Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Оцінка ризиків інформаційної безпеки аутсорсингу в фінансовому секторі

Виконав: студент VI курсу, групи СБм-62
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

_____ Дисевич Д.О.
(підпис) (прізвище та ініціали)

Керівник _____ Стадник М.А.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Лечаченко Т.А.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Загородна Н. В.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Дисевичу Денису Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка ризиків інформаційної безпеки аутсорсингу в фінансовому секторі

Керівник роботи Стадник Марія Андріївна, к.т.н., доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » листопада 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 25 грудня 2023р.

3. Вихідні дані до роботи Наукові публікації про ризики безпеки в фінансовому секторі

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз сучасного стану оцінки ризиків інформаційної безпеки
Опис об'єкту аналізу, складові Аутсорсингу в фінансовому секторі
Оцінка ризиків інформаційної безпеки за допомогою ISSRM та BNBAG
Охорона праці та безпека в надзвичайних ситуаціях
Висновки
Перелік використаних джерел
Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульний слайд
Актуальність роботи
Цілі та завдання
Модель домену Управління ризиками безпеки інформаційної системи (ISSRM)
Метод BNBAG - Граф атаки на базі байєсівської мережі
Порівняння моделей ISSRM та BNBAG
Угода про аутсорсинг
Зберігання договору аутсорсингу
Рівень ризику та вразливості на етапі впровадження для аналізу ISSRM
Аналіз вразливостей за допомогою BNBAG
Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., кандидат технічних наук, зав. кафедри КС		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2023	*Виконано*
2.	Підбір наукових джерел про ризики безпеки в	26.11.2023-28.11.2023	*Виконано*
	фінансовому секторі		
3.	Опрацювання наукових публікацій та збір даних по	29.11.2023-1.12.2023	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	2.12.2023-4.12.2023	*Виконано*
	роботи		
5.	Оформлення розділу «Аналіз сучасного стану	5.12.2023-7.12.2023	*Виконано*
	оцінки ризиків інформаційної безпеки»		
6.	Оформлення розділу «Опис об’єкту аналізу,	8.12.2023-10.12.2023	*Виконано*
	складові Аутсорсингу в фінансовому секторі»		
7.	Оформлення розділу «Оцінка ризиків	11.12.2023-13.12.2023	*Виконано*
	інформаційної безпеки за допомогою ISSRM		
	та BNBAG»		
8.	Виконання завдання до підрозділу «Охорона праці»	14.12.2023-15.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.12.2023-17.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	18.12.2023-19.12.2023	*Виконано*
11.	Нормоконтроль	19.12.2023-20.12.2023	*Виконано*
12.	Перевірка на плагіат	21.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи		

Студент _____ Дисевич Д.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Стадник М.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Оцінка ризиків інформаційної безпеки аутсорсингу в фінансовому секторі // Кваліфікаційна робота освітнього рівня «Магістр» // Дисевич Денис Олегович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2023 // С. 74, рис. – 11, табл. – 11, додат. – 1, бібліогр. – 47.

Ключові слова: РИЗИК, ІНФОРМАЦІЙНА БЕЗПЕКА, АУТСОРСИНГ, ФІНАНСИ, ОЦІНКА, УПРАВЛІННЯ.

У роботі було показано, як можна застосувати методи оцінки ризиків інформаційної безпеки в аутсорсинговій системі фінансової установи. Оцінка ризиків є частиною управління ризиками.

Метод ISSRM був обраний як метод управління ризиками, тоді як метод BNBAG служить імовірнісним методом оцінки ризиків. Ці два методи були застосовані в тематичному дослідженні, щоб зрозуміти їх схожість і різницю на практиці. Аутсорсинг був обраний як контекст для реалізації двох методів. Аутсорсинг є однією з головних проблем у фінансовому секторі.

Було представлено результати двох оцінок. Застосування методів оцінки ризику інформаційної безпеки реального процесу дало розуміння необхідності вдосконалення в цій галузі. Надано пропозицію щодо поєднання методу управління ризиками безпеки та імовірнісного методу.

ANNOTATION

Assessment of Information Security Risks of Outsourcing in the Financial Sector // The educational level "Master" qualification work // Denys Dysevych // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, SBm-62 group // Ternopil, 2023 // P. 74, fig. - 11, tables – 11, annexes - 1, ref. - 47.

Key words*:* RISK, INFORMATION SECURITY, OUTSOURCING, FINANCE, ASSESSMENT, MANAGEMENT.

The paper showed how to apply information security risk assessment methods in the outsourcing system of a financial institution. Risk assessment is part of risk management.

The ISSRM method was chosen as a risk management method, while the BNBAG method serves as a probabilistic risk assessment method. These two methods were applied in a case study to understand their similarities and differences in practice. Outsourcing was chosen as the context to implement the two methods. Outsourcing is one of the main problems in the financial sector.

The results of two assessments were presented. The application of information security risk assessment methods of a real process gave an understanding of the need for improvement in this area. A proposal for combining the security risk management method and the probabilistic method is provided.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BN (англ. Bayesian Network) – Байєсова мережа.

BNBAG (англ. Bayesian Network Based Attack Graph) – Граф атаки на базі байєсівської мережі.

BPMN (англ. Business Process Modelling Notation) – Нотація моделювання бізнес-процесів.

COSO (англ. Committee of Sponsoring Organizations of the Treadway Commission) – Комітет організацій-спонсорів Комісії Тредвея.

CWE (англ. Common Weakness Enumeration) – Перелік загальних недоліків.

DAG (англ. Directed Acyclic Graph) – Спрямований ациклічний граф.

DDoS (англ. Distributed Denial of Service) – розподілена відмова в обслуговуванні.

EBA (англ. European Banking Authority) – Європейське банківське управління.

ENISA (англ. European Union Agency for Network and Information Security) – Агентство Європейського Союзу з мережевої та інформаційної безпеки.

FAIR (англ. Factor Analysis of Information Risk) – Факторний аналіз інформаційного ризику.

FSA (англ. Financial Stability Authority) – Управління фінансової стабільності.

IEC (англ. International Electrotechnical Commission) – Міжнародна електротехнічна комісія.

IRAM (англ. Information Risk Assessment Methodology) – Методологія оцінки інформаційних ризиків.

IS (англ. Information System) - Інформаційна система.

ISO (англ. International Organization for Standardization) – Міжнародна організація зі стандартизації.

ISSRM (англ. Information System Security Risk Management) – Управління ризиками безпеки інформаційної системи.

MiFID (англ. Markets in Financial Instruments Directive) – Директива про ринки фінансових інструментів.

NIST (англ. National Institute of Standards and Technology) – Національний інститут стандартів і технологій.

NPT (англ. Node Probability Table) – Таблиця ймовірності вузла.

OCTAVE (англ. Operationally Critical Threat, Asset, and Vulnerability Evaluation) – Операційно критична оцінка загроз, активів і вразливостей.

OWASP (англ. Open Web Application Security Project) – Відкритий проект безпеки веб-додатків.

PSD2 (англ. Payment Services Directive 2) – Директива про платіжні послуги.

ЗМІСТ

ВСТУП

Актуальність теми. Оцінка ризику інформаційної безпеки у фінансовій установі важлива для розуміння ризику конфіденційності, цілісності та доступності активів. Визнається, що безпека третіх сторін набуває все більшого значення для організацій фінансового сектора. Фінансова установа прагне забезпечити інформацію під час обґрунтування бюджетних рішень. На жаль, загальновживані методи залежать від оціночних суджень та індивідуальних запевнень, що обмежує їхнє відображення існуючої невизначеності в реальності. Це проблема, оскільки організації не хочуть виділяти ресурси на безпеку без точної оцінки свого ризику. Розробка методів та засобів виявлення ризиків інформаційної безпеки є актуальним завданням на сьогоднішній час.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є розробка методів оцінки ризиків інформаційної безпеки аутсорсингу в фінансовому секторі. Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати стан досліджень в області оцінки ризиків інформаційної безпеки.

– Проаналізувати об’єкт аналізу, складові аутсорсингу в фінансовому секторі.

– Оцінити ризики інформаційної безпеки аутсорсингу в фінансовому секторі

– Повести порівняльний аналіз ризиків та методик їх оцінки.

Об’єкт дослідження система аутсорсингу в фінансовій сфері.

Предмет дослідження. методи аналізу ризиків.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримали подальший розвиток методи оцінки ризиків, зокрема при їх застосування в сфері фінансів.

Практичне значення одержаних результатів. Виконано аналіз ризиків аутсорсингу в фінансовій сфері із застосуванням поєднання двох методів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XI науково-технічній конференції «інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2023 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у одній праці конференції.

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 47 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 74 сторінки, який містить __ рисунків та __ таблиць.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цей розділ присвячений сучасному стану оцінки ризиків інформаційної безпеки. Представлено огляд існуючих стандартів управління ризиками. Два методи – ISSRM та BNBAG – описані детально, оскільки вони є предметом цієї роботи. Пояснюються процеси збору даних, методи розрахунку результату та значення результатів цих методів. Порівняння цих методів включено, щоб відобразити подібності та відмінності між двома методами.

1.1 Стандарти та основи управління ризиками інформаційної безпеки

Організаціям доступна низка стандартів і структур управління ризиками інформаційної безпеки.

По-перше, ISO/IEC 27005 [15], який є одним із стандартів ISO/IEC 2700x [16], є стандартом управління ризиками інформаційної безпеки. Оцінка ризику складається з ідентифікації, аналізу та оцінки ризику [7].

По-друге, NIST розробив свій стандарт управління інформаційними ризиками під назвою NIST 800-30 «Посібник з управління ризиками для систем інформаційних технологій» [17]. Він відомий своєю гнучкістю; тому його прийняли низка організацій. Існують інші доступні стандарти та рамки оцінки ризику, наприклад підхід FAIR [18], фреймворк OCTAVE Allegro [19], фреймворк COSO [20]. Незважаючи на це, ISO/IEC 27005 і NIST 800-30 є найвідомішими.

Робота зосереджена на оцінці ризиків інформаційної безпеки у фінансовій установі. Переглянувши відповідну літературу, ми зрозуміли, що для фінансових установ немає конкретного стандарту або основи управління ризиками інформаційної безпеки. Консультативний центр фінансового сектору Світового банку [21] видав документ із переліком низки відповідних документів, що стосуються фінансового сектору, які наголошують на питаннях оцінки ризиків безпеки та пропонують інструкції.

Класифікація методів оцінки ризиків інформаційної безпеки.

Метод оцінки ризиків інформаційної безпеки повинен мати характеристики, які описують кожен із наступних чотирьох класів [14]:

- Якісні, кількісні або гібридні – різні за своїми вхідними та вихідними вимогами.

- Керований активами, керований послугами або керований бізнесом – фокусується на іншому рівні організації.

- Горизонтальні або вертикальні – різні за оцінкою ресурсів.

- Нерозповсюджені або розповсюджені – різні за своїм підходом до поширення атак.

Методи ISSRM і BNBAG були зіставлені за допомогою категоризації, щоб зробити їх порівнянними з іншими методами.

1.2 Методи управління ризиками безпеки інформаційних систем

Метод ISSRM [8] є методом управління ризиками інформаційної безпеки. Це допомагає зрозуміти, які активи є цінними та потребують захисту від певних загроз. Крім того, він представляє варіанти лікування ризику за допомогою запропонованих заходів безпеки. Він пропонує модель домену, показники та процес для управління ризиками. Перша причина, чому було обрано ISSRM, полягає в його якісному характері, який відрізняється від іншого методу. Друга причина пов’язана з її схожістю з Методологією оцінки інформаційних ризиків 2 (IRAM 2).

Спочатку вважалося, що IRAM 2 буде проаналізовано, оскільки він раніше використовувався у фінансовій установі. ISSRM має подібні характеристики та елементи порівняно з IRAM 2, отже, це прийнятна альтернатива для використання.

Модель предметної області.

Модель предметної області ISSRM [8] була розроблена шляхом дослідження стандартів і методів управління ризиками безпеки. Модель домену для ISSRM, представлена на рис. 1.1., містить три групи концепцій: концепції,

пов’язані з активами, концепції, пов’язані з ризиком, і концепції, пов’язані з обробкою ризиків, які позначені відповідно жовтим, червоним і зеленим.

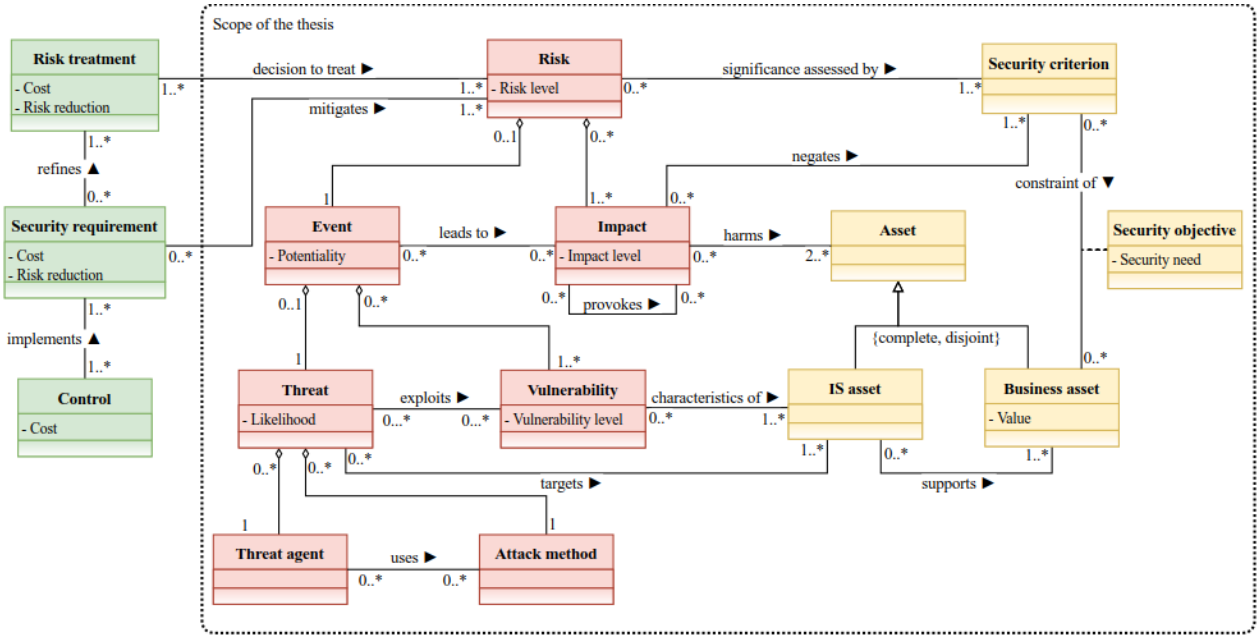

Рисунок 1.1 – Модель домену ISSRM (адаптовано з [11]).

Концепції, пов’язані з активами, підкреслюють, які активи важливо захищати відповідно до потреб безпеки системи. Активи – це або бізнес-активи, або активи інформаційної системи (IS). Бізнес-актив — це будь-яка інформація, процес або навички, необхідні організації для досягнення її бізнес-цілей. Він характеризується критерієм безпеки конфіденційності, доступності або цілісності. Активи інформаційної системи є цінними частинами IS, оскільки вони забезпечують підтримку бізнес-активів. Друга група — це концепції, пов'язані з ризиком, які ілюструють ризик та його складові. Ризик описується як загроза, яка може використовувати одну або кілька вразливостей, що призводить до впливу, який завдає шкоди двом або більше активам і скасовує критерій безпеки. Загроза – це комбінація агента загрози та методу атаки. Концепції, пов’язані з обробкою ризику, описують, як ставитися до ризику на основі знання існуючих засобів контролю, які реалізують вимоги безпеки та засоби, які зменшують ризик.

Обробка ризику – це рішення щодо уникнення, зменшення, передачі чи збереження ризику. Концепції, пов'язані з лікуванням ризиків, не входять до сфери дисертації.

Метрики

Метод ISSRM пропонує кілька метрик. По-перше, метрика вартості описує вартість бізнес-активу з урахуванням потенційного впливу, якщо бізнес-актив буде розкрито, модифіковано або зруйновано. По-друге, метрика потреби в безпеці виражає важливість критерію безпеки щодо бізнес-активу. Ці два показники описують концепції, пов'язані з активами. По-третє, метрика ймовірності описує ймовірність атаки з урахуванням мотивації супротивника та складності методу атаки. Показник рівня вразливості описує поширеність уразливості та ймовірність використання.

Потенціал обчислюється за допомогою показників рівня ймовірності та рівня вразливості, представлених у рівнянні 1.1.

Показник рівня впливу – це максимальне значення, яке призначається показнику потреби безпеки.

$$\text{Потенційність} = \text{Імовірність} + \text{Вразливість} - 1 \qquad (1.1)$$

Показник рівня ризику розраховується як добуток потенційності та рівня впливу. Він розраховується відповідно до рівняння 1.2.

Ці п'ять показників описують концепції, пов'язані з ризиком.

$$\text{Рівень ризику} = \text{Потенціал} \times \text{Вплив} \qquad (1.2)$$

У концепціях, пов'язаних з обробкою ризику, обробка ризику та вимоги до безпеки оцінюються з використанням зменшення ризику та вартості. Контролі оцінюються з точки зору вартості.

Процес ISSRM.

Процес ISSRM (Рис. 2) [8] представляє дії з управління ризиками інформаційної безпеки. Він починається з розуміння контексту, в якому працює організація, і визначення її бізнесу та активів IS. Наступним кроком є визначення цілей безпеки з точки зору конфіденційності, цілісності та доступності на основі рівня захисту, необхідного для активів. Тоді ризик аналізується та оцінюється.

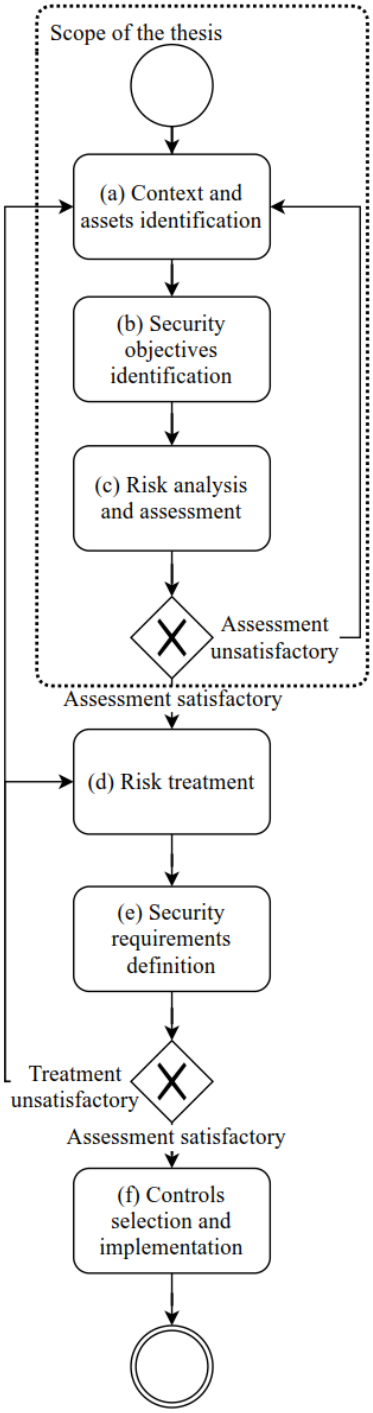

Рисунок 1.2 – Процес ISSRM [11]

Після цих заходів вирішується, задовільна оцінка чи ні. Ці попередні кроки можна повторити у разі незадовільних результатів. Наступний крок стосується лікування ризику: уникати, зменшувати, передавати чи приймати ризик. Потім необхідно визначити вимоги безпеки, щоб визначити необхідні умови безпеки для досягнення бажаного рівня безпеки на основі ідентифікованих ризиків.

Якщо лікування виявилося незадовільним, тоді весь процес можна розпочати спочатку або з етапу лікування ризику. Останній крок стосується

вибору та впровадження елементів керування на основі вимог безпеки. Перші три кроки формують оцінку ризику; таким чином, вони розглядаються в тематичному дослідженні дисертації. Обробка ризиків, визначення вимог безпеки та засоби контролю залишаються поза увагою дослідження. Моделювання загроз і вразливостей.

Частиною процесу ISSRM є аналіз і оцінка ризиків. Метод ISSRM розглядає ризик як успішне використання вразливості загрозою, що призводить до впливу, який завдає шкоди активу, і скасовує критерій безпеки відповідно до моделі домену. Тому було змодельовано загрози та вразливі місця. Загрози можна моделювати відповідно до таксономії, напр. Таксономія MI-TRE ATT&CK [22]; Threat Agent Library від Intel Corporation [23] або іншої.

Вибрана таксономія видана Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA) [24], оскільки він класифікує загрози, подібні до категоризації в IRAM 2.

Таксономія ENISA класифікує загрози на наступні класи [24]:

- Ненавмисна шкода, що відноситься до втрати конфіденційності, цілісності або доступності активів через помилки або помилки.

- Катастрофа, яка сталася через природні чи екологічні сили.

- Збої або несправності, які відбуваються без будь-якої причини.

- Збої, які виникають через недоступність ресурсів без їх атаки.

- Навмисний фізичний напад, який стосується фізичного збитку активів людьми.

- Мерзенна діяльність, яка вказує на будь-яку зловмисну або образливу діяльність щодо інформаційних систем.

- Перехоплення, яке є навмисною атакою на інформаційну систему з метою зміни зв'язку.

По-друге, доступні списки вразливостей, напр. MITER Common Vulnerabilities and Exposures [25] або NIST National Vulnerability Database repository [26]. Обрана таксономія для моделювання вразливостей – OWASP Top 10 (2017), оскільки вона використовувалася фінансовою установою раніше.

Огляд 10 найкращих категорій OWASP представлено в наступному списку [27]:

- Ін’єкція – агент загрози може надіслати шкідливий код інтерпретатору.

- Порушена автентифікація – система має недоліки автентифікації.

- Розкриття конфіденційних даних – дані не захищені відповідно до потреб.

- Зовнішні сутності XML – програма аналізує вхідні дані xml.

- Порушений контроль доступу – користувач системи може діяти відповідно до інших дозволів, ніж призначено.

- Неправильна конфігурація безпеки – агент загрози може отримати доступ до системи через відсутність належної конфігурації.

- Міжсайтовий сценарій – шкідливий код може бути запущений агентом загроз у браузері іншого користувача.

- Незахищена десеріалізація – під час перебудови формату даних в об’єкт використовується ненадійний ввід користувача.

- Використання компонентів із відомими вразливими місцями – відомі вразливості не виправляються.

- Недостатня реєстрація та моніторинг – агент загрози може досягти мети, навіть не будучи виявленим через відсутність реєстрації та моніторингу систем.

Певні вразливості було вибрано з категорій і скориговано відповідно до характеру дослідження. Огляд вразливостей наведено в таблиці 1.1

1.3 Метод графів атак на основі Байєсівських мереж.

Метод BNBAG [9, 10] — це імовірнісний метод оцінки ризику. Байєсова мережа (BN) використовується для моделювання та аналізу графіка атак. Причина, чому BNBAG використовується як підхід до моделювання ризику інформаційної безпеки, полягає в його відмінності від моделі ISSRM. Фінансова установа, щодо якої проводиться дослідження, висловила зацікавленість у потенційній кількісній оцінці деяких частин ризиків інформаційної безпеки. Оскільки фінансова установа не може надати повні дані для аналізу, підходящим є гібридний метод, наприклад BNBAG.

Таблиця 1.1 – Вразливості, які підлягали аналізу

OWASP category	Vulnerability	ID	Sample size	Mean	Standard deviation	Likelihood of exploit
Injection	SQL Injection	CWE89	11929	458,81	976,54	High
Broken authentication	Improper Authentication	CWE287	4258	163,77	486,42	High
Sensitive data exposure	Cleartext Transmission of Sensitive Information	CWE319	5782	222,38	690,75	High
XXE	XML External Entity Injection (XXE)	CWE611	9658	371,46	1035,29	High
Broken access control	Improper Authorization	CWE285	2641	101,58	252,03	High
Security misconfiguration	Security Misconfiguration	CWE16	28526	1097,15	3985,01	High
Cross-site scripting	Cross-Site Scripting (XSS)	CWE79	28503	1096,27	2033,40	High
Insecure deserialization	Deserialization of Untrusted Data	CWE502	-	-	-	Medium
Using components with known vulnerabilities	Using Components with Known Vulnerabilities	CWE937	1624	62,46	183,56	Medium
Insufficient logging and monitoring	Insufficient Security Logging	CWE778	446	17,15	71,79	Medium
Number of tested applications			120847			

Теорія ймовірностей Байєса.

Теорема ймовірностей Байєса надає версію для обчислення умовних ймовірностей. Імовірнісне міркування Байєса починається з гіпотези H, для якої ймовірність гіпотези P(H) називається попереднім переконанням щодо H.

Докази E використовуються для перегляду переконань щодо H за допомогою ймовірності доказів P (H|E). Розраховано заднє переконання щодо H у світлі доказів [9].

Теорема Байєса стверджує, що ймовірність гіпотези за наявності доказів дорівнює ймовірності доказів за умови гіпотези, помноженої на ймовірність гіпотези, поділеної на ймовірність доказів [28]. Теорема Байєса представлена в наступному рівнянні 1.3 [28]:

$$P(H|E) = \frac{P(E|H) \times P(H)}{P(E)} \quad (1.3)$$

де P(H) – попереднє переконання щодо H;

P(E) – ймовірність доказів;

P(E|H) – ймовірність доказів E;

P (H|E) – альтернативне переконання щодо H.

Є ситуації, коли немає інформації про P(E), тоді маргіналізація, тобто сума ймовірностей усіх подій, може бути використана за рівнянням 1.4 [9]:

$$P(E) = \sum_h P(E, H) \quad (1.4)$$

де P (E) – ймовірність доказів;

P(E,H) – ймовірність доказів та ймовірність гіпотези.

Теорема Байєса дозволяє оновлювати та змінювати оцінки, якщо були зібрані нові дані. Якщо існує сильна попередня віра в істинність певної гіпотези, то після отримання додаткових даних, які не підтверджують цю гіпотезу, теорема Байєса віддасть перевагу альтернативній гіпотезі, яка краще пояснює дані [9].

Графи атак

Граф атак із структурою дерева забезпечує корисну структуру для представлення вразливостей інформаційної системи та залежностей між ними. Графік атак показує можливі вектори атак для компрометації заданої цілі шляхом успішного послідовного використання вразливостей [10].

Усі вразливості, які формують вектор атаки, мають бути успішно використані. Для досягнення головної мети в системі може бути кілька шляхів атаки. Логічні графи атак базуються на принципі монотонності, тобто коли зловмисник отримав привілеї, ніхто їх не віддасть [10].

Монотонність вводить DAGs, тобто існує спрямований некруговий рух між структурою вузлів [9]. Простий приклад графа DAG представлено на рис. 1.3.

Дуги від A до B, від B до D і від C до D означають, що існує спрямована причинна залежність A від B і B від D, і C на D. Не може бути дуги від D до A через ациклічну структуру графа.

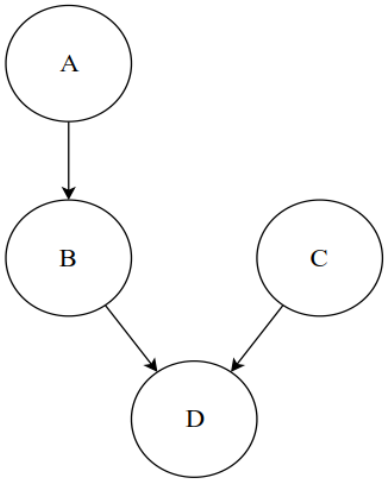

Рисунок 1.3 – Приклад структури DAG Виникнення події в дереві атаки моделюється імовірнісним чином

Ці моделі містять один або багато параметрів, значення яких відомі лише з невизначеністю [29]. Граф атак класифікується як якісна модель, оскільки він розглядає інформаційну систему як безпечну чи ні [30].

Процес BNBAG BN - це набір змінних, представлених у вигляді вузлів, і прямі залежності між краями цих вузлів. Він має форму DAG і має набір таблиць ймовірності вузла (NPT) [9]. Процес оцінки ризиків інформаційної безпеки за допомогою BNBAG представлено на рис. 1.4. Він складається з наступних кроків:

– ідентифікація можливого набору вразливостей у системі;

– створення вузлів уразливості, тобто спрямованих дуг між вузлами, де поява експлойта обумовлена експлойтом попереднього;

– специфікація NPT для кожного вузла вразливості;

– міркування та обчислення.

Етапи ідентифікації вразливостей (перший етап) і створення спрямованих дуг між ними (другий етап) було виконано відповідно до таксономії OWASP Top 10, представленої в описі процесу ISSRM.

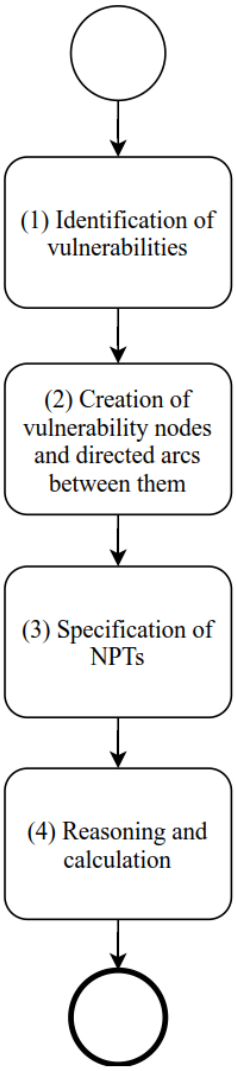

Рисунок 1.4 – BNBAG процес

Третій крок стосується NPT. NPT — це таблиця ймовірностей, яка представляє розподіл ймовірностей вузла з урахуванням його батьків [9]. NPT включають умовний розподіл ймовірностей, який є інформацією про кожен вузол у BNBAG. є вузлом, представляє батьківський вузол(и) і є ймовірністю

того, що вузол стане успішним, враховуючи стан його батьківського вузла(ів) [10].

Згідно з рис. 1.3., NPT для D є розподілом ймовірностей D, заданим множиною батьків D, якими є B і C; NPT B — це розподіл ймовірностей B з урахуванням його батьківського вузла A. Якщо вузол не має батьків, NPT — це просто розподіл ймовірностей цього вузла. На рис. 1.3 вузол A і вузол C не мають жодних батьків, тому NPT A є розподілом ймовірностей A, а NPT C є розподілом ймовірностей C. Будь-яка пара змінних, які не пов’язані одна з одною, вказують незалежність між ними.

Четвертий крок стосується обчислення результату. При оцінці ризику інцидент може статися, лише якщо використано одну або декілька вразливостей.

Рівняння 1.5. вказує, що якщо інцидент є істинним, якщо вразливість є істинною, то це дорівнює ймовірності вразливості. Рівняння 1.6 показує, що якщо в системі немає вразливостей, то інциденту немає. Рівняння 1.7. вказує на те, що якщо існує експлуатація вразливості, то інциденту потенційно не може бути. Рівняння 1.8 вказує, що якщо немає вразливостей, то немає інцидентів. Щоб обчислити NPT для інциденту, наступні рівняння 1.6-1.9 використовуються всередині комірок NPT:

$$P(Incident=T|Vulnerability=T)=P(Vulnerability) \quad (1.5)$$

$$P(Incident=T|Vulnerability=F)=0 \quad (1.6)$$

$$P(Incident=F|Vulnerability=T)=1-P(Vulnerability) \quad (1.7)$$

$$P(Incident=F|Vulnerability=F)=1 \quad (1.8)$$

Таким чином, ймовірність інциденту в системі є ймовірністю того, що принаймні одна з вразливостей стане використаною. Рівняння 1.9. описує ймовірність інциденту:

$$P(Incident=T)=1 - \prod P(vulnerabilities=F) \quad (1.9)$$

BN можна побудувати якісно, автоматично з даних або використовуючи їх комбінацію. Побудова графіків атак і обчислень може бути трудомістким, оскільки вимагає багато навичок, досвіду та творчості. Крім того, спілкування між експертами має бути інтенсивним і продуктивним [31].

Позитивним є те, що коли конструкція буде готова, параметри BN можна постійно оновлювати в міру надходження нової інформації.

1.4 Порівняння ISSRM і BNBAG.

Методи ISSRM і BNBAG мають схожість і відмінності в процесі оцінки ризику, концепціях, які використовуються, меті та змінних. Для опису цієї інформації та загального огляду складено три таблиці.

Таблиця 1.2. зроблена для порівняння методів у контексті їхнього процесу, згідно з рис. 1.2. та рис. 1.4.

По-перше, процес ідентифікації бізнес-активів та активів ІБ та визначення цілей безпеки в ISSRM виконується для визначення обсягу відповідних активів. BNBAG не розглядає активи, натомість визначаються відповідні вразливості, які описуються ідентифікацією вразливостей.

По-друге, аналіз і оцінка ризиків проводяться для визначення відповідних агентів загрози та методів їх атаки, які використовуються для використання однієї або багатьох вразливостей, що призводить до впливу на компанію.

Причиною цього етапу є обчислення рівня ризику відповідно до ISSRM. У BNBAG друга фаза виконується шляхом створення вузлів уразливості, створення дуг між умовними вузлами атаки, визначенням NPS та обчисленням ймовірності інциденту. Причиною цього етапу є аналіз вразливостей для розрахунку ймовірності використання вразливості.

Таблиця 1.2 – Порівняння процесів ISSRM та BNBAG

Огляд процесу	ISSRM	BNBAG
Визначення обсягу оцінки ризику	(a) Ідентифікація активів бізнесу та ІБ (b) Визначення цілей безпеки	(1) Виявлення вразливостей
Визначення релевантного загрози та потенціал вразливості, розрахунок ризику	(c) Аналіз та оцінка ризиків	(2) Створення вразливості вузлів і спрямованих дуг між вузлами (3) Визначення NPT (4) Міркування та обчислення
Прийняття рішення про ризик лікування	(d) Обробка ризиків (e) Визначення вимог безпеки	-
Впровадження відповідних засобів контролю	(f) Контролює вибір і впровадження	-

Хоча два методи досить різні за своєю природою, це відображення використовується в дипломній роботі для подальшого аналізу. ISSRM – це метод управління ризиками, тому обробка ризиків і вибір засобів контролю розглядаються як частина процесу. Обробка ризиків і визначення вимог безпеки здійснюються для прийняття рішення щодо планів обробки ризиків.

Крім того, ISSRM займається вибором і впровадженням засобів контролю, щоб прийняти рішення щодо відповідних засобів контролю для впровадження вимог безпеки, які зменшують ризик. Оскільки BNBAG є ймовірнісним методом оцінки ризику, він не розглядає обробку ризиків, вимоги безпеки чи засоби контролю як частину свого процесу.

Таблиця 1.3. являє собою порівняння між моделлю домену ISSRM і методом BNBAG.

Перша частина доменної моделі ISSRM складається з активів IS, бізнес-активів, які разом утворюють активи. Також вивчаються мета безпеки та критерій безпеки з точки зору конфіденційності, цілісності та доступності. Причина полягає в тому, щоб описати відповідні IS та бізнес-активи з точки зору їх потреби в конфіденційності (C), цілісності (I) і доступності (A).

Таблиця 1.3 – Порівняння моделей ISSRM та BNBAG

Огляд моделі	ISSRM	BNBAG
Пошук відповідних активів і визначення їхньої потреби в безпеці з точки зору конфіденційності, цілісності та доступності	IS актив Бізнес-актив Актив Мета безпеки Критерій безпеки	-
Визначення можливих агентів загроз, їх методи атаки та ймовірність успішної атаки	Агент загрози Метод нападу Загроза	Таблиця ймовірності вузла
Виявлення вразливостей та їх залежності одна від одної	Вразливість	Вразливі місця Залежності між вразливостями
Визначення ймовірності успішної атаки	Подія	Ймовірність інциденту
Визначення впливу можливої атаки	Вплив	-
Знаходження розміру ризику	Ризик	-
Вирішення щодо варіантів лікування ризику	Контроль лікування ризику	
Визначення необхідної безпеки	Вимоги безпеки	-

BNBAG не включає активи та їхню потребу в безпеці з точки зору C-I-A, що підлягає аналізу. Загроза в ISSRM визначається як особа або група людей з

певними атрибутами, напр. мотивація та спроможність, а також їхній метод атаки, який вказує на їхні дії, спрямовані на активи IS. Ці два домени поєднуються, що створює загрозу. BNBAG описує загрозу за допомогою таблиць ймовірності вузла, які описують ймовірність використання вразливості зловмисником, припускаючи її існування в системі.

BNBAG не розглядає загрозу з точними атрибутами. Уразливість у ISSRM — це слабка сторона активу ІБ, яка може бути використана загрозою.

У BNBAG основна увага зосереджена на визначенні вразливостей системи або процесу та різних залежностей між визначеними вразливими місцями. Подія в ISSRM — це успішне використання вразливості загрозою. BNBAG описує подібну ситуацію з ймовірністю інциденту, яка є ймовірністю успішного використання вразливості.

BNBAG не має інших частин у своїй моделі для оцінки ризику інформаційної безпеки. Модель предметної області ISSRM набагато багатша в цьому сенсі, оскільки в оцінку ризику включено ряд компонентів. Вплив — це потенційний результат у вигляді втрат після успішної атаки. Ризик — це як подія, так і її відповідний вплив. Коли ризик виявлено, вирішується, як його лікувати на основі знання існуючих засобів контролю, які реалізують вимоги безпеки. ISSRM і BNBAG використовують змінні в процесі оцінки ризику.

Порівняння змінних представлено в таблиці 1.4.

ISSRM використовує метрику цінності та потреби в безпеці для визначення вартості бізнес-активу з точки зору конфіденційності, цілісності та доступності. BNBAG не враховує показники, пов’язані з активами. ISSRM використовує ймовірність для визначення ймовірності загрози.

BNBAG явно не використовує жодних змінних для опису загрози. ISSRM використовує метрику рівня вразливості для визначення рівня слабкості. BNBAG також використовує вразливості для опису ймовірності виявлення певних слабких місць у системі, які можуть бути використані. ISSRM розраховує потенціал для опису ймовірності виникнення загрозливої події.

BNBAG використовує ймовірність для оцінки ймовірності того, що вразливість буде використана загрозою. ISSRM використовує рівень впливу для визначення впливу успішної події загрози. BNBAG не розглядає розрахунок впливу як частину процесу оцінки ризику. Основною метою ISSRM є обчислення рівня ризику, який описує ризик.

Таблиця 1.4 – Порівняння змінних ISSRM і BNBAG

Опис змінних	ISSRM	BNBAG
Вартість активів бізнесу та ІС	Вартість	-
Потреба безпеки активів	Потреба безпеки	-
Можливі ласощі, ймовірність їх ініціювання успішної атаки та їх сила Ймовірність	-	
Уразливості системи	Рівень уразливості	Уразливості
Імовірність успішної атакипроти системи	Потенційність	Ймовірність
Вплив успішної атаки	Рівень впливу	-
Величина ризику	Рівень ризику	Ймовірність інциденту
Вартість лікування ризику та обсяг зменшення ризику	Вартість лікування ризику Зниження ризику за рахунок лікування ризику	-
Вартість вимог до безпеки та обсяг зниження ризику	Вартість вимог до безпеки	Зменшення ризику через вимогу безпеки
Вартість контролю	Вартість контролю	-

Метою BNBAG є обчислення ймовірності інциденту, який описує ймовірність атаки на одну або багато вразливостей, виявлених в інформаційній системі, що призводить до ризику для організації. ISSRM також використовує

показники зниження вартості та ризику для опису обробки ризиків, вимог безпеки та засобів контролю.

BNBAG не розглядає обробку ризиків і засоби контролю як частину цього. Ці два методи можна порівняти з точки зору класифікації якісних, кількісних і гібридних підходів і таксономії, введеної Шамелі-Сенді та ін. [14]. Таблиця 1.5. представлена для короткого огляду класифікації методів ISSRM і BNBAG. Відмінні характеристики, які описують ці методи, також представлені в таблиці 1.5.

Наступні параграфи ілюструють, як ISSRM і BNBAG вписуються в таксономію, запропоновану Shameli-Sendi [14]. Оцінки ризиків інформаційної безпеки традиційно класифікуються як якісні, кількісні та гібридні [14]. Метод ISSRM є якісним методом, оскільки він використовує значення суб'єктивних суджень або змінні діапазону як вхідні дані для аналізу та результатів рангу ризиків. BNBAG є гібридним методом, оскільки він використовує чисельні чи суб'єктивні оцінки як вхідні дані для аналізу та виводить ймовірність інциденту, розраховану за допомогою статистики Байєса. Оцінка ризиків інформаційної безпеки може бути виконана з трьох точок зору, класифікованих як керована активами, керована послугами або керована бізнесом [14].

Таблиця 1.5 – Характеристики ISSRM та BNBAG

Характеристики	ISSRM	BNBAG
Оцінка	Якість	гібрид
Вхід/вихід	Діапазон/ранг	Немонетарний/немонетарний
Перспектива	керований активами	керований вразливістю
Оцінка ресурсів	V(I)+H(I)	H(D)
Вимірювання ризику	Нерозповсюджене	Розповсюджене
Техніка розрахунку	Операція множення	Байєсівський мережевий графік атак
Етапи оцінювання	(1) RA; (2) RE; (3) RR	(1) RA; (2) RE
Результат	Рівень ризику	Імовірність інциденту

Хоча ці три є найпоширенішими, ми також також пропонуємо перспективу, орієнтовану на вразливість. ISSRM містить концепцію, пов’язану з активами, концепцію, пов’язану з ризиком, і концепцію, пов’язану з обробкою ризику, включену в метод. Незважаючи на це, основна увага приділяється захисту активів з точки зору конфіденційності, цілісності та доступності.

BNBAG — це перспектива, орієнтована на вразливості, оскільки основна увага приділяється виявленню вразливостей і потенційного інциденту, коли одна або більше вразливостей були використані.

Оцінка ресурсів – це етап аналізу ризику, який визначає цінність ресурсів [14]. Вертикальна оцінка ресурсу враховує ступінь внеску ресурсу на верхні рівні. ISSRM оцінює активи як незалежні (V(I)) без внеску на інші рівні. Крім того, ресурси оцінюються незалежно (H(I)). BNBAG не розглядає активи як частину аналізу, але оцінює ресурси залежно (H(D)).

Останнім кроком оцінки ризику є вимірювання ризику, де розрізняють два типи вимірювань: нерозповсюджені та розповсюджені [14]. ISSRM розглядає вплив лише з точки зору втрати конфіденційності, цілісності або доступності одного активу, що є причиною того, чому цей тип методу не розповсюджується.

BNBAG є типом поширення, оскільки він використовує умовні ймовірності. Він вимірює ймовірність використання вразливості за умови успішного використання її батьків. Іншими характеристиками для опису методів є техніка розрахунку, етапи оцінки та результат. ISSRM використовує операцію множення для обчислення ризику як добутку впливу та ймовірності. BNBAG використовує байєсівський мережевий графік атак для розрахунку ймовірності успішного інциденту.

У BNBAG ризик – це стан невизначеності, розрахований за допомогою байєсівської теорії ймовірностей і характеристик графа атаки. Етапи оцінки ризику – аналіз ризику (RA), оцінка ризику (RE) і реагування на ризик (RR) – були детально описані в попередніх розділах. Метод ISSRM включає всі етапи, тоді як BNBAG не враховує RR.

Загалом, результатом методів, які мають відношення до цього дослідження, є рівень ризику та ймовірність інциденту.

1.5 Висновок до першого розділу

У цьому розділі представлені сучасні стандарти, рамки та методи оцінки ризиків інформаційної безпеки. По-перше, було надано огляд стандартів і структур управління ризиками інформаційної безпеки. По-друге, представлено можливу класифікаційну таксономію методів оцінки ризиків інформаційної безпеки. Основна увага в цій главі була зосереджена на огляді методів ISSRM і BNBAG в контексті їхніх процесів, моделей домену та показників. Надано інформацію про процеси збору даних, методи обчислення результатів і значення результатів. Порівняння ISSRM і BNBAG було зроблено як відображення між відповідними етапами, моделями домену та показниками цих методів. Крім того, ISSRM і BNBAG були порівняні в контексті таксономії класифікації, що допомагає порівняти їх також з іншими методами, які виходять за межі цієї дисертації. Подано огляд доступних стандартів, рамок і методів, які можна використовувати для оцінки ризиків інформаційної безпеки в організації.

2 ОПИС ОБ'ЄКТУ АНАЛІЗУ, СКЛАДОВІ АУТСОРСИНГУ В ФІНАНСОВОМУ СЕКТОРІ

У цьому розділі представлено приклад в контексті фінансової установи. Основна увага зосереджена на оцінці ризику інформаційної безпеки, який потенційно може характеризувати аутсорсинг. Впроваджено систему аутсорсингу та її складові. Крім того, аутсорсинг як бізнес-процес було змодельовано та візуалізовано, щоб дати загальне уявлення про його складність.

2.1 Аутсорсинг у фінансових установах

Сьогодні організації часто передають певні продукти чи послуги стороннім організаціям. Причини аутсорсингу можуть бути різними, напр. отримання доступу до кращих навичок, досвіду та технологій, нездатність надавати послуги всередині країни, бажання зосередитися на основних бізнес-процесах, оптимізація використання внутрішнього персоналу, зниження витрат і підвищення гнучкості [32]. Основною проблемою, пов'язаною з аутсорсингом, є обмежений контроль над послугами та рішеннями, розробленими або підтримуваними сторонньою організацією [33]. Через залежність між аутсорсинговою організацією і третім особами ризики, з якими стикається третя сторона, також можуть мати вплив на аутсорсингову організацію [33]. Фінансові установи є жорстко регульованими організаціями.

В Естонії, відповідно до глави 5 Закону про надзвичайні ситуації [34], постачальники платіжних послуг були внесені до списку життєво важливих постачальників послуг, що «є послугою, яка має величезний вплив на функціонування суспільства і переривання якої є безпосередня загроза життю чи здоров'ю людей або діяльності іншої життєво важливої служби чи служби загального інтересу» [34].

Фінансові установи повинні дотримуватися правил і норм. Треті сторони зазвичай нерегульовані, і вони можуть не розуміти важливості правил [35]. Відповідно до Базельського комітету з банківського нагляду [11], постачальник

фінансових послуг, який бажає передати низку послуг і рішень на аутсорсинг, відповідає за управління та моніторинг діяльності нерегульованої сторони. Тема аутсорсингу охоплена низкою нормативних актів, яких повинні дотримуватися фінансові установи, напр. Директива 2014/65/ЄС, відома як Директива про ринки фінансових інструментів (MiFID) [36], і Директива 2015/2366/ЄС, відома як Директива про платіжні послуги 2 (PSD2) [37].

Послуги, що надаються сторонніми постачальниками, можна класифікувати за такими категоріями: телекомунікації, безпека, управління даними, програмне забезпечення, апаратне забезпечення, автоматизація та послуги інформаційних систем. Постачальники телекомунікаційних послуг надають мережеві рішення WAN, загальні компоненти SWIFT, хостинг веб-сайтів, VoIP, доступ до Інтернету та лінії передачі даних. Служба безпеки, передана аутсорсингу, є рішенням для захисту організації від DDoS-атак. Деякі рішення, пов’язані з центром обробки даних, які належать до послуг управління даними, також були передані на аутсорсинг.

Розробка програмного забезпечення, яка була передана аутсорсингу, в основному пов’язана з розробкою та інтеграцією мобільних додатків. Крім того, деякі ліцензії на програмне забезпечення та підтримку було придбано у сторонніх постачальників, включаючи телефонні системи та хмарні служби. Так само було інтегровано кілька інших рішень PaaS, розроблених стороннім постачальником. Технічне обладнання було поставлено, а інформаційні системи розроблені та обслуговуються третіми сторонами.

Це приклади послуг, які передаються на аутсорсинг. Аутсорсинг як бізнес-процес описано в наступних розділах.

2.2 Система аутсорсингу та її компоненти.

Аутсорсинг — це відносини між аутсорсинговою організацією та зовнішньою третьою стороною для надання послуг і рішень, які в іншому випадку надавалися б самою аутсорсинговою організацією. Для майбутнього

аналізу ризиків інформаційної безпеки система аутсорсингу визначається як набір таких компонентів:

- Співробітники організації, які відповідають за виконання одного або багатьох завдань у контексті аутсорсингу, наприклад керівник проекту, власник контракту, кадровий персонал. - представник джерел, IT-спеціаліст, менеджер з інформаційної безпеки, комітет із закупівель, юрисконсульт, менеджер з операційного ризику, менеджер з відповідності тощо.

- Зовнішні сторони, які надають послуги або контролюють дотримання правових і нормативних вимог, або захищають інтереси працівників, наприклад постачальники послуг, Управління фінансової стабільності (FSA), профспілки.

- Інфраструктура, необхідна для спілкування сторін, наприклад служба електронної пошти.

- Інфраструктура, необхідна для зберігання інформації, така як система управління зберіганням контрактів і база даних документів.

- Інформація, якою обмінюються сторони, наприклад угода про аутсорсинг, план оцінки ризиків та багато іншого.

Загальна система аутсорсингу відносно складна. Вона потребує залучення, співпраці та комунікації значної кількості сторін, що підтримується відповідними потребами інфраструктури та застосуванням.

2.3 Цілі безпеки аутсорсингу.

Основна увага роботи зосереджена на інформаційній безпеці та важливості її підтримки в контексті стороннього аутсорсингу. Цілі інформаційної безпеки, які необхідно забезпечити, описуються наступним чином:

- Конфіденційність зберігається, коли дані захищені від несанкціонованого доступу.

- Цілісність зберігається, коли дані точні, не модифіковані чи змінені.

- Доступність зберігається, коли забезпечено доступ до даних для уповноважених осіб. Ці три цілі є найпоширенішими.

Фінустанова в даному випадку не має виняткових поглядів.

Загальний бізнес-процес аутсорсингу проілюстровано на рис. 2.1. Він розділений на п’ять етапів, які відрізняються кількістю та складністю завдань. Огляд із менш детальним уявленням про фази описано далі. Визначення можливостей — це перша фаза, під час якої вживаються початкові кроки для оцінки можливостей аутсорсингу. Керівник проекту створює область аутсорсингу, починає його перевірку та передає його юрисконсульту.

Рисунок 2.1 – Фази аутсорсингу

Юридичний радник розглядає обсяг, приймає рішення про його застосовність і чи повідомляти FSA. У разі потреби звертаються до FSA. FSA формує свою відповідь і надсилає її юридичному раднику, який передає загальну відповідь щодо застосовності керівнику проекту.

Якщо обсяг відхилено, керівник проекту повинен його поновити. Якщо обсяг застосовний, слід створити орієнтовний план проекту та бізнес-обґрунтування. Керівник проекту також розробляє початкову оцінку ризику та подає ініціацію процесу затвердження нового продукту. Останні два документи надаються менеджеру з операційного ризику або інформаційної безпеки.

Попереднє дослідження — це другий етап, під час якого створюється високорівневе рішення для аутсорсингу. Керівник проекту надсилає інформацію в відділ кадрів про майбутній аутсорсинг. Відділ кадрів вирішує, чи інформувати про це профспілки. Якщо вирішено повідомити профспілки, то інформація надсилається їм.

Керівник проекту також подає заявку на закупівлю, а комітет із закупівель вирішує, продовжувати чи ні. Якщо запит на купівлю схвалено, керівник проекту визначає інвентар додатків і визначає потреби в розробці. Підтримку слід запитувати у власника системи або менеджера з інформаційної безпеки. Також керівник проекту оновлює раніше створені документи.

Проектування та планування — це третя фаза, яка поділяється на фазу проектування процесу та фазу постачальника послуг. Фаза проектування процесу спрямована на розробку детального рішення для аутсорсингу. На цьому етапі керівник проекту разом із юрисконсультом починає складати угоду про аутсорсинг.

Також керівник проекту створює внутрішній план виходу та управління безперервністю бізнесу. Це робиться разом із підтримкою менеджера з операційного ризику. Крім того, керівник проекту разом із менеджером із відповідності створює плани комунікації, які описують, чи буде керуватися комунікацією з FSA і як саме.

Також керівник проекту оновлює раніше створені документи. Етап постачальника послуг важливий для аналізу можливих постачальників послуг і підготовки до наступного етапу. Керівник проекту аналізує можливих постачальників послуг і надсилає покупцеві угоду про аутсорсинг. Покупець зв'язується з постачальниками послуг і знайомить їх з угодою аутсорсингу. Зроблено вибір постачальника послуг. У випадку внутрішнього аутсорсингу керівник проекту передає юридичні документи представнику організації, який їх підписує.

Крім того, керівник проекту створює початковий план оцінки реалізації вартості, який оцінює фінансовий результат і перераховує ключових працівників, пов’язаних з аутсорсингом. Також оновлюються раніше створені документи. Впровадження — це четвертий етап, під час якого підписується угода про аутсорсинг і реалізується загальний процес аутсорсингу.

Цей етап був використаний в аналітичній частині дипломної роботи для проведення оцінки ризиків інформаційної безпеки за допомогою методів ISSRM та BNBAG. Причина полягає в тому, що в ньому представлені різні компоненти інформаційної системи, і це важливо в контексті аутсорсингу. Він розділений на підпроцеси, описані в розділі

Управління, контроль і звітність є останнім етапом аутсорсингу. Він описує наступні дії та наступні дії, коли угоду про аутсорсинг було підписано і обраний постачальник послуг почав надавати необхідні послуги та рішення для

суб’єкта аутсорсингу. Керівник проекту відстежує фінансові результати та документує відповідні відгуки, оновлює реалізацію вартості та створює ключові знання. Власник договору контролює виконання договору та роботу постачальника послуг.

Крім того, власник контракту несе відповідальність за моніторинг управління ризиками та пом’якшення, а також внутрішній план виходу та управління безперервністю бізнесу. Власник контракту повинен оцінити економічну життєздатність постачальника послуг. Власник реєстру щонайменше раз на рік складає звіти про аутсорсинг для контролю за виконанням контракту, фінансовим станом постачальника послуг, критичними інцидентами, ризиками та відповідними планами дій.

Ці звіти зберігаються в базі даних документів, доступ до якої мають уповноважені сторони. П'ять етапів разом утворюють бізнес-процес аутсорсингу.

Активи в системі аутсорсингу.

Впровадження представляє важливі внутрішні та зовнішні комунікаційні сторони, потреби в інфраструктурі для зв’язку та зберігання, а також інформацію, яка протікає через систему. Опис процесу майбутньої фази впровадження на основі внутрішнього довідника фінансової установи з аутсорсингу. Точність інформаційного потоку, взаємодіючих сторін, інформаційної системи та бізнес-активів було перевірено відповідальною особою фінансової установи.

Графи процесів на основі нотації моделювання бізнес-процесів (BPMN) були складені автором. Для моделювання бізнес-процесів використовувалося відкрите програмне забезпечення draw.io. Щоб полегшити аналіз, впровадження було розділено на чотири етапи, порядок яких показано на рис. 2.2.

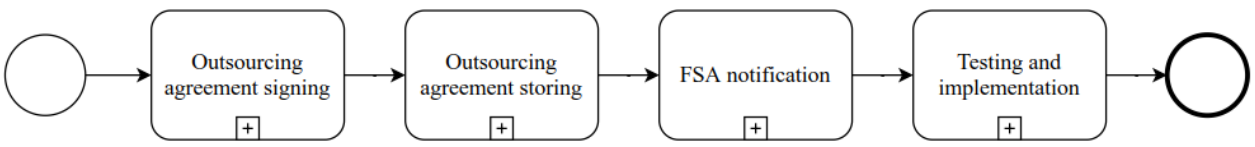

Рисунок 2.2 – Етапи впровадження

Перший етап, підписання угоди про аутсорсинг, детально описано на рис. 2.3 та рис. 2.4. Наступні кроки описують бізнес-процес підписання угоди про аутсорсинг керівником проекту, описаний на рис. 2.3.

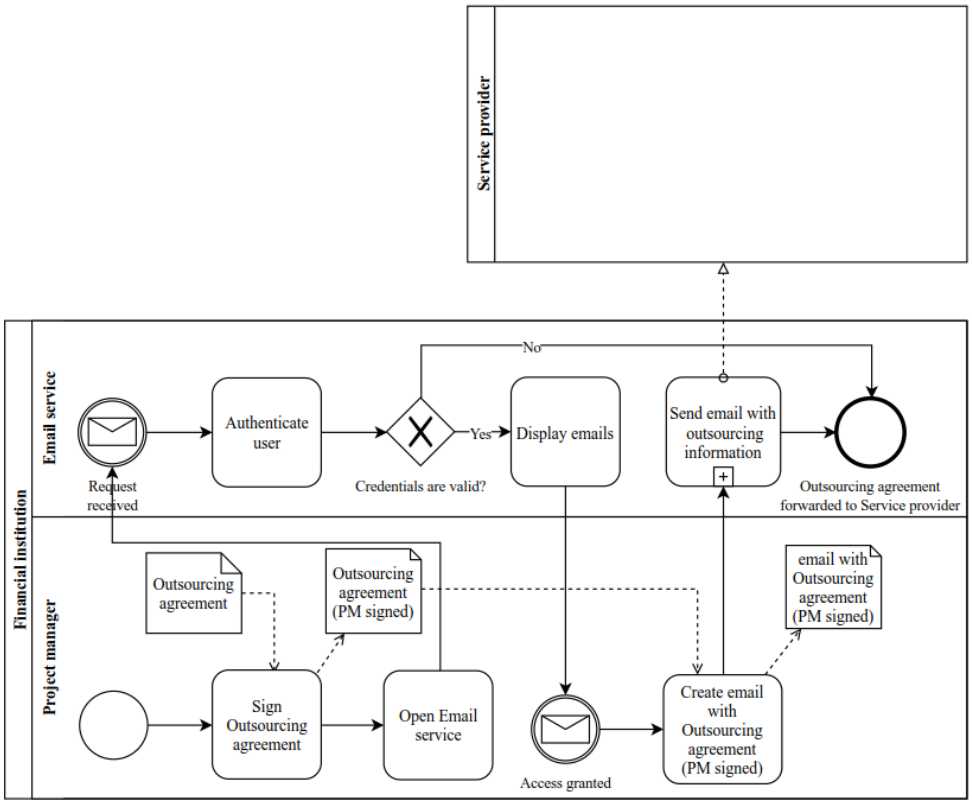

Рисунок 2.3 – Угода про аутсорсинг, підписана керівником проекту

Менеджер проекту (PM) підписує угоду про аутсорсинг, а керівник проекту відкриває службу електронної пошти. Сервіс електронної пошти отримує запит і аутентифікує користувача. Якщо облікові дані дійсні, електронні листи відображатимуться. Якщо облікові дані недійсні, доступ до служби електронної пошти не буде надано. Керівник проекту створює електронний лист із угодою про аутсорсинг (підписано PM).

Служба електронної пошти надсилає електронний лист із угодою про аутсорсинг (підписану PM) постачальнику послуг. Наступні кроки описують передачу угоди про аутсорсинг, підписаної обома сторонами, до керівника проекту. Це показано на рис. 2.4. Служба електронної пошти отримує електронний лист із підписаною угодою про аутсорсинг, зберігає його та повідомляє одержувача електронного листа. Керівник проекту отримує сповіщення та відкриває службу електронної пошти. Сервіс електронної пошти

отримує запит і аутентифікує користувача. Якщо облікові дані дійсні, завантаження електронного листа буде дозволено. Якщо облікові дані недійсні, завантаження електронної пошти буде заборонено. Керівник проекту завантажує електронну пошту з угодою про аутсорсинг (підписано). Договір аутсорсингу підписується обома сторонами.

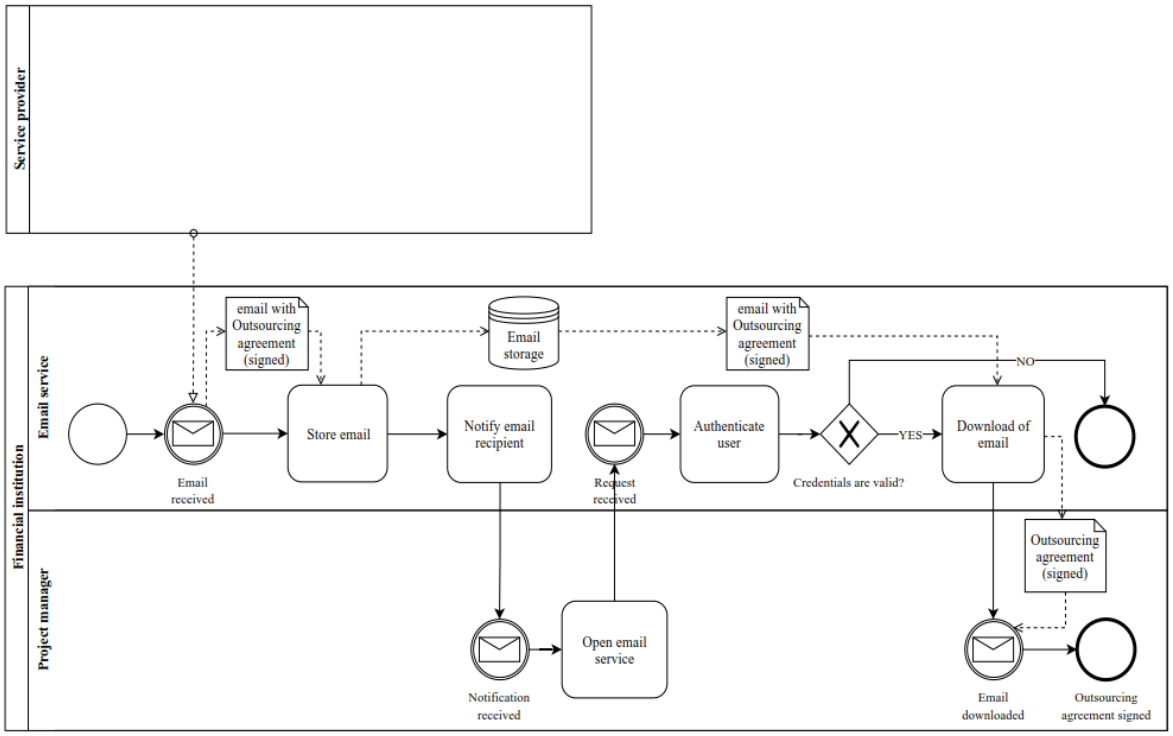

Рисунок 2.4 – Угода про аутсорсинг, підписана обома сторонами.

Другий етап реалізації — це зберігання угоди про аутсорсинг, яка представлена на рис. 2.5.

Процес надсилання електронної пошти однаковий, тому на малюнку він не показаний. Наступні кроки описують зберігання угоди про аутсорсинг.

Власник контракту отримує електронний лист із угодою про аутсорсинг (підписаною) та допоміжними матеріалами. Власник контракту відкриває систему керування контрактами. Система управління контрактами отримує запит на доступ і аутентифікує користувача. Якщо облікові дані дійсні, буде перевірено дозволи на доступ до системи. Якщо облікові дані недійсні, це означає, що спроба входу в журнал не вдалася. Якщо дозволи дійсні, доступ буде надано. Якщо дозволи недійсні, доступ не буде надано. Власник контракту вводить угоду про аутсорсинг (підписану) до системи керування контрактами.

Система керування контрактами отримує запит і перевіряє введені користувачем дані.

Якщо введені користувачем дані дійсні, буде оброблено угоду про аутсорсинг (підписану). Якщо введені користувачем дані недійсні, процес зупиняється. Система управління контрактами зберігає договір аутсорсингу (підписаний) і повідомляє власника контракту. Власник контракту отримує сповіщення.

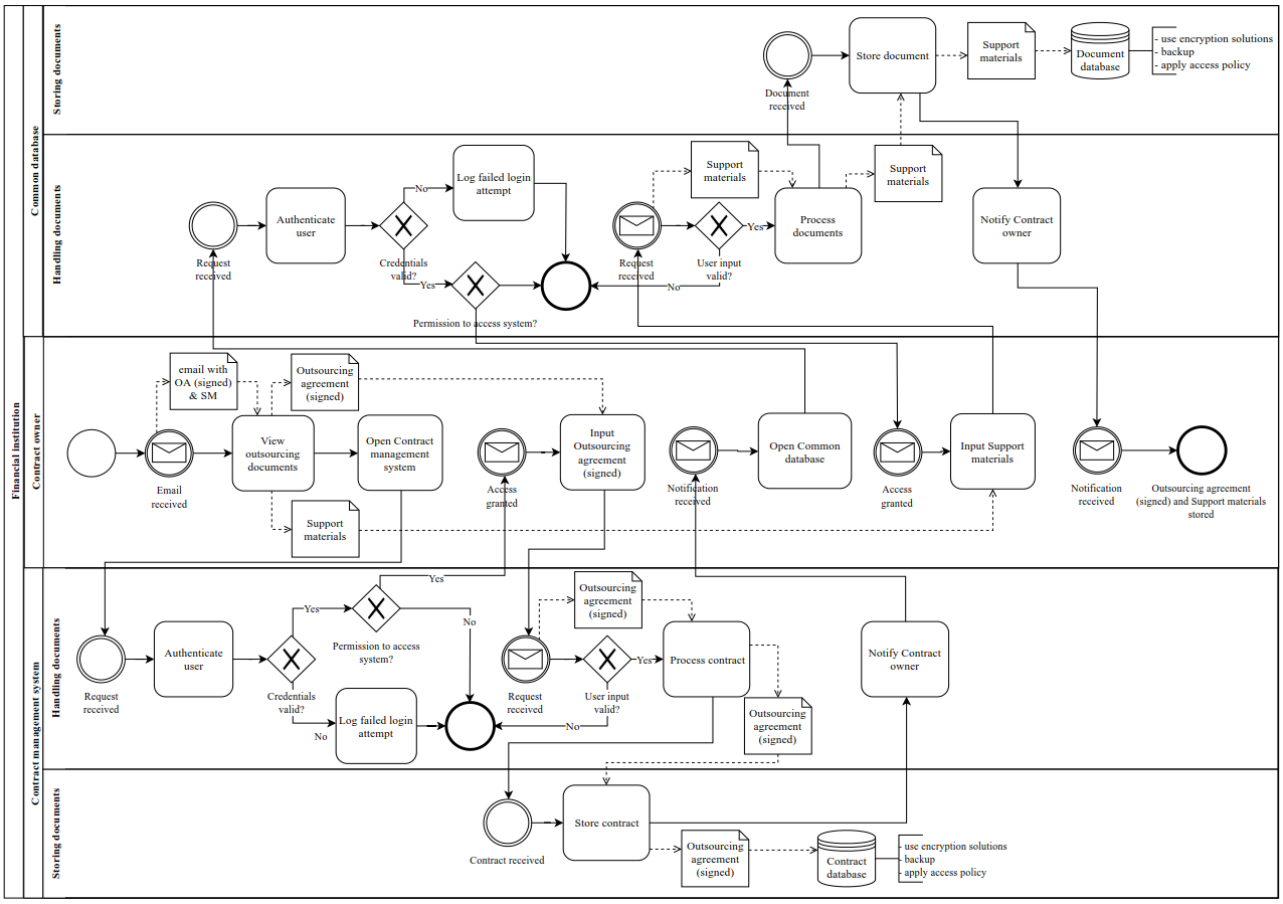

Рисунок 2.5 – Зберігання договору аутсорсингу.

Власник контракту відкриває загальну базу даних. Загальна база даних отримує запит на доступ і аутентифікує користувача. Якщо облікові дані дійсні, буде перевірено дозволи на доступ до системи. Якщо облікові дані недійсні, тоді спроба входу в систему керування контрактами не вдалася. Якщо дозволи дійсні, доступ буде надано. Якщо дозволи недійсні, доступ не буде надано.

Допоміжні матеріали власника контракту. Загальна база даних отримує запит і перевіряє введені користувачем дані. Якщо дані користувача дійсні, допоміжні матеріали будуть оброблені. Якщо введені користувачем дані

недійсні, процес зупиняється. Загальна база даних зберігає допоміжні матеріали та повідомляє власника контракту. Власник контракту отримує сповіщення. Договір аутсорсингу (підписаний) та допоміжні матеріали зберігаються. Третій етап впровадження — це етап сповіщення FSA, який зображено на рис. 2.6.

Для завершення етапу виконуються наступні кроки. Представник відповідності підписує заявку FSA та відкриває службу електронної пошти. Сервіс електронної пошти отримує запит і аутентифікує користувача. Якщо облікові дані дійсні, електронні листи відображатимуться. Якщо облікові дані недійсні, доступ до служби електронної пошти не буде надано. Представник відділу відповідності створює електронний лист із заявкою FSA (підписується). Сервіс електронної пошти надсилає електронний лист із заявкою FSA (підписаний). FSA повідомлено.

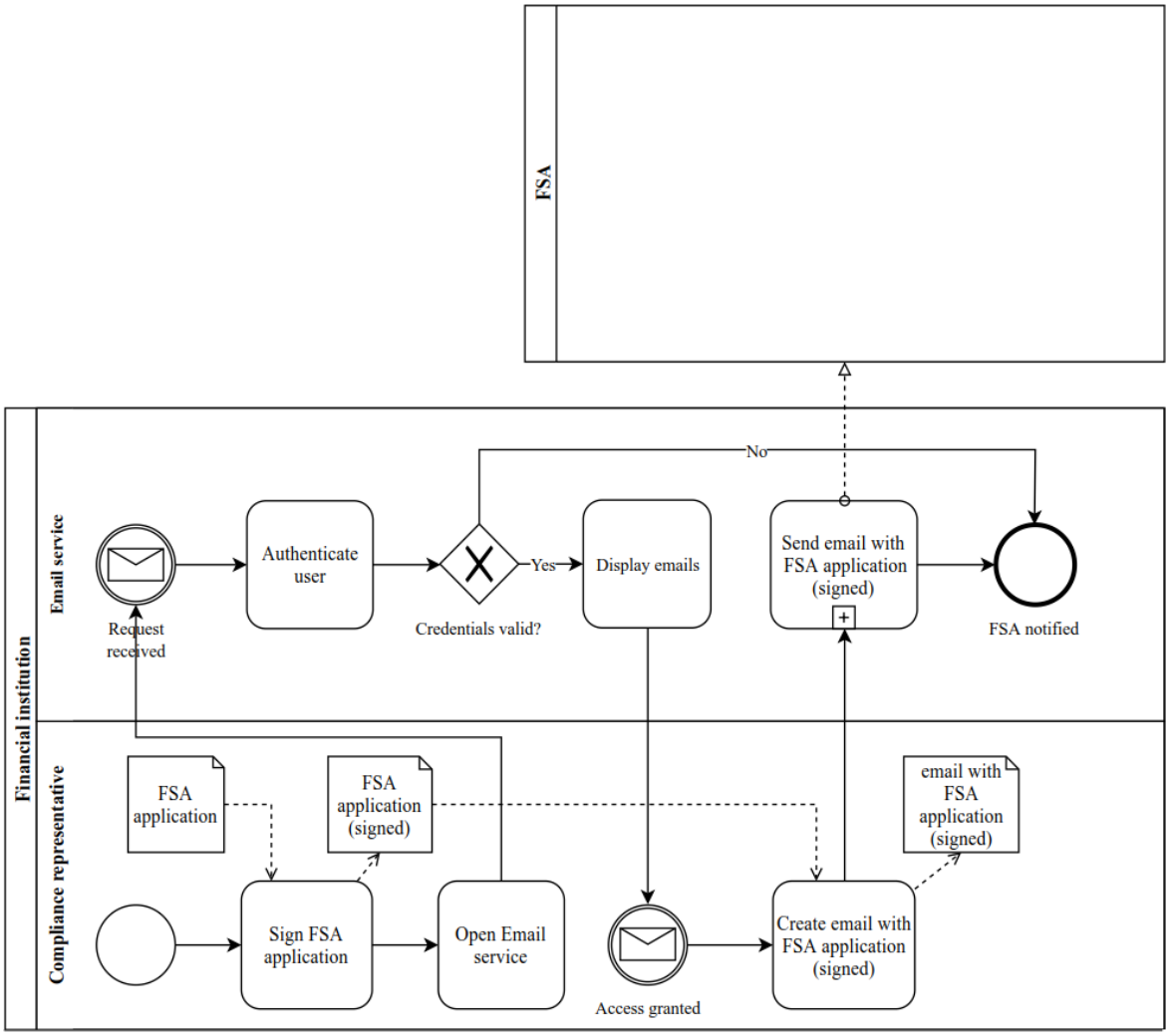

Рисунок 2.6 – Повідомлення FSA

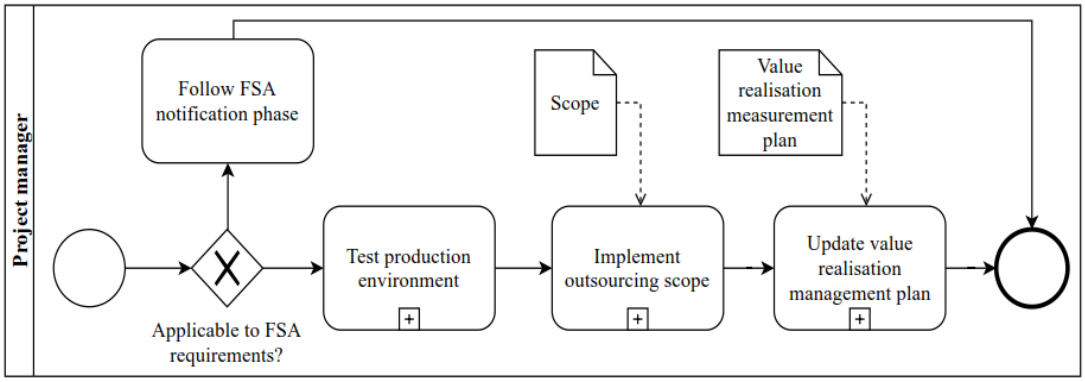

Рисунок 2.7 – Тестування та впровадження

Четверта фаза впровадження – це тестування та впровадження, що показано на рис. 2.7, щоб дати повний огляд бізнес-процесу впровадження. Довідник фінансової установи з аутсорсингу не охоплює це детально; отже, тут представлено просто як завдання, за виконання яких відповідає керівник проекту. На цьому етапі керівник проекту несе відповідальність за перевірку програм у робочому середовищі. (B) він виконує реалізацію обсягу аутсорсингу та оновлює план вимірювання реалізації вартості.

2.4 Висновок до другого розділу

У розділі подано огляд аутсорсингу в контексті фінансової установи, підкреслюючи можливості та ризики, які характеризують аутсорсинг. Аутсорсинг третіх сторін був відзначений як одна з головних проблем у фінансовому секторі. Впроваджено систему аутсорсингу та її компоненти в контексті фінансової установи. Описано загальний процес аутсорсингу.

Він складається з наступних п’яти етапів: визначення можливостей, попереднє дослідження, проектування та планування, реалізація та управління, подальші дії та звітність. Щоб звузити сферу оцінки ризику, етап реалізації був обраний для подальшого аналізу, оскільки він представляє як внутрішні, так і зовнішні комунікаційні сторони, інформаційні системи, які використовуються для обміну інформацією та її зберігання. Процес поділено на чотири етапи: підписання угоди про аутсорсинг, зберігання угоди про аутсорсинг,

повідомлення FSA, тестування та впровадження. Ці процеси були проілюстровані за допомогою мови моделювання BPMN.

3 ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ ISSRM ТА BNBAG

3.1 Оцінка ризиків інформаційної безпеки за допомогою ISSRM

У розділі описано доменну модель ISSRM. Щоб визначити сценарії ризиків інформаційної безпеки на етапі впровадження аутсорсингу. Процес оцінки ризиків інформаційної безпеки починається з визначення активів бізнесу та інформаційної системи. З цього варіанта використання реалізації системні активи, які підтримують бізнес-активи, такі:

– Внутрішні сторони: керівник проекту, власник контракту, представник із відповідності.
– Зовнішні сторони: постачальник послуг, FSA.
– Інфраструктура та послуги: служба електронної пошти.
– Програми/компоненти для підтримки діяльності: система управління контрактами, спільна база даних, сховище електронної пошти, база даних контрактів, база даних документів.

Основні бізнес-активи на етапі впровадження:

– Угода про аутсорсинг.
– Допоміжні матеріали.
– Застосунок FSA.

У цьому розділі визначено загрози та вразливі місця інформаційної системи. Сценарії потенційного ризику були створені з використанням потенційних загроз, які можуть використовувати вразливі місця, що призведе до впливу на фінансову установу. Результат оцінки ризиків інформаційної безпеки представлено у вигляді списку пріоритетних сценаріїв ризику.

Загрози в системі аутсорсингу з використанням ISSRM

Згідно з моделлю домену ISSRM загроза – це агент загрози, який використовує метод атаки для використання вразливості активу інформаційної системи. Відповідно до звіту ENISA [38] та інформації від фінансової установи,

домінуючими агентами ворожої загрози є злочинні групи та національні держави. Випадковий агент загрози може бути внутрішнім співробітником з привілейованим доступом до систем або без нього. Крім того, випадковий агент загрози може бути співробітником партнера або постачальника з доступом до систем або даних. Згідно з дослідженнями ENISA та Європолу [38] [39] та інформацією фінансової установи, наступні методи атаки найчастіше використовуються агентами загроз.

Поширення зловмисного програмного забезпечення є провідним методом атаки в усіх галузях. Більше зловмисного програмного забезпечення для фінансового сектора стосується великої кількості зареєстрованих банківських троянів і троянів-вимагачів. Також зросла кількість методів атак із застосуванням методів соціальної інженерії, які зарекомендували себе як ефективні методи зараження інформаційних систем.

Розподілена відмова в обслуговуванні (DDoS) все ще націлена на доступність систем. Крім того, шахрайські атаки, крадіжки інформації та витоки даних є помітними загрозами, з якими стикаються фінансові установи. На етапі впровадження аутсорсингу всі названі агенти загроз потенційно можуть використовувати описані методи атаки для використання однієї або кількох уразливостей.

Вибір відповідного методу атаки було зроблено залежно від наявних уразливостей у системі. Для класифікації загроз використовувалася таксономія загроз ENISA [24], описана в теоретичному розділі. Розглянуті вектори атак підпадають під категорії нечесної діяльності та перехоплення: ін’єкційна атака, несанкціонований доступ, викрадення, несанкціоноване використання ІС, зловживання ІС, фішинг, шкідливе програмне забезпечення та збір інформації. Представлено відповідні агенти загроз і загальні методи атак.

Уразливості системи аутсорсингу з використанням ISSRM.

Представлено огляд потоку інформації на етапі впровадження системи аутсорсингу. Інформація передається через засоби інформаційної системи. Відповідно до доменної моделі ISSRM, уразливості — це характеристики визначених активів інформаційної системи, які можуть бути використані

загрозою. Топ-10 таксономії OWASP [27] було використано для характеристики вразливостей. Класи вразливості в OWASP Top 10 відображаються на етапі впровадження у спосіб, який представлено в таблиці 3.1. Причини використання OWASP Top 10 пояснюються в теоретичному розділі.

Таблиця 3.1 – Уразливості на етапі впровадження для аналізу ISSRM.

Категорія OWASP	Ідентифікатор уразливості	Уразливість на етапі впровадження	Актив цільової інформаційної системи
Ін'єкційний	CWE89	Неправильна нейтралізація спеціальних елементів, які використовуються в команді SQL на серверах баз даних	Система управління контрактами або Загальна база даних
Порушена автентифікація	CWE287	Неправильна автентифікація в службі електронної пошти	Служба електронної пошти
Викриття конфіденційних даних	CWE319	Передача конфіденційної інформації в відкритому вигляді між користувачем і служба електронної пошти	Служба електронної пошти
XXE	CWE611	-	-
Порушений контроль доступу	CWE285	Некоректна авторизація в базах даних	База даних контрактів або база даних документів
Неправильна конфігурація безпеки	CWE16	Відсутність відповідної реалізації контролю доступу до баз даних	База даних контрактів або база даних документів

У таблиці 3.1 представлено вибірку вразливостей як характеристик активів інформаційної системи. Залежно від оцінки, на етапі впровадження системи аутсорсингу можуть бути виявлені додаткові вразливості.

Вплив у системі аутсорсингу з використанням ISSRM.

Згідно з моделлю домену ISSRM, коли агент загрози з методом атаки успішно використовує одну або більше вразливостей у системі, це призведе до впливу, який шкодить активу та зводить нанівець. критерій безпеки. Таблиця 6. представляє вісім потенційних сценаріїв ризику на етапі впровадження аутсорсингу, де агент загрози з методом атаки успішно використовує вразливість, що призводить до впливу. Загрози класифіковано відповідно до таксономії ENISA [24], яка була введена в теоретичному розділі.

Таблиця 3.2 – Загрози, вразливості та вплив для аналізу ISSRM

Загроза	**Сценарій ризику**
Ін'єкційна атака	Загроза: зловмисник із мотивацією прочитати угоду про аутсорсинг із бази даних контрактів і матеріалів підтримки із загальної бази даних, надсилаючи створені оператори впровадження SQL через систему керування контрактами або загальну базу даних. Метод атаки: 1. Отримайте доступ до системи керування контрактами або програми загальної бази даних. 2. Визначте неперевірене поле введення користувача. 3. Надішліть створені оператори впровадження SQL через програму. 4. Отримайте доступ до даних. CWE89: неправильна нейтралізація спеціальних елементів, які використовуються в команді SQL на серверах баз даних. Наслідки: втрата конфіденційності угоди про аутсорсинг і допоміжних матеріалів.

Загроза	Сценарій ризику
Несанкціонований доступ до ІБ	Загроза: зловмисник з мотивацією отримати доступ до угоди про аутсорсинг на сервері електронної пошти за допомогою кейлоггера для отримання пароля користувача, пов'язаного зі смарт-карткою, і викрадення смарт-картки. Метод атаки: 1. Використовуйте кейлоггер, щоб отримати пароль, пов'язаний зі смарт-карткою користувача. 2. Вкрасти смарт-карту. 3. Використовуйте викрадену смарт-карту та пароль для підключення до мережі. 4. Отримайте доступ до служби електронної пошти. CWE287: неправильна автентифікація в службі електронної пошти. Вплив: втрата конфіденційності угоди про аутсорсинг.
Викрадення	Загроза: зловмисник із мотивацією змінити передану угоду про аутсорсинг, використовуючи ту саму мережу, що й користувач, перехоплюючи та перехоплюючи маркер сеансу. Метод атаки: 1. Використовуйте ту саму мережу. 2. Перевірте трафік для маркера сеансу в незашифрованому трафіку. 3. Захоплення маркера сесії. 4. Змініть транспортовані дані. CWE319: передача конфіденційної інформації в відкритому вигляді між користувачем і службою електронної пошти. Вплив: втрата конфіденційності угоди про аутсорсинг.

Загроза	Сценарій ризику
Несанкціоноване використання програмного забезпечення	Загроза: зловмисник із мотивацією отримати угоду про аутсорсинг і матеріали підтримки з баз даних, виконавши довільний SQL-запит до баз даних, не маючи на це авторизації, і отримавши угоду про аутсорсинг і матеріали підтримки в результаті запиту. Метод атаки: 1. Станьте автентифікованим користувачем системи. 2. Запустіть довільний SQL-запит у базі даних Contract або Common database без будучи уповноваженим це робити. 3. Отримати результат запиту. 4. Отримати договір аутсорсингу та допоміжні матеріали з баз даних. CWE285: неправильна авторизація в базах даних. Наслідки: втрата конфіденційності угоди про аутсорсинг і допоміжних матеріалів.
Зловживання IS	Загроза: зловмисник із мотивацією отримати угоду про аутсорсинг із бази даних контракту та матеріали підтримки із загальної бази даних, знаючи про неправильно налаштовані бази даних і зловживаючи законно призначеними правами доступу. Метод атаки: 1. Знати про неправильне налаштування прав доступу користувачів у базі даних Contract або Common. 2. Використовуйте неправильну конфігурацію прав доступу користувача в базі даних Contract або Common database. 3. Зловживання законно призначеними правами доступу до документа в базі даних. CWE16: Відсутність належного контролю доступу до баз даних. Наслідки: втрата конфіденційності угоди про аутсорсинг і допоміжних матеріалів.

Загроза	Сценарій ризику
Фішинг	Загроза: зловмисник із мотивацією викрасти конфіденційну інформацію із системи керування контрактами та загальної бази даних, вставивши шкідливий сценарій у URL-адресу та надіславши його як фішинговий електронний лист цільовому користувачеві. Метод атаки: 1. Створіть шкідливий сценарій і вставте його в HTTP-запит. 2. Надішліть фішинговий електронний лист користувачеві з URL-адресою. 3. Отримувати відповідь від програми після того, як користувач натисне на шкідливу програму URL. CWE79: неправильна нейтралізація введення під час створення веб-сторінки в програмах баз даних. Вплив: втрата конфіденційності системи управління контрактами та загальної бази даних.
Шкідливе програмне забезпечення	Загроза: зловмисник із мотивацією прочитати та змінити Угоду про аутсорсинг і матеріали підтримки шляхом створення шкідливого програмного забезпечення для використання відомих невиправлених уразливостей. Метод атаки: 1. Знайте про невиправлені вразливості в управлінні контрактами системи або Загальної бази даних. 2. Створіть зловмисне програмне забезпечення для використання вразливостей. 3. Отримайте доступ до бази даних контрактів або бази даних документів. 4. Прочитайте та змініть угоду про аутсорсинг і допоміжні матеріали. CWE937: Наявність відомих невиправлених уразливостей на серверах баз даних. Вплив: втрата конфіденційності та цілісності угоди про аутсорсинг і допоміжних матеріалів.

Загроза	Сценарій ризику
Збір інформації	Загроза: зловмисник, який має мотивацію збирати угоду про аутсорсинг і матеріали підтримки, розробляючи вектори атаки, щоб націлити інформацію в базі даних, не залишаючи жодного сліду для криміналістичного аналізу. Метод атаки: 1. Мати знання про неповний запис подій. 2. Здійснювати несанкціоноване сканування інформаційних систем. 3. Розробити вектори атак для атаки на інформацію бази даних без жодного сліду для рідкий аналіз. 4. Зберіть угоду про аутсорсинг і допоміжні матеріали. CWE778: Недостатнє реєстрування невдалих спроб входу на сервери баз даних. Наслідки: втрата конфіденційності угоди про аутсорсинг і допоміжних матеріалів.

Ці сценарії базуються на суб’єктивній оцінці автора. Моделювання сценаріїв важливе для ілюстрації потенційних векторів атак, які агент загрози може розгорнути, щоб використати вразливі місця в системі, що призведе до певного впливу. Архітектура та дизайн інформаційних систем фінансової установи є складними; отже, важко запропонувати потенційні вектори атак для націлювання на вразливі місця в системі. Фінансові установи мають відповідати вимогам, напр. MiFID [36] і PSD2 [37].

Орієнтація на нерегульованого постачальника послуг, чиї системи добре інтегровані з фінансовою установою, може призвести до більшого впливу на фінансову установу. Незважаючи на протилежне, аналіз сторони постачальника послуг був залишений поза увагою через відсутність знань про архітектуру інформаційної системи постачальника послуг, інтеграцію між системами та потік інформації.

Ризики інформаційної безпеки в системі аутсорсингу з використанням ISSRM

Ризики важливо оцінити, щоб мати основу для прийняття рішень щодо можливих варіантів лікування або вибору засобів контролю. Установи фінансового сектору зобов'язані оцінювати свої ризики, щоб відповідати законам і нормам. Відповідно до доменної моделі ISSRM, ризик - це комбінація загрозливої події та її викликаного впливу.

Усі визначені сценарії фази впровадження, представлені в таблиці 3.2, оцінюються за допомогою метрик ISSRM, а результати представлені в таблиці 3.3.

Існує сім метрик, які визначаються для розрахунку рівня ризику загрози успішне використання однієї або кількох вразливостей, що призводить до впливу на організацію. Потреба в безпеці оцінюється як високий рівень потреби в конфіденційності чи цілісності або доступності для всіх бізнес-активів, що також вказує на те, що вплив оцінюється як таке ж значення відповідно до правил розрахунку методу ISSRM.

Імовірність загрози базується на суб’єктивному судженні щодо мотивації зловмисника та рівня складності атаки. Рівень уразливості оцінюється як середнє значення поширеності та значення виявленості вразливості на основі оцінки OWASP [27]. Інші показники розраховуються за допомогою рівнянь, наведених у теоретичному розділі дисертації.

Ці сценарії ризику можуть бути розставлені за пріоритетністю відповідно до їх рівня ризику, який вказує на рівень критичності ризику для організації та вартості бізнес-активів. Як видно, вартість бізнес-активів вважається високою в усіх сценаріях ризику. Крім того, існує ряд атак, які мають однаковий рівень ризику. Тому важко прийняти рішення розпочати лікування ризику з найбільш критичного.

Проте ризики можна розподілити за наступним списком на основі рівня ризику в таблиці 3.3:

- Фішинг.
- Ін’єкційна атака, шкідливе програмне забезпечення.
- Неправильне використання інформаційної системи.

Таблиця 3.3 – Рівень ризику для аналізу ISSRM.

Загроза	Бізнес-актив	Опис ризику					
Ін'єкційна атака	Договір аутсорсингу та допоміжні матеріали	Зловмисник із мотивацією прочитати угоду про аутсорсинг із бази даних контракту та матеріалів підтримки із загальної бази даних, надсилаючи створені оператори впровадження SQL через систему керування контрактом або загальну базу даних через неправильну нейтралізацію спеціальних елементів, які використовуються в команді SQL у сервери баз даних призводять до втрати конфіденційності угоди про аутсорсинг і матеріалів підтримки.					
	Вартість бізнес-активів	Розрахунок рівня ризику					
		Потреба безпеки	Імовірність загрози	Рівень вразливості	Потенційність	Вплив	Рівень ризику
	3	3	3	2.5	4.5	3	13.5
Несанкціонований доступ до IS	3	3	1	2	2	3	6
Викрадення	3	3	2	2.5	3.5	3	10.5
Несанкціоноване використання програмного забезпечення	3	3	2	2	3	3	9
Зловживання ІС	3	3	2	3	4	3	12
Фішинг	3	3	3	3	5	3	12
Шкідливе програмне забезпечення	3	3	3	3.5	4.5	3	13.5
Збір інформації	3	3	2	2	3	3	9

- Викрадення.

- Несанкціоноване використання програмного забезпечення, збір інформації.

- Несанкціонований доступ до інформаційних систем.

Ідеєю роботи є оцінка ризиків інформаційної безпеки, яка полягає у виявленні, аналізі та оцінці ризиків. ISSRM — це метод управління ризиками, який включає обробку ризиків і контроль як частину всього процесу. Відповідно до ілюстрації процесу ISSRM, процес оцінки ризику складається з (а) ідентифікації контексту та активів, (б) визначення цілей безпеки та (в) аналізу та оцінки ризику.

У цьому розділі наведено огляд оцінки ризиків інформаційної безпеки за допомогою методу ISSRM. По-перше, впроваджено відповідні активи етапу впровадження аутсорсингу. Було перераховано як бізнес-активи, так і активи допоміжної інформаційної системи. Описано потенційні загрози, які описуються як агент загрози з методом атаки. Таксономія загроз ENISA [24] була використана для узгодження аналізу загроз з існуючою практикою фінансової установи. На наступному етапі були визначені вразливості, які є характеристиками активів інформаційної системи. Було використано таксономію 10 найпопулярніших уразливостей OWASP [27], оскільки вона використовувалася у фінансовій установі раніше. Після опису вразливостей і загроз було представлено вісім сценаріїв ризику з додаванням потенційного впливу на організацію. Результати оцінки ризику представлені в таблиці 7. Сценарії були розставлені за пріоритетністю відповідно до рівня ризику, який був розрахований за допомогою метрик ISSRM. Загалом, у цей розділ включено ілюстрацію того, як оцінку ризику можна зробити на етапі впровадження за допомогою методу ISSRM.

3.2 Оцінка ризиків інформаційної безпеки з використанням BNBAG.

Метод BNBAG [9, 10] є імовірнісним методом оцінки ризику.

Кроки процесу BNBAG наступні:

- Визначення вразливостей системи аутсорсингу.
- Ілюстрування залежностей між вразливими місцями.
- Обчислення NPT.
- Оцінка ймовірності атаки.

Виявлення вразливостей у системі аутсорсингу з використанням BNBAG.

Метод BNBAG [9, 10] є методом оцінки ризику, пов'язаного з уразливістю. Вразливі місця — це слабкі місця в системі, якими може скористатися зловмисник. Для аналізу BNBAG було вибрано вибірку вразливостей, які використовувалися в ISSRM: неправильна нейтралізація спеціальних елементів, що використовуються в команді SQL (CWE89), неправильна автентифікація (CWE287), передача конфіденційної інформації відкритим текстом (CWE319), порушена авторизація (CWE285), неправильна конфігурація елементів керування доступом (CWE16), неправильна нейтралізація введення під час генерації веб-сторінки (CWE79), наявність відомих невиправлених уразливостей (CWE937) і недостатнє реєстрування невдалих спроб входу (CWE778). Усі дані можна знайти на етапі впровадження системи аутсорсингу. Додаткова інформація про вразливості доступна на веб-сторінці MITRE CWE [41].

Метод BNBAG дозволяє моделювати залежності між вразливими місцями. Хоча в системі може бути присутнім багато різних залежностей, для аналізу поточного прикладу було вибрано наступний обмежений список залежностей:

- CWE287 і CWE89 – неправильна автентифікація може залежати від успішного використання вразливості SQL-ін'єкції [42].

- CWE285 і CWE16 – неналежна авторизація може залежати від неправильної конфігурації засобів контролю доступу, реалізованих в IS. В аналізі ймовірність успішної атаки експлойтом незалежної вразливості визначається як добуток ймовірності виявлення вразливості в системі на ймовірність її використання. В аналізі для середньої оцінки ймовірності

виявлення уразливості в системі використовуються загальнодоступні дані, надані проектом OWASP [40].

Список CWE використовується для оцінки ймовірності використання вразливості [41]. Список CWE описує ймовірність експлойту за допомогою низьких/середніх/високих, які відповідають числам 0,2/0,6/1,0.

Графік атак у системі аутсорсингу з використанням BNBAG.

Вибір виявлених уразливостей та їхніх залежностей, використовується для побудови прикладу графіка атак, показаного на рис. 3.1. ілюстративний приклад, який дозволяє продемонструвати, як можна моделювати залежності між вразливими місцями під час оцінки ризику.

У наступному аналізі інцидент визначається як потенційний компроміс конфіденційності, цілісності або доступності, що є загальним визначенням інциденту інформаційної безпеки у фінансовій галузі. Інцидент у методі BNBAG є подією в методі ISSRM. Графік атак на рис. 3.1 показує всі розглянуті вектори атак, які можуть бути використані для виклику інциденту.

По-перше, уразливості можуть бути спрямовані незалежно для успішного інциденту.

По-друге, використання однієї вразливості може збільшити ймовірність використання іншої вразливості із залежністю, тобто потенційне використання другої вразливості залежить від успіху попередньої. Ця ситуація проілюстрована залежністю між уразливостями CWE285 і CWE16, а також залежністю між уразливостями CWE287 і CWE89.

Можна націлюватися на вразливості незалежно. Крім того, можна використовувати вектор атаки, який успішно використовує один вузол уразливості, дозволяючи зловмиснику також використовувати залежну вразливість. У Розділі 5.3 сформовані таблиці ймовірності вузла, щоб проілюструвати обчислення спільної ймовірності інциденту, враховуючи залежності між різними вузлами вразливості. 5.3 Таблиці ймовірності вузла в системі аутсорсингу з використанням BNBAG NPT надають вхідні дані для обчислення загальної ймовірності успішного інциденту.

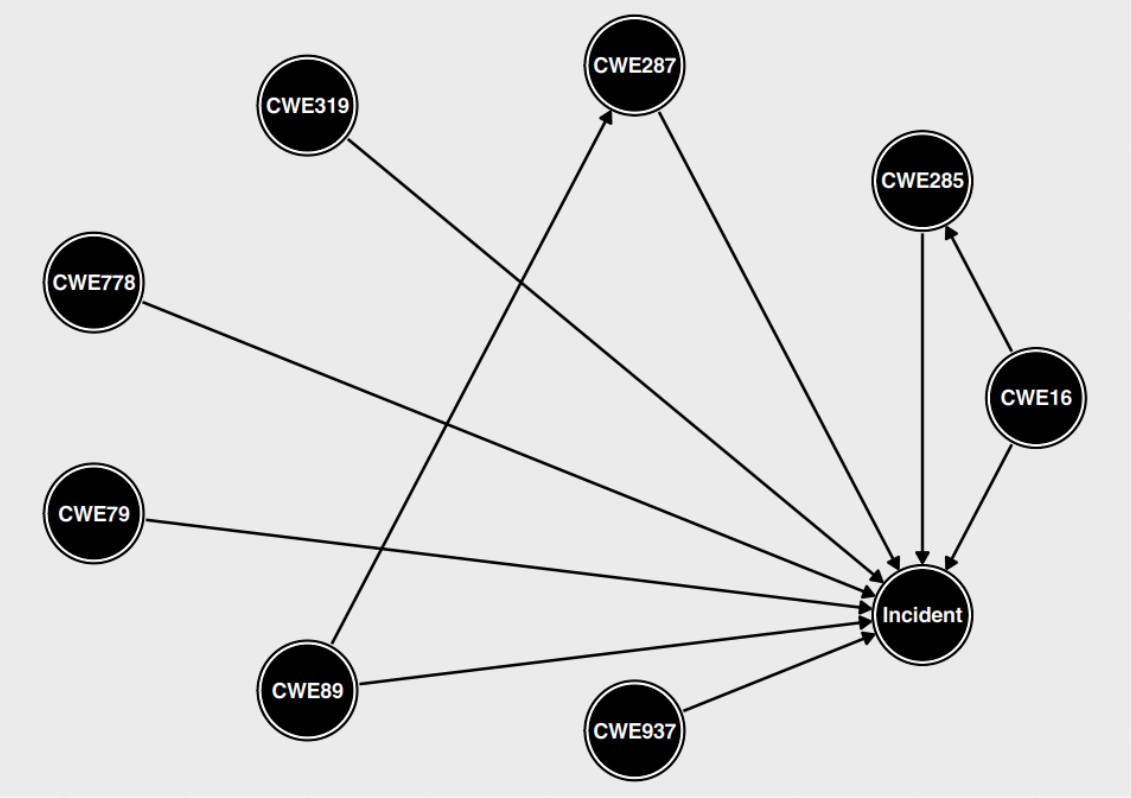

Рисунок 3.1 –Граф атак, що моделює набір вибраних уразливостей для аналізу BNBAG.

NPT для незалежних і залежних уразливостей представлені в таблиці 8. Справжнє значення (T) являє собою ймовірність появи експлойту певної вразливості. Він розраховується як ймовірність наявності вразливості в системі, помножена на ймовірність її використання. Значення false (F) представляє ймовірність ненастання такої події. Оскільки ймовірність хибного значення (F) представляє ймовірність появи доповнення, тоді вона обчислюється як один мінус ймовірність появи експлойту. NPT для всіх виявлених вразливостей наведено в таблиці 3.4, включаючи умовні ймовірності вразливостей CWE285 і CWE287. Імовірності CWE285 і CWE287 вказують на їх потенційну залежність від наявності в системі вразливостей CWE16 або CWE89.

По-перше, NPT для CWE285 з урахуванням CWE16 вказує на те, що ймовірність CWE285 є істинною, враховуючи, що CWE16 є істинною зі значенням 0,15 на основі суб’єктивних даних. Це означає, що якщо елементи керування доступом налаштовано неправильно, то існує ймовірність того, що користувач неправильно авторизований. Імовірність того, що CWE є істинним,

враховуючи, що CWE16 є хибним, становить 0,02, тобто незалежна ймовірність CWE285, яка розраховується на основі даних.

По-друге, представлено NPT для CWE287 з урахуванням CWE89. Імовірність того, що CWE287 є істинним, враховуючи, що CWE89 є істинним, становить 0,09. Це значення базується на суб'єктивних даних. Імовірність того, що CWE287 є істинним, якщо CWE89 є хибним, становить 0,04, тобто незалежна ймовірність уразливості CWE287.

Таблиця 3.4 – NPT вразливостей для аналізу BNBAG.

NPT	**CWE16**
T	0.24
F	0.76

NPT	**CWE89**
T	0.10
F	0.90

NPT	**CWE319**
T	0.05
F	0.95

NPT	**CWE79**
T	0.24
F	0.76

NPT	**CWE937**
T	0.01
F	0.99

NPT	**CWE778**
T	0.00(1)
F	0.99(9)

NPT	CWE16	
CWE285	T	F
T	0.15	0.02
F	0.85	0.98

NPT	CWE89	
CWE287	T	F
T	0.09	0.04
F	0.91	0.96

Імовірності вузлів залежних змінних обчислюються за допомогою рівняння 1.4 для попереднього розрахунку граничної ймовірності. По-перше, CWE285 залежить від CWE16, як показано на графіку атаки на рис. 3.1.

Імовірність успішної атаки через уразливість CWE285 обчислюється для CWE16 як істинне, так і хибне.

$$P(CWE285 = T) = \sum_{CWE16} P(CWE285 = T \mid CWE16)P(CWE16) = 0.15 \times 0.24 + 0.02 \times 0.76 = 0.05$$

По-друге, CWE287 залежить від CWE89 згідно з графіком атак. NPT уразливості CWE287 обчислюється за допомогою рівняння 1.4.

Імовірність CWE287 є істинною, якщо CWE89 є істинною чи хибною.

$P(CWE287 = T) = \sum_{CWE89} P(CWE287 = T|CWE89)P(CWE89) = 0.09 \times 0.1 + 0.04 \times 0.9 = 0.05$

Значення 0,05 як результат обох рівнянь вказує на те, що існує 5% ймовірність того, що CWE285 є істинним, і існує 5% ймовірність того, що CWE287 є істинним.

Значення NPT для CWE285 і CWE287, представлені в таблиці, враховують, що якщо вразливість CWE16 або вразливість CWE89 були використані, то залежні ймовірності CWE285 або CWE287 потрібно переглянути. Уявлення про ймовірність CWE285 або CWE287 можна переглянути за допомогою теореми Байєса в рівнянні 1.3.

Те саме стосується, якщо виявлено, що вразливість CWE285 або CWE287 була використана, тоді переконання щодо ймовірності CWE16 або CWE89 можуть переглянути за допомогою теореми Байєса. Якщо відомо, що вразливість CWE285 є істинною, це потенційно призводить до збільшення ймовірності того, що уразливість CWE16 є істинною. Апостеріорну ймовірність CWE16 можна обчислити за допомогою рівняння 1.3.

Оскільки результат обчислення не використовується в майбутньому аналізі, ця інформація була представлена лише для ілюстрації потенційного використання теореми Байєса. Такий самий аналіз можна провести, якщо виявлено, що вразливість CWE287 використовується.

Якщо відповідні дані зібрано, ймовірності можна оновити відповідно до тієї ж теореми. Розраховані ймовірності можна використовувати для міркування про ризик. Ці шість NPT використовуються для формування результату аналізу BNBAG у наступному розділі.

Обґрунтування та розрахунок у системі аутсорсингу з використанням BNBAG.

Ймовірності вразливостей, виявлених у системі, були розраховані в вище. Інцидент потенційно може статися, якщо принаймні одна вразливість успішно використана. Якщо використовуються дві або більше вразливості, ймовірність інциденту є сумою ймовірностей уразливостей, описаних у рівнянні 1.9.

Щоб обчислити ймовірність інциденту, потрібно використовувати NPT уразливостей. На графіку атак показано 6 вразливостей. Це означає, що існує 64

комбінації вразливостей, які потенційно можуть призвести до успішного інциденту. Щоб дати огляд результатів, було розраховано дві ймовірності.

Імовірність інциденту — це ймовірність того, що принаймні одна вразливість буде використана. Перша ймовірність інциденту була розрахована з використанням вразливостей як незалежних подій. Друга ймовірність інциденту також враховує умовні ймовірності в розрахунку.

1. $P(incident) = 1 - \prod P(vulnerabilities = F) = 0.54$
2. $P(incident) = 1 - \prod P(vulnerabilities = F) = 0.56$

Результати відрізняються один від одного. Якщо залежності не враховано, ймовірність інциденту становить 0,54. Якщо були враховані залежності між уразливими місцями, ймовірність інциденту становить 0,56. Уразливості можна класифікувати за ступенем серйозності, яка визначається як імовірність існування вразливості в системі та ймовірність її використання. Наступний список представляє вразливості відповідно до їх серйозності:

- CWE16 Неправильна конфігурація безпеки.
- CWE79 Міжсайтові сценарії.
- CWE89 SQL-ін’єкція.
- CWE319 Передача конфіденційної інформації у відкритому тексті.
- CWE287 Неналежна автентифікація.
- CWE285 Неналежна авторизація.
- CWE937 Використання компонента з відомими вразливими місцями.
- CWE778 Недостатнє ведення журналу безпеки.

Підсумовуючи, метод BNBAG можна використовувати для оцінки інформаційної безпеки ризики. Ілюстрацію процесу було показано в розділі.

3.3 Висновок до третього розділу

У цьому розділі наведено огляд оцінки ймовірності в рамках оцінки ризику інформаційної безпеки за допомогою методу BNBAG та ISSRM.

По-перше, було виявлено відповідні вразливості на етапі впровадження системи аутсорсингу.

В аналізі було застосовано класифікацію 10 найпопулярніших вразливостей OWASP, оскільки вона використовувалася у фінансовій установі раніше. Залежності між вразливими місцями визначено та проілюстровано на графіку атак.

Впроваджено відповідні активи етапу впровадження аутсорсингу. Було перераховано як бізнес-активи, так і активи допоміжної інформаційної системи. Описано потенційні загрози, які описуються як агент загрози з методом атаки.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Система управління охороною праці.

Система управління охороною праці (СУОП) — це сукупність органів управління підприємством, які на підставі комплексу нормативної документації проводять цілеспрямовану, планомірну діяльність щодо здійснення завдань і функцій управління з метою забезпечення здорових, безпечних і високопродуктивних умов праці. Створення СУОП здійснюється шляхом послідовного визначення мети і об'єкта управління, завдань і заходів щодо охорони праці, функцій і методів управління, побудови організаційної структури управління, складання нормативно-методичної документації. Головна мета управління охороною праці є створення здорових, безпечних і високопродуктивних умов праці, покращення виробничого побуту, запобігання травматизму і профзахворюванням.

Охорона праці базується на законодавчих, директивних та нормативно-технічних документах. При управлінні охороною праці не повинні прийматись рішення та здійснюватись заходи, що суперечать діючому законодавству, державним нормативним актам про охорону праці, стандартам безпеки праці, правилам та нормам охорони праці.

До основних функцій управління охороною праці належать:

- прогнозування і планування робіт, їх фінансування;
- організація та координація робіт;
- облік показників, аналіз та оцінка стану умов і безпеки праці;
- контроль за станом охорони праці та функціонуванням СУОП;
- стимулювання діяльності з охорони праці.

Функція планування, в основі якої лежить прогностичний аналіз, має вирішальне значення в СУОП. Планування роботи з охорони праці поділяється на перспективне, поточне та оперативне.

Перспективне планування охоплює найбільш важливі, трудомісткі й довгострокові за терміном виконання заходи з охорони праці, виконання яких,

як правило, вимагає сумісної роботи кількох підрозділів підприємства. Можливість виконання заходів перспективного плану має бути підтверджена обґрунтованим розрахунком необхідного матеріально-технічного забезпечення і фінансових витрат із зазначенням джерел фінансування. Основною формою перспективного планування роботи з охорони праці є розроблення комплексного плану підприємства (на 3—5 років) щодо покращення стану охорони праці.

Поточне планування здійснюється у межах календарного року шляхом розроблення та включення відповідних заходів до розділу "Охорона праці" колективного договору.

Оперативне планування роботи з охорони праці здійснюється за підсумками контролю стану охорони праці у структурних підрозділах і на підприємстві в цілому або перевірок органів державного нагляду. Оперативні заходи щодо усунення виявлених недоліків зазначаються у наказі роботодавця.

Оперативне планування роботи з охорони праці здійснюється за підсумками контролю стану охорони праці в структурних підрозділах і на підприємстві в цілому. Оперативні заходи щодо усунення виявлених недоліків зазначаються безпосередньо у наказі власника підприємства, який видається за підсумками контролю, або у плані заходів, як додатку до наказу.

Функція СУОП щодо організації та координації робіт передбачає формування органів управління охороною праці на всіх рівнях управління і всіх стадіях виробничого процесу, визначення обов'язків, прав, відповідальності та порядку взаємодії осіб, що приймають участь в процесі управління, а також прийняття та реалізацію управлінських рішень.

Контроль за станом охорони праці. Дійове управління охороною праці можна здійснювати тільки при наявності повної, своєчасної і вірогідної інформації про стан охорони праці. Одержати таку інформацію, виявити можливі відхилення від норм безпеки, а також перевірити виконання планів та управлінських рішень можна тільки на підставі регулярного та об'єктивного контролю.

До основних форм контролю за станом охорони праці належать: оперативний контроль; контроль, що проводиться службою охорони праці

підприємства; громадський контроль; адміністративно-громадський трьохступеневий контроль; відомчий контроль вищих органів. Необхідно зазначити, що крім контролю, здійснюється нагляд за охороною праці з боку державних та профспілкових інспекцій.

Адміністрація (роботодавець) для створення безпечних і нешкідливих умов праці працівників і для власної безпеки зобов'язана керуватися переліком таких основних нормативно-законодавчих актів і документів з охорони праці:

Закон України «Про охорону праці»;

Типове положення про службу охорони праці;

Положення про порядок розслідування нещасних випадків, що сталися під час навчально-виховного процесу в навчальних закладах (Наказ МОН України № 616 від 31.08.2001 року):

Порядок розслідування та ведення обліку нещасних випадків, професійних захворювань і аварій на виробництві (Постанова КМУ № 1112 від 25 серпня 2004 року);

Типове положення про навчання з питань охорони праці;

Положення про розробку інструкцій з охорони праці;

Перелік робіт з підвищеною небезпекою;

Граничні норми підняття і переміщення важких речей жінками;

Граничні норми підняття і переміщення важких речей неповнолітніми;

Положення про медичний огляд працівників окремих категорій;

Перелік посад посадових осіб, які зобов’язані проходити попередню і періодичну перевірку знань з охорони праці;

Порядок розробки і затвердження власником нормативних актів про охорону праці, чинних на підприємстві;

Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального захисту (Наказ Держгірпромнагляду від 24.03.2008 року № 53);

Порядок проведення атестації робочих місць за умовами праці (Постанова Кабінету Міністрів України N 442 від 01.09.1992 року);

Типове положення про комісію з питань охорони праці;

Типове положення «Про кабінет охорони праці».

Стимулювання діяльності з охорони праці спрямовано на створення зацікавленості працівників у забезпеченні здорових та безпечних умов праці. Стимулювання передбачає як моральні, та матеріальні заохочення, так і покарання за невиконання покладених на конкретну особу зобов'язань стосовно безпеки праці або порушення вимог щодо охорони раці. До числа останніх належать: премії, винагороди за виконану конкретну роботу, винахідництво та раціоналізаторські пропозиції з питань охорони праці. Джерелом стимулювання діяльності з охорони праці є фонди охорони праці.

4.2 Вимоги до робочого середовища користувача ЕОМ: мікроклімат, освітлення, рівень шуму, електромагнітне випромінювання

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства внутрішніх справ України і зареєстрованого в Міністерстві юстиції України з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з розрахунку 2 шт. на кожні 20 кв. м площі приміщення з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог Правил пожежної безпеки в Україні.

Правила експлуатації ЕОМ встановлюють вимоги безпеки та санітарно-гігієнічні вимоги до обладнання робочих місць користувачів ЕОМ і працівників, що виконують обслуговування, ремонт та налагодження ЕОМ, та роботи з застосуванням ЕОМ, відповідно до сучасного стану техніки та наукових досліджень у сфері безпечної організації робіт з експлуатації ЕОМ та з урахуванням положень міжнародних нормативно-правових актів з цих питань.

Гігієнічні вимоги до параметрів виробничого середовища включають вимоги до параметрів мікроклімату, освітлення, рівень шуму і електромагнітного випромінювання.

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря.

Приміщення з ЕОМ повинні мати природне і штучне освітлення. Природне світло повинно проникати через бічні світлопрорізи, зорієнтовані, як правило, на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості не нижче 1,5%. При виробничій потребі дозволяється експлуатувати ЕОМ у приміщеннях без природного освітлення за узгодженням з органами державного нагляду за охороною праці та органами і установами санітарно-епідеміологічної служби.

Загальне освітлення має бути виконане у вигляді суцільних або переривчатих ліній світильників, що розміщуються збоку від робочих місць (переважно зліва) паралельно лінії зору працівників.

Рівні шуму на робочих місцях осіб, що працюють з відеотерміналами та ЕОМ, визначені ДСанПіН 3.3. 2-007-98.

Для забезпечення нормованих рівнів шуму у виробничих приміщеннях та на робочих місцях застосовуються шумопоглинальні засоби, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками.

Рівні електромагнітного випромінювання та магнітних полів повинні відповідати вимогам ГОСТ 12.1. 006 "ССБТ. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведенню контроля", СН N 3206-85 "Гранично допустимі рівні магнітних полів частотою 50 Гц" та ДСанПіН 3.3. 2-007-98.

4.3 Створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території

Державна система моніторингу довкілля - це система спостережень, збирання, оброблення, передавання, збереження та аналізу інформації про стан довкілля, прогнозування його змін і розроблення науково-обгрунтованих

рекомендацій для прийняття рішень про запобігання негативним змінам стану довкілля та дотримання вимог екологічної безпеки. Це Положення визначає порядок створення та функціонування такої системи в Україні.

Система моніторингу є складовою частиною національної інформаційної інфраструктури, сумісної з аналогічними системами інших країн.

Система моніторингу – це відкрита інформаційна система, пріоритетами функціонування якої є захист життєво важливих екологічних інтересів людини і суспільства; збереження природних екосистем; відвернення кризових змін екологічного стану довкілля і запобігання надзвичайним екологічним ситуаціям.

Створення і функціонування системи моніторингу з метою інтеграції екологічних інформаційних систем, що охоплюють певні території, грунтується на принципах:

— узгодженості нормативно-правового та організаційно-медичного забезпечення, сумісності технічного, інформаційного і програмного забезпечення її складових частин;

— систематичності спостережень за станом довкілля та техногенними об'єктами, що впливають на нього;

своєчасності отримання, комплексності оброблення та використання інформації про стан довкілля, що надходить і зберігається в системі моніторингу;

— об'єктивності первинної, аналітичної і прогнозної інформації про стан довкілля (екологічної інформації) та оперативності її доведення до органів державної влади, органів місцевого самоврядування, громадських організацій, засобів масової інформації, населення України, заінтересованих міжнародних установ та світового співтовариства.

Моніторинг довкілля здійснюють:

— Мінприроди - ґрунтів на природоохоронних територіях (вміст ЗР, у тому числі радіонуклідів); державного екологічного картування території України для оцінки його стану та його змін під впливом господарської діяльності; наземних екосистем (фонова кількість ЗР, у тому числі радіонуклідів); видів рослинного і

тваринного світу, що перебувають під загрозою зникнення, та видів, що перебувають під особливою охороною.

— Мінекономіки - грунтів сільськогосподарського використання (радіологічні, агрохімічні та токсикологічні визначення, залишкова кількість пестицидів, агрохімікатів і важких металів); сільськогосподарських рослин і продуктів з них (токсикологічні та радіологічні визначення, залишкова кількість пестицидів, агрохімікатів і важких металів).

— Держлісагентство - грунтів земель лісового фонду (радіологічні визначення, залишкова кількість пестицидів, агрохімікатів і важких металів); лісової рослинності (стан, продуктивність, пошкодження біотичними та абіотичними чинниками, біорізноманіття, радіологічні визначення); мисливської фауни (видові, кількісні та просторові характеристики);

— Держгеокадастр - грунтів і ландшафтів, зрошуваних і осушених земель (вторинне підтоплення і засолення тощо); берегових ліній річок, морів, озер, водосховищ, лиманів, заток, гідротехнічних споруд (динаміка змін, ушкодження земельних ресурсів);

— Мінрегіон - питної води централізованих систем водопостачання (вміст ЗР, обсяги споживання); стічних вод міської каналізаційної мережі та очисних споруд (вміст ЗР, обсяги надходження);

— Держгеонадра - підземних вод (ресурси та використання); ендогенних та екзогенних процесів (видові і просторові характеристики, активність прояву).

Фінансування робіт із створення і функціонування системи моніторингу та її складових частин здійснюється відповідно до порядку фінансування природоохоронних заходів за рахунок коштів, передбачених у державному та місцевих бюджетах згідно із законодавством.

Покриття певної частини витрат на створення і функціонування складових частин і компонентів системи моніторингу може здійснюватися за рахунок інноваційних фондів у межах коштів, передбачених на природоохоронні заходи, міжнародних грантів та інших джерел фінансування.

4.4 Організація цивільного захисту на об’єктах промисловості та виконання заходів щодо запобігання виникненню надзвичайних ситуацій техногенного походження

Виходячи з принципів побудови цивільного захисту в Україні слід підкреслити, що територіально - виробничий принцип знайшов втілення в організації цивільного захисту на об'єктах народного господарства, а також на територіях областей, міст і районів, в тому числі міських та сільських.

Відповідно до статті 16 Кодексу цивільного захисту України та з метою запобігання виникненню надзвичайних ситуацій техногенного характеру (далі - надзвичайні ситуації), забезпечення стійкого функціонування об’єктів в умовах особливого періоду Кабінет Міністрів України.

Поставляє установити, що дія цієї постанови поширюється на органи управління цивільного захисту, а саме на центральні органи виконавчої влади, Раду міністрів Автономної Республіки Крим, обласні, Київську та Севастопольську міські, районні, районні у мм. Києві та Севастополі державні адміністрації, військово-цивільні адміністрації, органи місцевого самоврядування та об’єкти незалежно від форми власності, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам та які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду, є об’єктами підвищеної небезпеки.

Для керівництва поточної роботи з цивільного захисту на об'єкті економіки створюється основний орган управління - штаб цивільного захисту. До складу штабу цивільного захисту входять: начальник штабу і його заступники (помічники) з оперативно-розвідувальної частини, бойової підготовки, житлового сектора.

Посада начальника штабу цивільного захисту передбачається штатним розкладом об'єкта. Начальник штабу є першим заступником начальника цивільного захисту об'єкта і має право за його ім'ям віддавати накази та розпорядження з цивільного захисту. Він є безпосереднім організатором

управління цивільним захистом і сповіщення про загрозу або факт надзвичайної ситуації, розвідки, дозиметричного і хімічного контролю, веде поточне та перспективне планування, підготовку формувань і виробничого персоналу з цивільного захисту та контроль за виконанням всіх заходів з цивільного захисту.

Керівникам функціональних та територіальних підсистем єдиної державної системи цивільного захисту та підприємствам, установам, організаціям незалежно від форми власності, на які поширюється дія цієї постанови, забезпечити:

— уточнення планів реагування на надзвичайні ситуації і планів локалізації та ліквідації наслідків аварій, здійснення заходів щодо запобігання їх виникненню;

— готовність до здійснення оповіщення органів управління та сил цивільного захисту, населення про загрозу виникнення або виникнення надзвичайної ситуації та інформування їх про межі поширення, наслідки, способи та методи захисту, а також дії у зоні можливої надзвичайної ситуації;

— спостереження та контроль за ситуацією на об’єктах, на які поширюється дія цієї постанови, територіях цих об’єктів та/або за їх межами, а також здійснення постійного прогнозування можливості виникнення надзвичайних ситуацій, їх масштабів;

— готовність наявних сил і засобів цивільного захисту, можливість залучення додаткових сил і засобів у разі виникнення надзвичайних ситуацій;

— створення і використання матеріальних резервів для запобігання виникненню надзвичайних ситуацій і ліквідації їх наслідків.

Державній службі з надзвичайних ситуацій узагальнювати аналітичні матеріали та подавати їх для розгляду Державній комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій для забезпечення координації заходів щодо запобігання виникненню надзвичайних ситуацій державного рівня.

Остаточне рішення щодо рівня надзвичайної ситуації з подальшим відображенням її у даних статистики, у тому числі при відсутності достатніх відомостей щодо розвитку надзвичайної ситуації, приймає спеціально уповноважений центральний орган виконавчої влади, до компетенції якого

входить вирішення питань захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру, за погодженням у разі потреби із зацікавленими міністерствами та іншими центральними органами виконавчої влади. Обов'язково враховується (за його наявності) експертний висновок регіональної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій щодо рівня надзвичайної ситуації

4.5 Висновок до четвертого розділу

В даному розділі було розглянуто актуальні теми безпеки в надзвичайних ситуаціях. Були отримані знання стосовно експлуатації ЕОМ правил і вимогам, які затверджені комітетами по нагляду за охороною праці та іншими органами, які відповідають за безпеку життєдіяльності. Також запобігти негативним змінам стану довкілля та запобігання ліквідації в надзвичайних ситуацій, які загрожують життю і здоров’ю людей.

ВИСНОВКИ

У роботі було показано, як можна застосувати методи оцінки ризиків інформаційної безпеки в аутсорсинговій системі фінансової установи. Оцінка ризиків є частиною управління ризиками.

Метод ISSRM був обраний як метод управління ризиками, тоді як метод BNBAG служить імовірнісним методом оцінки ризиків. Ці два методи були застосовані в тематичному дослідженні, щоб зрозуміти їх схожість і різницю на практиці. Аутсорсинг був обраний як контекст для реалізації двох методів. Аутсорсинг є однією з головних проблем у фінансовому секторі.

Було представлено результати двох оцінок. Застосування методів оцінки ризику інформаційної безпеки реального процесу дало розуміння необхідності вдосконалення в цій галузі. Надано пропозицію щодо поєднання методу управління ризиками безпеки та імовірнісного методу.

Було представлено результати двох оцінок. Застосування методів оцінки ризику інформаційної безпеки реального процесу дало автору дисертації розуміння необхідності вдосконалення в цій галузі. Надано пропозицію щодо поєднання методу управління ризиками безпеки та імовірнісного методу.

Визначено відповідні активи, які потребують захисту в контексті аутсорсингу у фінансовій установі. Розраховано таблиці ймовірності вузла для кожної вразливості.

Для покращення результатів оцінки ризиків запропоновано поєднати метод управління ризиками безпеки та метод імовірнісної оцінки ризиків. Рекомендовано комбінувати методи за допомогою наступних етапів: ідентифікація активів і цілей безпеки на основі методу ISSRM, аналіз загроз за методом ISSRM, моделювання вразливостей на основі BNBAG, опис подій загрози та потенціалу вплив за допомогою ISSRM.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 International Telecommunication Union. Measuring the Information Society Report, 2018. URL : https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-E.pdf.

2 International Telecommunication Union and World Telecommunication, Individuals using the Internet (% of population), International Telecommunication Union, 2018. URL : https://data.worldbank.org/indicator/IT.NET.USER.ZS.

3 D. Reinsel, J. Gantz, J. Rydning. Data Age 2025: The Evolution of Data to Life-Critical. International Data Corporation, sponsored by Seagate, Framingham, Massachusetts, 2017. 25 p.

4 A. Hunt, E. Thrower, M. Yeomans and B. Heynderickx. Quantitative Techniques in Information Risk Analysis," Information Security Forum, 2018. 12 p.

5 S. L. Savage. The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty. Hoboken. New Jersey. John Wiley & Sons, Inc., 2009. p. 155.

6 Institute of Risk Management. A Risk Practitioners Guide to ISO 31000: 2018. Institute of Risk Management, London, 2018. URL : https://www.demarcheiso17025.com/document/A%20Risk%20Practitioners%20Guide%20to%20ISO%2031000%20%96%202018.pdf.

7 British Standards Institution and ISO/IEC. Information technology — Security techniques — Information security risk management. BSI. London, 2008. 38 p.

8 E. Dubois, P. Heymans, N. Mayer and R. Matulevičius. A Systematic Approach to Define the Domain of Information System Security Risk Management. in Intentional Perspectives on Information Systems Engineering, Berlin, Springer, 2010. pp. 289-306.

9 N. Fenton and M. Neil. Risk Assessment and Decision Analysis with Bayesian Networks. Boca Raton: Taylor & Francis Group, 2013. 660 p.

10 L. Munoz-Gonzalez and E. C. Lupu. Bayesian Attack Graphs for Security Risk Assessment. in IST-153 Workshop on Cyber Resilience, Munich, 2017. URL : https://ceur-ws.org/Vol-2040/paper7.pdf.

11 Basel Committee on Banking Supervision. The Joint Forum: Outsourcing in Financial Services," February 2005. URL : https://www.bis.org/publ/joint12.pdf.

12 European Banking Authority. Risk Assessment of the European Banking System, December 2018. URL : https://eba.europa.eu/documents/10180/2518651/Risk_Assessment_Report_December_2018.pdf.

13 L. Õunapuu, Kvalitatiivne ja Kvantitatiivne Uurimisviis Sotsiaalteadustes, Tartu: Tartu Ülikool, 2014. URL : https://dspace.ut.ee/server/api/core/bitstreams/3538e168-6012-4e90-8484-4bb59be8b14a/content.

14 A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet. Taxonomy of Information Security Risk Assessment (ISRA). Computers & Security, vol. 57, 2016. pp. 14-30.

15 ISO/IEC. ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management, 2018. URL : https://www.iso.org/standard/75281.html.

16 ISO/IEC. ISO/IEC 27000 family. ISO, May 2019. URL : https://www.iso.org/isoiec-27001-information-security.html.

17 National Institute of Standards and Technology. NIST Special Publication 800-30: Guide for Conducting Risk Assessment. NIST. Gaithersburg, 2012. URL : https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

18 FAIR Institute. Measuring and Managing Information Risk: a FAIR Approach. URL : https://www.fairinstitute.org/fair-book.

19 R. A. Caralli, J. F. Stevens, L. R. Young, W. E. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon and Software Engineering Institute, 2007. URL : https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf.

20 COSO. Enterprise Risk Management - Integrated Framework. September 2004. URL : https://www.coso.org/Pages/erm-integratedframework.aspx.

21 Financial Sector Advisory Center of World Bank Group. Financial Sector's Cybersecurity: A Regulatory Digest," October 2017. URL :

http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf.

22 MITRE Corporation. MITRE ATTA&CK, 2018. URL : https://attack.mitre.org.

23 T. Casey. White Paper: Threat Agent Library Helps Identify Information Security Risks, September 2007. URL : https://pdfs.semanticscholar.org/391e/70510353ba762fa1580a6d9c002eefd2d86b.pdf .

24 ENISA. Threat Taxonomy. September 2016.URL : https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

25 MITRE Corporation. CVE Common Vulnerabilities and Exposures. MITRE Corporation, 2019. URL : https://cve.mitre.org.

26 National Institute of Standards and Technology. National Vulnerability Database. NIST. URL : https://nvd.nist.gov.

27 OWASP Foundation. OWASP Top 10, 2017. URL : https://www.owasp.org/images/7/72/OWASP_Top_10-017_%28en%29.pdf.pdf.

28 D. W. Hubbard. How to Measure Anything: Finding the Value of "Intangibles" in Business. Hoboken, New Jersey: John Wiley & Sons, Inc., 2007. URL : https://www.professionalwargaming.co.uk /HowToMeasureAnythingEd2DouglasWHubbard.pdf.

29 D. Kelly, C. Smith, Bayesian Inference for Probabilistic Risk Assessment: A Practitioner's Guidebook, London: Springer, 2011. URL : https://www.researchgate.net/publication/222596177_Bayesian_inference_in_probabilistic_risk_assessment-The_current_state_of_the_art.

30 M. Frigault, L. Wang, S. Jajodia and A. Singhal. Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks. in Network Security Metrics, Switzerland, Springer International Publishing AG, 2017. p. 1-23.

31 U. B. Kjærulff and A. L. Madsen. Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis, vol. II, New York: Springer, 2013. URL : https://link.springer.com/book/10.1007/978-1-4614-5104-4.

32 S. Cullen, P. Seddon and L. P. Willcocks. Domberger's Theory of Contracting Applied to IT Outsourcing," in Information Systems and Outsourcing, New York, Palgrave Macmillan, 2009, p. 130.

33 R. Pompon. IT Security Risk Control Management: an Audit Preparation Plan, Settle: Apress. 2016, p. 283-284.

34 Estonian Parliament. Riigi Teataja: Emergency Act. 1 July 2017. URL : https://www.riigiteataja.ee/en/eli/525062018014/consolide.

35 D. Singh. Outsourcing in Financial Services. Journal of Banking Regulation, vol. VI. no. 3, 2005. p. 202–204.

36 European Parliament and European Council. Directive 2014/65/EU "Markets in Financial Instruments Directive", 2014. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=ET.

37 European Parliament and European Council. Directive 2015/2366/EU "Payment Service Directive 2"," 25 November 2015. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

38 ENISA. Threat Landscape Report 2018 January 2019. URL : https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

39 Europol. Internet Organised Crime Threat Assessment (IOCTA). 2018. URL : https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

40 OWASP Top 10 project. Official OWASP Top 10 Repository, 2017. URL : https://github.com/OWASP/Top10/tree/master/2017/datacall/analysis.

41 MITRE Corporation. CWE List Version 3.2. MITRE Corporation, 11 December 2018. URL : https://cwe.mitre.org/data/index.html.

42 MITRE Corporation. CWE-287: Improper Authentication. January 2019. URL : https://cwe.mitre.org/data/definitions/287.html.

43 MITRE Corporation. Seven Pernicious Kingdoms. 3 January 2019. URL : https://cwe.mitre.org/data/definitions/700.html.

44 Tenable Inc. The Nessus Family. 2019. URL : https://www.tenable.com/products/nessus.

45 Offensive Security. OpenVAS Vulnerability Scanning. 2019. URL : https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/.

46 J. Pearl and T. S. Verma. A Theory of Inferred Causation. 1991. URL : https://ftp.cs.ucla.edu/pub/stat_ser/R156.pdf.

47 M. Scutari and J.-B. Denis, Bayesian Networks with Examples in R, London: CRC Press, 2015, p. 106-107.

Додаток А

Тези конференцій А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004

Д.О. Дисевич, В. І. Козак, А .Д. Головко, С. Т. Гаврись
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ХМАРНА ІНФРАСТРУКТУРА ДЛЯ СИСТЕМИ ПЛАТІЖНИХ ШЛЮЗІВ

D. O. Dysevuch, V. I. Kozak, A. D. Holovko, S. T. Havrys

CLOUD INFRASTRUCTURE FOR THE SYSTEM OF PAYMENT GATEWAYS

Внутрішні інфраструктури переносяться в хмару завдяки розширеним можливостям технічного управління, технічному вдосконаленню, а також гнучкості та економічно ефективним варіантам, які пропонує хмара. Крім того, архітектура підприємства змінюється, коли системи переміщуються в іншу інфраструктуру. Завдяки таким інфраструктурним змінам ризики безпеки можуть збільшуватися або зменшуватися, водночас можуть з'являтися нові ризики, а деякі ризики можна усунути. Ідентифікація активів для аналізу ризиків, заснована лише на моделюванні бізнес-процесів, не має інтеграції та представлення взаємозв'язку між IT-інфраструктурою та бізнес-процесами.

Отже, певними активами інформаційної системи можна знехтувати в аналізі ризиків. Під час аналізу ризиків безпеки двох інфраструктур необхідно врахувати відмінності в архітектурі підприємства, оскільки неідентифіковані активи інформаційної безпеки можуть бути вразливими та становити ризик для безпеки відповідної організації. У цій роботі активи ідентифікуються за допомогою архітектурного моделювання для виконання аналізу ризиків. Крім того, моделі представляють відмінності, що стосуються активів інформаційної безпеки у внутрішній інфраструктурі та хмарній інфраструктурі, на додаток до відображення відповідних бізнес-процесів. Моделювання загроз на основі STRIDE використовується для визначення ризиків безпеки, що стосуються активів ІБ, отриманих від архітектури підприємства.

Рівень хмарних технологій було змодельовано з використанням інформації, зібраної від популярних хмарних провайдерів, таких як OpenVAS, Amazon і Rack space. Представлена в роботі хмарна модель є узагальненою. Середовище хмарного центру обробки даних не є спеціальним, тому хмарні спільні орендарі можуть перебувати в одному гіпервізорі, навіть якщо мережа розділена. Доступ до послуг зберігання та спільного пулу ресурсів мають усі співкористувачі, підключені до сховища. Користувачі хмарного обслуговування вважаються поза сферою дії через дуже розподілену природу підтримки постачальників, задіяних у хмарних службах. Хмара має розширені функції, а використовувані технології відрізняються. Приклад: хмарна мережа даних. Основна архітектурна відмінність між хмарою та внутрішньою інфраструктурою полягає в тому, що хмара має компоненти, пов'язані з віртуалізацією. Комутатори, мережі в хмарі здебільшого є логічними розділеннями. Хмара має спільний пул ресурсів, щоб сприяти зростанню потреб у ресурсах. Тому доступ до сховища не можна відокремити від інших користувачів загальнодоступної хмари. У хмарній архітектурі також можна ідентифікувати ті самі бізнес-процеси завдяки припущенню, зробленому в рамках дослідження. Серед бізнес-процесів, змодельованих в обох інфраструктурах, буде взято до уваги обробку платіжних транзакцій. Розширення процесу платіжних транзакцій буде обговорено в розділі 4 для виявлення бізнес-активів. На рис. 1 представлено абстракцію хмарного центру обробки даних та інтеграцію з бізнес-процесами PayGate.