(Settlement, on_delete=models.DO_NOTHING,
                        related_name='oki', verbose_name='Населений пункт')
```

```
    street = models.CharField('Вулиця', max_length=150)
    house = models.CharField('Будинок', max_length=10)
    fin_institution = models.ForeignKey(FinancialInstitution, on_delete=models.DO_NOTHING,
                                        related_name='oki', verbose_name='Фінансова установа')
    crit_categories = models.ForeignKey(CriticalityCategories, on_delete=models.DO_NOTHING,
                                        related_name='oki', verbose_name='Категорія критичності')
    cyber_level = models.ForeignKey(ImplementationLevel, on_delete=models.DO_NOTHING,
related_name='+', null=True, blank=True, verbose_name='Рівень впровадження кіберзахисту')
    operator = models.ForeignKey(OperatorKI, on_delete=models.DO_NOTHING, related_name='oki',
verbose_name='Оператор')
    owner = models.ForeignKey(Contact, on_delete=models.DO_NOTHING,
related_name='oki_owner', verbose_name='Власник', blank=True, default=False)
    created_at = models.DateTimeField('Дата створення в системі', auto_now_add=True)
    is_active = models.BooleanField('Активна', blank=True, default=False)
    info = models.TextField('Додаткова інформація', blank=True, default='')
    crc = models.CharField('CRC', max_length=64, blank=True, null=True)

    def __str__(self):
        return f'{self.name} (Кат.{self.crit_categories}, {self.fin_institution}/{self.region},
{self.settlement}, {self.street}{self.house})'

    class Meta:
        verbose_name = "Об'єкт критичної інфраструктури"
        verbose_name_plural = "Об'єкти критичної інфраструктури"

class Audit(models.Model):

    name = models.CharField('Назва', max_length=255)
    created_at = models.DateTimeField('Дата створення', auto_now_add=True)
    updated_at = models.DateTimeField('Останні зміни', auto_now=True)
    author = models.ForeignKey(User, on_delete=models.DO_NOTHING, related_name='oki',
verbose_name='Автор')
    object_ki = models.ForeignKey(ObjectKI, on_delete=models.DO_NOTHING,
related_name='analysis', verbose_name="Об'єкт критичної інфраструктури")
    physical_security = models.BooleanField('Фізична охорона', blank=True, null=True)
    restrictive_structures = models.BooleanField('Обмежувальні споруди', blank=True, null=True)
    access_control = models.BooleanField('Контроль доступу', blank=True, null=True)
    video_surveillance = models.BooleanField('Відеоспостереження', blank=True, null=True)
    alarms = models.BooleanField('Сигналізація', blank=True, null=True)
    fire_protection = models.BooleanField('Протипожежний захист', blank=True, null=True)
    backup_power = models.BooleanField('Резервне енергозабезпечення', blank=True, null=True)
    personnel_protection = models.BooleanField('Захист персоналу', blank=True, null=True)
    user_authentication = models.BooleanField('Автентифікація користувачів', blank=True,
null=True)
    regular_update = models.BooleanField('Регулярне оновлення', blank=True, null=True)
    ids = models.BooleanField('Система виявлення і захисту від кібератак (IPS/IDS)', blank=True,
null=True)
    information_protection = models.BooleanField('Захист інформації', blank=True, null=True)
    monitoring = models.BooleanField('Моніторинг', blank=True, null=True)
    backup = models.BooleanField('Резервне копіювання', blank=True, null=True)
    personnel_training = models.BooleanField('Навчання персоналу з кібербезпеки', blank=True,
null=True)
```

```
    physical_security_score = models.PositiveIntegerField('Оцінка фізичної безпепки', blank=True, null=True)
    cyber_security_score = models.PositiveIntegerField('Оцінка кібербезпеки', blank=True, null=True)
    integral_security_score = models.PositiveIntegerField('Інтегральна оцінка безпеки', blank=True, null=True)
    recommendation = models.TextField('Рекомендації', blank=True, default='')
    info = models.TextField('Додаткова інформація', blank=True, default='')
    crc = models.CharField('CRC', max_length=64, blank=True, null=True)

    def __str__(self):
        return self.name

    class Meta:
        ordering = ['-created_at']
        verbose_name = "Аудит"
        verbose_name_plural = "Аудити"
```

---

core/templates/admin/report_oki.html - шаблон звіту

```
{% load static %}
<!doctype html>
<html lang="uk">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <meta name="robots" content="NONE,NOARCHIVE">
    <title>Звіт | {{ site_header }}</title>
    <link href="{% static '/css/bootstrap_v4.6.2.min.css' %}" rel="stylesheet">

    <style>
      #spinner {
          position: fixed !important;
          left: 50% !important;
          top: 50%;
      }
    </style>
  </head>
  <body>

    <div id="spinner" class="spinner-border text-secondary" role="status" hidden>
      <span class="sr-only">Loading...</span>
    </div>

    <div class="container-fluid">
      <div class="row">
        <div class="col-12">
          <h1 class="my-5 text-center">Звіт безпеки об’єктів критичної інфраструктури</h1>
```

```
      </div>
    </div>
    <div class="row">
      <div class="col-6">
        <h4>Chart1</h4>
        <div class="chart-container" style="position: relative; height:60vh; width:90vw">
          <canvas id="chart1"></canvas>
        </div>
      </div>
      <div class="col-6">
        <h4>Chart2</h4>
        <div class="chart-container" style="position: relative; height:60vh; width:90vw">
          <canvas id="chart2"></canvas>
        </div>
      </div>
    </div>
  </div>

  <script src="{% static '/js/jquery-3.6.3_01.min.js' %}"></script>
  <script src="{% static '/js/bootstrap_v4.6.2.bundle.min.js' %}"></script>
  <script src="{% static '/js/chart.umd.min.js' %}"></script>

  {{ chart1_data|json_script:"chart1_data" }}
  {{ chart2_data|json_script:"chart2_data" }}

  <script>
    const chart1_values = JSON.parse(document.getElementById('chart1_data').textContent);
    const ctx1 = document.getElementById('chart1');
    new Chart(ctx1, {
        type: 'bar',
        data: chart1_values,
        options: {
            scales: {
                y: {
                    beginAtZero: true
                }
            }
        }
    });
  </script>

  <script>
    const chart2_values = JSON.parse(document.getElementById('chart2_data').textContent);
    const ctx2 = document.getElementById('chart2');
    new Chart(ctx2, {
        type: 'pie',
        data: chart2_values,
    });
  </script>

 </body>
</html>
```

---
dictionary/admin.py - оголошення довідників в адмінці

```
from django.contrib import admin
from core.admin import administrator_admin

from dictionary.models import (
    Region,
    Settlement,
    FinancialInstitutionType,
    CriticalityCategories,
    ImplementationLevel,
)


@admin.register(Region, site=administrator_admin)
class RegionAdmin(admin.ModelAdmin):

    fields = (
        'name',
    )
    readonly_fields = ()

    list_display = (
        'name',
    )

    def has_delete_permission(self, request, obj=None):
        return False


@admin.register(Settlement, site=administrator_admin)
class SettlementAdmin(admin.ModelAdmin):

    fields = (
        'name',
        'region',
    )
    readonly_fields = ()

    list_display = (
        'name',
        'region',
    )

    def has_delete_permission(self, request, obj=None):
        return False
```

```
@admin.register(FinancialInstitutionType, site=administrator_admin)
class FinancialInstitutionTypeAdmin(admin.ModelAdmin):

    fields = (
        'name',
    )
    readonly_fields = ()

    list_display = (
        'name',
    )

    def has_delete_permission(self, request, obj=None):
        return False


@admin.register(CriticalityCategories, site=administrator_admin)
class CriticalityCategoriesAdmin(admin.ModelAdmin):

    fields = (
        'name',
    )
    readonly_fields = (
    )

    list_display = (
        'name',
    )

    def has_delete_permission(self, request, obj=None):
        return False


@admin.register(ImplementationLevel, site=administrator_admin)
class ImplementationLevelAdmin(admin.ModelAdmin):

    fields = (
        'name',
    )
    readonly_fields = (
    )

    list_display = (
        'name',
    )

    def has_delete_permission(self, request, obj=None):
        return False
```

---
system/settings.py - основний файл конфігурації

```
import os
from pathlib import Path

# Build paths inside the project like this: BASE_DIR / 'subdir'.
BASE_DIR = Path(__file__).resolve().parent.parent

SECRET_KEY = '@olo9^0H!u748-5^-1elfs7e@m!u509-57ej5_*p@c@ol9^0b9^-+d&!z_z8=naqrx'

DEBUG = True
DEBUG_TOOLBAR = False

ALLOWED_HOSTS = []

# Application definition

INSTALLED_APPS = [
    'django.contrib.admin',
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.messages',
    'django.contrib.staticfiles',

    'django_otp',
    'totp2fa.apps.Totp2FaConfig',
    "crispy_forms",
    "crispy_bootstrap5",
    "slick_reporting",

    'users',
    'dictionary',
    'core',
]

MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django_otp.middleware.OTPMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware',
]

ROOT_URLCONF = 'system.urls'
```

```
TEMPLATES = [
    {
        'BACKEND': 'django.template.backends.django.DjangoTemplates',
        'DIRS': [os.path.join(BASE_DIR, 'templates')],
        'APP_DIRS': True,
        'OPTIONS': {
            'context_processors': [
                'django.template.context_processors.debug',
                'django.template.context_processors.request',
                'django.contrib.auth.context_processors.auth',
                'django.contrib.messages.context_processors.messages',
            ],
        },
    },
]

WSGI_APPLICATION = 'system.wsgi.application'


# Password validation

AUTH_PASSWORD_VALIDATORS = [
    {
        'NAME': 'django.contrib.auth.password_validation.UserAttributeSimilarityValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.MinimumLengthValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.CommonPasswordValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',
    },
]


# Internationalization

LANGUAGE_CODE = 'uk'
TIME_ZONE = 'Europe/Kiev'
USE_I18N = True
USE_TZ = True

AUTH_USER_MODEL = 'users.User'

# Static files (CSS, JavaScript, Images)

STATIC_URL = 'static/'
MEDIA_URL = 'media/'
```

```
# Default primary key field type

DEFAULT_AUTO_FIELD = 'django.db.models.BigAutoField'

CRISPY_TEMPLATE_PACK = "bootstrap5"
CRISPY_ALLOWED_TEMPLATE_PACKS = "bootstrap5"

SLICK_REPORTING_SETTINGS = {
    "CHARTS": {
        "apexcharts": {
            "entryPoint": "DisplayApexPieChart",
            "js": ("https://cdn.jsdelivr.net/npm/apexcharts", "slick_reporting/slick_reporting.chartsjs.js"),
            "css": {"all": ("https://cdn.jsdelivr.net/npm/apexcharts/dist/apexcharts.min.css",)},
        },
    },
}

SITE_HEADER = f"Консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури"

try:
    from .settings_local import *
except ImportError:
    pass
```

Додаток В. Ілюстративний матеріал

ЗАХИЩЕНИЙ КОНСОЛІДОВАНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС СИСТЕМНОГО АНАЛІЗУ БЕЗПЕКИ ФІНАНСОВОЇ ІНФРАСТРУКТУРИ РЕГІОНУ

ВИКОНАЛА СТУДЕНТКА ГРУПИ 2КІТС-22М **ЯРЕМЧУК Я.Ю.**

НАУКОВИЙ КЕРІВНИК: К.Т.Н., ДОЦ. КАФ МБІС **КАРПІНЕЦЬ В.В.**

АКТУАЛЬНІСТЬ РОБОТИ

Важливим є забезпечення безпеки критичних об’єктів фінансових установ, оскільки будь-яке порушення може мати серйозні наслідки для економіки і фінансової системи регіону та країни в цілому.

Актуальним є створення консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури, спрямованого на забезпечення безпеки фінансової системи та запобігання потенційним загрозам, допоможе проводити моніторинг безпеки фінансової інфраструктури, аналізувати загрози та виявляти її можливі проблеми.

Така система забезпечить цілісне представлення про безпеку фінансової інфраструктури, зручний доступ до інформації для аналітиків, а також дозволить вчасно приймати рішення щодо запобігання потенційним загрозам.

ОБ’ЄКТ ДОСЛІДЖЕННЯ	ПРЕДМЕТ ДОСЛІДЖЕННЯ	НАУКОВА НОВИЗНА
оцінювання стану безпеки критичних об’єктів фінансової інфраструктури	сукупність теоретичних засад і практичних заходів створення консолідованого інформаційного ресурсу	вперше розроблено захищений консолідований інформаційний ресурс аналізу безпеки фінансової інфраструктури регіону

3

КРИТИЧНА ІНФРАСТРУКТУРА

Критична інфраструктура – це сукупність об’єктів державної інфраструктури, найбільш важливих для економіки і промисловості, функціонування суспільства і безпеки населення, виведення з ладу або руйнування яких може вплинути на національну безпеку і обороноздатність, природне середовище, призвести до значних фінансових і людських втрат.

4

НОРМАТИВНО-ПРАВОВА БАЗА ДЕРЖАВИ ЩОДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНИХ ІНФРАСТРУКТУР

– Стратегія кібербезпеки України (указ Президента України №447/2021 від 26.08.2021 р.),

– Закон України «Про основні засади забезпечення кібербезпеки України» (№45, 2017 р.),

– Закон України «Про критичну інфраструктуру та її захист» (№ 1882-IX від 16.11.2021 р.).

– Постанова КМ України «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури» (№ 518 від 19.09.2019 р.),

– Постанова КМ України «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» (№ 943 від 09.10.2020 р.).

5

МІЖНАРОДНІ СТАНДАРТИ **ISO**, ЩО ЗАБЕЗПЕЧУЮТЬ БЕЗПЕКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ISO/IEC 27001:2015 (ISO/IEC 27001:2013, Cor 1:2014, IDT);

ISO/IEC 27010:2018 (ISO/IEC 27010:2015, IDT);

ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT).

6

ФІНАНСОВА ІНФРАСТРУКТУРА

Фінансова інфраструктура є однією з ключових складових критичної інфраструктури регіону і включає у себе сукупність установ, які функціонують на ринку фінансових послуг, таких як банки, страхові компанії, пенсійні фонди, платіжні системи, розрахункові й клірингові центри, кредитні установи, фінансові регулятори та інші фінансові установи.

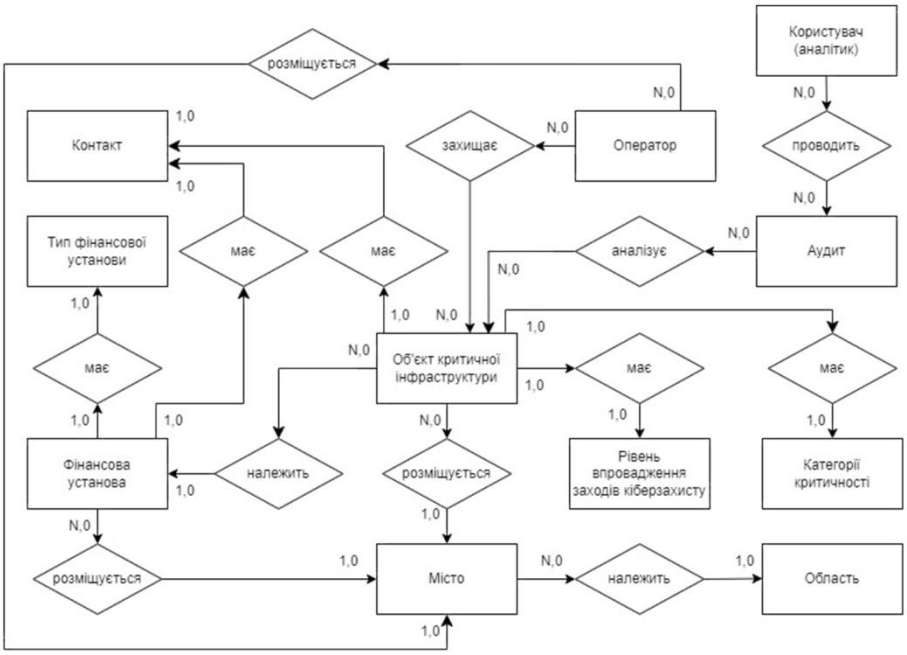
7

РОЗРОБКА ЗАХИЩЕНОГО КОНСОЛІДОВАНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

- розроблено і реалізовано основні модулі захищеного консолідованого інформаційного ресурсу аналізу безпеки фінансової інфраструктури регіону.
- досліджено і враховано особливості фінансової інфраструктури;
- спроектована і розроблена база даних для функціонування інформаційного ресурсу;
- реалізовано аналітичні звіти у різних розрізах;
- створено захист інформаційного ресурсу.

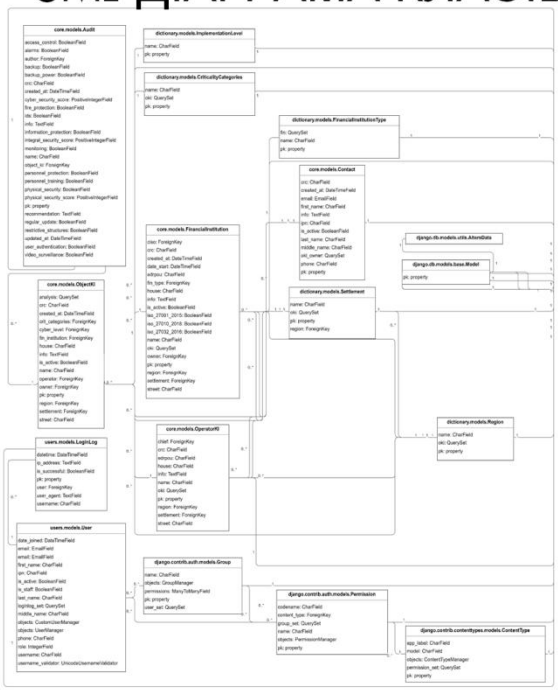
8

ER-МОДЕЛЬ БАЗИ ДАНИХ



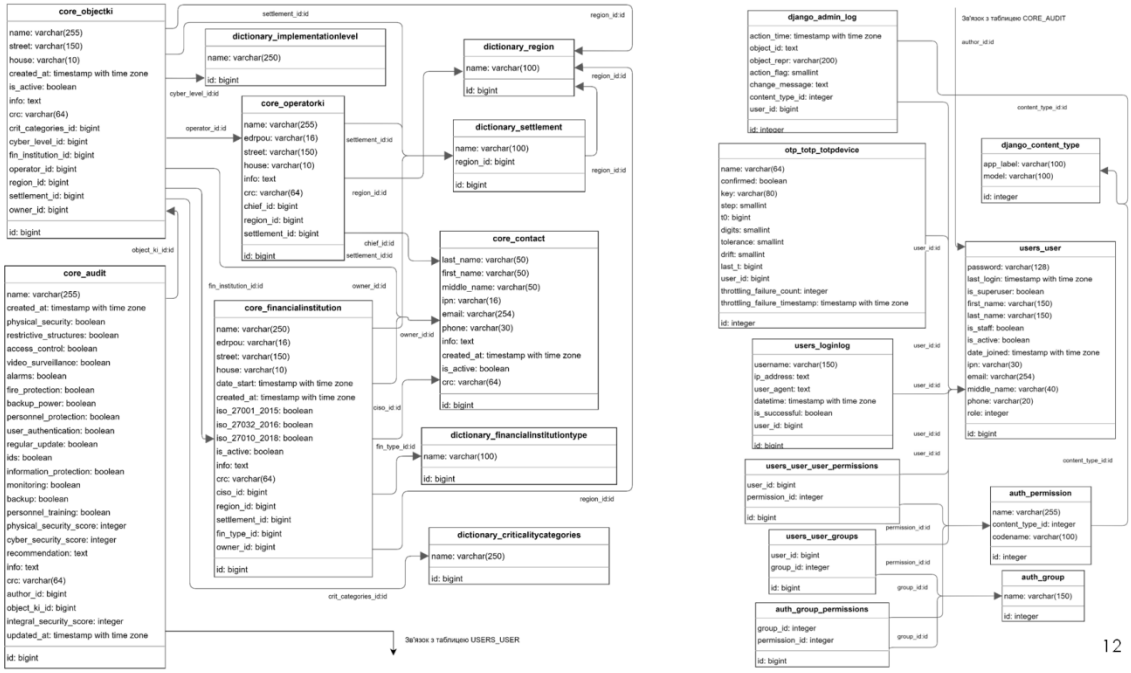
ВИКОРИСТАНІ ТЕХНОЛОГІЇ

UML-ДІАГРАМА КЛАСІВ



11

РЕАЛІЗОВАНА БАЗА ДАНИХ



12

ЗАХИСТ ІНФОРМАЦІЙНОГО РЕСУРСУ

РОЗРОБЛЕНО

- двофакторна автентифікація (2FA)
- розділення доступів згідно ролей
- контрольна сума запису
- журнал дій користувача
- журнал спроб входу в систему

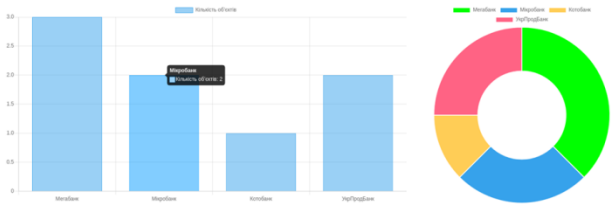
НАЛАШТОВАНО

- захист від міжсайтових сценаріїв XSS (Cross site scripting)
- захист від підробки міжсайтового запиту CSRF (Cross-site request forgery)
- захист від SQL-ін'єкції
- захист від клікджекінгу (Clickjacking)
- перевірка заголовка хосту (Host header check)
- політика реферрерів (HTTP referrer)
- політика відкриття між джерелами (Cross-origin opener policy)
- безпека сесії

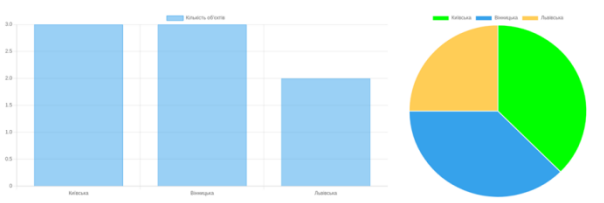
13

АНАЛІТИЧНІ ЗВІТИ (1 – 4)

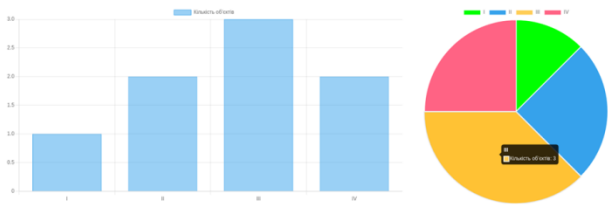
Рейтинг фінансових установ за кількістю об'єктів інфраструктури



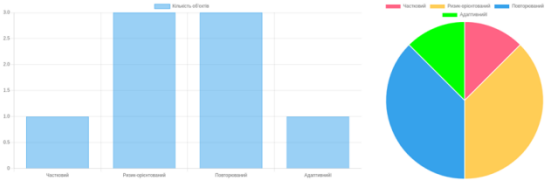
Рейтинг областей за кількістю об'єктів інфраструктури



Рейтинг об'єктів фінансової інфраструктури за категоріями критичності

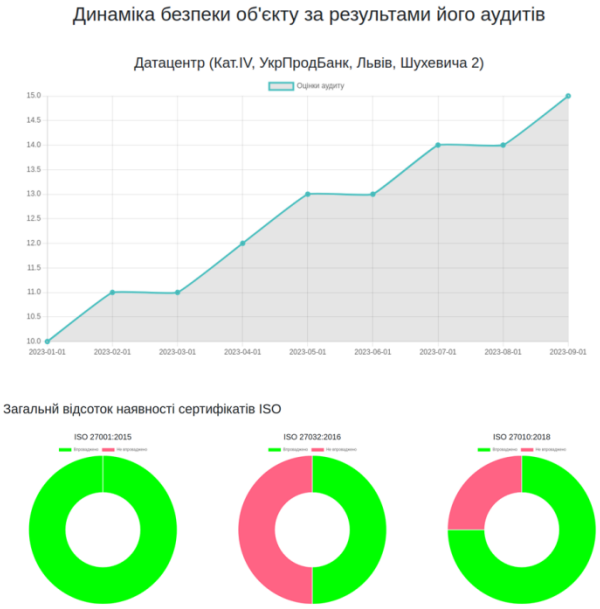


Рейтинг об'єктів фінансової інфраструктури за рівенем впровадження кіберзахисту



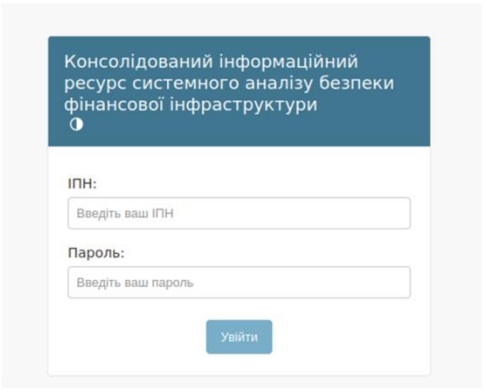
14

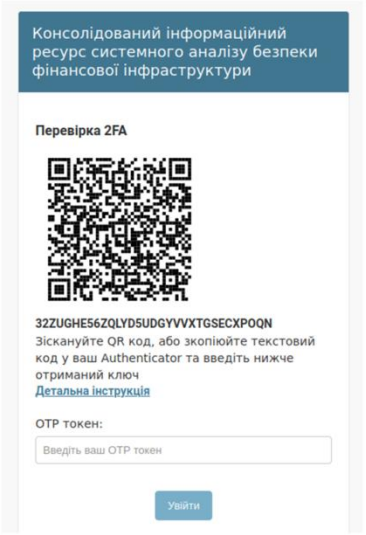
АНАЛІТИЧНІ ЗВІТИ (5 – 6)



15

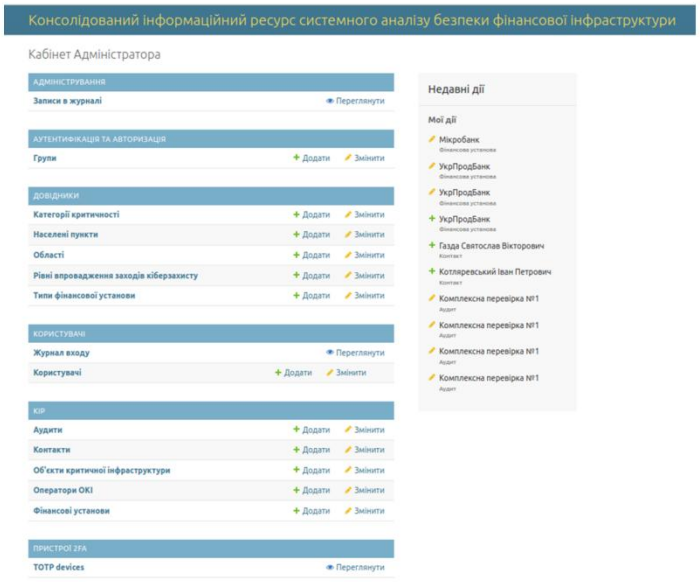
ІНТЕРФЕЙС – ВХІД І НАЛАШТУВАННЯ 2FA





16

ІНТЕРФЕЙС – КАБІНЕТ АДМІНІСТРАТОРА



17

ВИСНОВКИ

У магістерській роботі вперше розроблено захищений консолідований інформаційний ресурс для системного аналізу безпеки фінансової інфраструктури регіону, що дозволило аналізувати і покращити безпеку важливих об’єктів фінансової інфраструктури, а також має можливості для подальшого вдосконалення ресурсу.

Досліджено методи збору даних та вимоги до створення консолідованого інформаційного ресурсу для системного аналізу безпеки фінансової інфраструктури.

Розроблено архітектуру та функціонал консолідованого інформаційного ресурсу, базу даних, використовуючи метод сутність-зв'язок, визначено сутності та їх взаємозв'язки для упорядкування інформації про стан безпеки фінансової інфраструктури.

Здійснено реалізацію бази даних та розроблено необхідні програмні засоби для аналізу інформації про безпеку об’єктів фінансової інфраструктури з формуванням відповідних аналітичних звітів.

За тематикою роботи опубліковано **12** публікацій, зокрема,
5 статей у фахових виданнях та **7** тез доповідей на наукових конференціях.

18

Дякую за увагу!

Додаток Г. Протокол перевірки на антиплагіат

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Захищений консолідований інформаційний ресурс системного аналізу безпеки фінансової інфраструктури регіону

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 94 % Схожість 6 %

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Коваль Н.П. (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Яремчук Я.Ю. (прізвище, ініціали)

Керівник роботи _____ (підпис) Карпінець В.В. (прізвище, ініціали)