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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Зубенко Ольги Володимирівни*

академічної групи *125м-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Використання методики факторного аналізу інформаційних ризиків в процесі забезпечення кібербезпеки малих комерційних підприємств*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Зубенко О.В.* **академічної групи** ***1**25м-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Використання методики факторного аналізу інформаційних ризиків в процесі забезпечення кібербезпеки малих комерційних підприємств*

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Інформаційні ризики малих комерційних підприємств*

Предмет досліджень *Особливості застосування методики факторного аналізу інформаційних ризиків на малих комерційних підприємствах*

Мета *впорядкування процедури проведення аналізу та оцінки інформаційних ризиків на малому підприємстві*

Вихідні дані для проведення роботи *Вітчизняна та міжнародна правова база у сфері інформаційної та кібербезпеки, наукові публікації вітчизняних та іноземних авторів, офіційні статистичні дані , результати науково-дослідницької та переддипломної практик*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у визначенні особливостей застосування методу FAIR на малому комерційному підприємстві*

Практична цінність *полягає у розробці інструменту для вибору відповідної методики оцінки ризиків для малого комерційного підприємства; розробка рекомендацій щодо використання методу FAIR на малому комерційному підприємстві*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та бути поданим у вигляді, що дозволяє безпосереднє використання методу FAIR на малому комерційному підприємстві

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Аналіз нормативно-правової бази у сфері управління ризиками	03.09.18-06.10.18
Дослідження існуючих методів оцінки ризиків та їх порівняння	07.10.18-31.10.18
Розробка методичних рекомендацій для використання методу FAIR на малому комерційному підприємстві	01.11.18-24.11.18
Визначення капітальних та експлуатаційних витрат на реалізацію запропонованої методики	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від реалізації результатів роботи очікується позитивним завдяки зниженню можливого збитку на малих підприємствах від реалізації існуючих інформаційних загроз через зниження рівня інформаційних ризиків з використанням засобів управління ризиками та методичних рекомендацій з використання методу оцінки ризиків, що запропоновані у дипломній роботі*

Соціальний ефект *дипломної роботи полягає у підвищенні впевненості керівництва та працівників підприємства у його надійності з точки зору ефективності забезпечення безпеки інформації*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:

ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення»;

Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв, О.В. Кручінін – Дніпро:НГУ, 2018. – 52с;

Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет "Дніпровська політехніка", 2017. – 17 с.

Завдання видано _____ Тимофєєв Д.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Зубенко О.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 115 с., 9 рис., 14 табл., 5 додатків, 42 джерел.

Об’єкт дослідження: інформаційні ризики малих комерційних підприємств.

Предмет дослідження: особливості застосування методики факторного аналізу інформаційних ризиків (FAIR).

Мета роботи: впорядкування процедури проведення аналізу та оцінки інформаційних ризиків на малому підприємстві.

Методи дослідження: спостереження, порівняння, аналіз, опис.

В першому розділі проаналізовано теоретичну базу в сфері управління ризиками та досліджено існуючі кількісні методи оцінки ризиків.

В спеціальній частині наведено три способи порівняння запропонованих методів оцінки ризиків в метою вибору відповідної для використання на підприємстві. Розроблено спосіб порівняння, що враховує вимоги, відповідно до особливостей малого бізнесу. Наведено опис типового малого комерційного підприємства та розроблені методичні рекомендації для використання методу FAIR.

В економічному розділі обґрунтовано економічну доцільність застосування запропонованих методичних рекомендацій до методу FAIR на малому комерційному підприємстві з метою оцінки існуючих ризиків.

Наукова новизна полягає у визначенні особливостей застосування методу FAIR на малих комерційних підприємствах.

Практична цінність полягає у розробці інструменту для вибору відповідної методики оцінки ризиків; розробці методичних рекомендацій щодо використання методу FAIR на малому комерційному підприємстві.

ІНФОРМАЦІЙНИЙ РИЗИК, FAIR, АНАЛІЗ РИЗИКІВ, ОЦІНКА РИЗИКІВ, УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ, ФАКТОРНИЙ АНАЛІЗ ІНФОРМАЦІЙНИХ РИЗИКІВ, МЕТОД ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, АКТИВ, КІЛЬКІСНИЙ АНАЛІЗ.

РЕФЕРАТ

Пояснительная записка: 115 с., 9 рис., 14 табл, 5 прилож., 42 источников.

Объект исследования: информационные риски малых коммерческих предприятий.

Предмет исследования: Особенности применения методики факторного анализа информационных рисков (FAIR).

Цель работы: упорядочение процедуры проведения анализа и оценки информационных рисков на малом предприятии..

Методы исследования: наблюдение, сравнение, анализ, описание.

В первом разделе проанализирована теоретическая база в области управления рисками и исследованы существующие количественные методы оценки рисков.

В специальной части приведены три способа сравнения предложенных методов оценки рисков для выбора подходящей для использования на предприятии. Разработан инструмент для сравнения, что учитывает требования, в соответствии с особенностями малого бизнеса и разработаны методические рекомендации для использования метода FAIR.

В экономическом разделе обоснована экономическая целесообразность применении предложенных методических рекомендаций к методу FAIR на малом коммерческом предприятии с целью оценки существующих рисков.

Научная новизна заключается в определения особенностей применения метода FAIR на малых коммерческих предприятиях.

Практическая ценность состоит в разработке инструмента для выбора соответствующей методики оценки рисков; разработке методических рекомендаций для использования метода FAIR.

ИНФОРМАЦИОННЫЙ РИСК, FAIR, АНАЛИЗ РИСКОВ, ОЦЕНКА РИСКОВ, УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ, ФАКТОРНЫЙ АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ, МЕТОД ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ, УГРОЗА, УЯЗВИМОСТЬ, АКТИВ, КОЛИЧЕСТВЕННЫЙ АНАЛИЗ.

ABSTRACT

An Explanatory Note: 115 p., 9 fig., 14 tables., 5 add., 42 sources.

The object of this study is information risks of small commercial enterprises..

The subject of this study: features of the application of factor analysis of information risk (FAIR).

The purpose of the study: developing the procedure for carrying out the analysis and evaluation of information risks in a small enterprise.

Methods that were used: observation, comparison, analysis, description.

The first part of the study contains the theoretical framework in the field of risk management and an analysis of the existing quantitative methods of risk assessment.

The main part of the study considers three methods of comparing the proposed risk assessment methods for selecting an appropriate one for use in the enterprise. A comparison tool has been developed that takes into account the requirements in accordance with the characteristics of a small business and has developed guidelines for using the FAIR method.

In the economic part feasibility of applying the proposed guidelines to FAIR method in a small commercial enterprise in order to assess existing risks is substantiated.

Scientific novelty lies in determining the features of the application of the FAIR method in small commercial enterprises.

The practical value is contained in developing of a tool for selecting the appropriate risk assessment methodology; developing guidelines for using the FAIR method.

INFORMATION RISK, FAIR, RISK ANALYSIS, RISK EVALUATION, INFORMATION RISK MANAGEMENT, FACTOR ANALYSIS OF INFORMATION RISKS, INFORMATION RISK ASSESSMENT METHODS RISKS, THREATS, VULNERABILITIES, ASSETS, QUANTITATIVE ANALYSIS.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ДСТУ – державний стандарт України;

ІБ – інформаційна безпека;

ІР – інформаційний ризик;

ІТ – інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД — несанкціонований доступ;

ОАР – оцінка та аналіз ризиків;

ПЗ – програмне забезпечення;

СУІБ – систему управління інформаційною безпекою;

ENISA – The European Union Agency for Network and Information Security;

FAIR – Factor analysis of information risk;

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission.

ЗМІСТ

с.

ВСТУП..... 11
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ. 12
1.1 Аналіз поточного стану кібербезпеки. 12
1.2 Дослідження теоретичної бази у сфері управління інформаційними ризиками підприємств 18
1.3 Особливості використання інформаційних технологій на малому комерційному підприємстві 21
1.3.1 Аналіз ландшафту загроз на малому комерційному підприємстві 27
1.4 Застосування системного підходу до забезпечення кібербезпеки 30
1.5 Аналіз рекомендацій та підходів до управління аналізу та оцінці ризиків (АОР) 35
1.5.1 Аналіз основних стандартів з управління, аналізу та оцінки ризиків 46
1.6 Аналіз сучасних методик АОР..... 55
1.7 Постановка задачі..... 71
1.8 Висновки 73
РОЗДІЛ 2. РОЗРОБКА МЕТОДИЧНИХ РЕКОМЕНДАЦІЙ ДЛЯ ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ТА ОЦІНКИ РИЗИКІВ НА МАЛОМУ ПІДПРИЄМСТВІ 74
2.1 Визначення критеріїв обрання методу АОР 74
2.2 Розробка інструменту для підбору методики АОР для малого комерційного підприємства 77
2.3 Визначення відповідного методу АОР для типового малого підприємства України 81
2.4 Розробка методичних рекомендацій для використання методу FAIR на малому підприємстві..... 83
2.5 Висновки 86
РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА..... 87
3.1 Характеристика підприємства 87

3.2 Розрахунок витрат на проведення АОР на підприємстві 87
3.2.1 Розрахунок капітальних витрат на проведення АОР 88
3.2.2 Розрахунок експлуатаційних витрат на проведення АОР 90
3.3 Визначення загального економічного ефект від проведення АОР 90
3.4 Розрахунок економічної доцільності застосування методу FAIR на малому комерційному підприємстві 92
3.5 Висновки 93
ВИСНОВКИ 94
ПЕРЕЛІК ПОСИЛАНЬ 96
ДОДАТОК А. Відомості матеріалів дипломної роботи 101
ДОДАТОК Б. Перелік документів на оптичному носії 102
ДОДАТОК В. Відгук керівника економічного розділу 103
ДОДАТОК Г. Відгук від керівника дипломної роботи 104
ДОДАТОК Д. Методичні рекомендації з використання методу FAIR 105

ВСТУП

Питання кібербезпеки стосується інтересів не лише державних установ та інших об’єктів критичної інфраструктури, а і комерційних підприємств. Швидкий розвиток інформаційних та комунікаційних технологій призводить до виникнення нових засобів кіберзлочинності та постійний розвиток засобів, що використовуються для кібератак, що призводить до стрімкого зростання кібербезпеки.

Дослідження в області аналізу ризиків інформаційної безпеки проводилися безліччю вчених, серед яких можна виділити Горбенко І. Д., Корченко О. Г., Астахов А. М., Daniel Wentre, Thomas R., Швець, Г.А. Остапенко, Д.А. Котенко, І.Л. Алфьорова, А.Г. Кащенко, М.В. Тимоніна, T.R. Peltier, C. Kairab, C. Alberts, G. Brændeland, A. Papoulis, N.E. Fenton, M. Neil, M. Tailor, F.V. Jensen, і ін.

Над розв’язанням проблеми забезпечення інформаційної безпеки підприємств працювали А.П. Дикий, О.І. Захаров, Е.Е. Ібрагімов, Н.С. Іванова, О.О. Мельник, М.В. Наконечна, О.В. Орлик, Л.С. Сорока, В.Н. Ясенів. Різні аспекти захисту облікової інформації розглядали І.В. Горячківська, В.В. Євдокимов, І.Ю. Кравченко, Н.Л. Шишкова, В.А. Шпак та ін. Питання визначення загроз кібербезпеки під час захисту облікової інформації знайшли відображення у роботах Ю.Ю. Мороз, Ю.С. Цаль-Цалка, В.В. Сторож.

Аналіз опублікованих робіт і існуючих підходів показує, що відкритими залишаються ряд питань, пов'язаних з автоматизацією процесу отримання кількісної оцінки ризику в реальному часі, питання оцінки ймовірності реалізації загроз в умовах нестачі статистичних даних, питання використання суперечливих даних.

Основними завданнями дипломної роботи є проведення вибору відповідної методики для використання на типовому малому комерційному підприємстві та розробка методичних рекомендацій з впровадження АОР з використанням обраного методу.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз поточного стану кібербезпеки

Посилаючись на дані дослідження [25] кіберзагроз підприємствам у 2017 році, 9 з 10 компаній стикаються з зовнішніми кіберзагрозами. Результати дослідження показали, що рівень небезпеки в сфері інформаційних технологій надзвичайно високий. За останній рік 91% компаній, представники яких взяли участь у опитуванні, стикалися з загрозами інформаційній безпеці

Багато організацій постраждали від кіберзлочинців: наприклад, третина вірусних атак закінчилася втратою даних, при цьому для 10% фірм це була важлива для бізнесу інформація.

Перераховуючи кіберзагрози, які видаються найбільш значними, більшість учасників дослідження в усьому світі ставлять на перше місце віруси, шпигунське ПЗ і інші шкідливі програми (61%). Спам назвали джерелом загрози 56% респондентів. Третє місце (36%) зайняли фішингові атаки, за ними йдуть збої, викликані проникненням в корпоративну мережу (24%), і DDoS-атаки (19%). Розповсюдження шкідливих програм - найчастіша причина проблем з безпекою, яка випереджає в рейтингу спам і фішингові атаки. Однак, перші п'ять місць у рейтингу займають зовнішні загрози.

Рисунок 1.1 – Відсоткове співвідношення загроз для підприємств у 2017 році

У звіті також згадується, що 81% з опитаних українських компаній закривають співробітникам доступ до соціальних мереж.

Результати дослідження показують, що представники компаній добре обізнані про рівень небезпеки, однак ступінь захищеності бізнесу від кіберзагроз залишає бажати кращого: деякі компанії погано захищені, в ряді організацій обрані заходи захисту не відповідають характеру небезпеки і серйозності можливих наслідків для бізнесу.

В даний час витрати на забезпечення безпеки корпоративної мережі в рік складають в середньому 225 тисяч грн для малого бізнесу, 2 мільйона грн для середнього бізнесу і 90 мільйонів грн для великих корпорацій. Важливо відзначити, що більшість учасників дослідження вважають бюджет, що виділяється в їхніх організаціях на інформаційну безпеку, недостатнім і вимагає збільшення [25].

У 2017 році ENISA опублікували звіт «ENISA Threat Landscape Report 2017», де зазначались головні загрози за період 2017 року. Цей звіт є результатом однорічного збирання, аналізу та оцінки інформації, що стосується кіберзагроз, що знаходиться у суспільному надбанні [5].

Опитування, проведене в 2017 році, передбачало тісну співпрацю з CERT-EU, групою зацікавлених сторін ENISA та використовувало доступ до інформаційного порталу загроз CYJAX. За цей період не було виявлено жодної нової загрози, в порівнянні з 2016 роком, однак в рейтингу є чимало змін.

Методом фішинга було створено рекорде число порушення даних, який був виявлений в 2017 році.

Таблиця 1.1 – Топ загроз 2017 року за дослідженнями ENISA

№ п/п	Загроза	Стан рівня загрози на 2017 рік, в порівнянні з 2016 роком
1.	Зловмисне шкідливе ПЗ	без змін
2.	Атаки на веб-ресурси	підвищився
3.	Атаки на веб-додатки	підвищився
4.	Фішинг	підвищився
5.	Спам	підвищився
6.	Відмова в обслуговуванні	підвищився
7.	Шкідливе ПЗ, що блокує доступ до комп'ютерної системи, доки не буде виплачена сума грошей	підвищився
8.	Витік інформації через НСД	підвищився
9.	Внутрішні загрози	без змін
10.	Фізичне втручання/втрата чи крадіжка даних	без змін

Цього року, Уряд Великобританії опублікував офіційну статистику з питань кібербезпеки, а також витрати та наслідки кіберпорушень та нападів «Cyber Security Breaches Survey 2018». Окремим пунктом розглядались кіберззагрози у малому та мікро бізнесі. Були зазначені наступні дані:

- директори або керівництво мікро- та малих підприємств у 74% стверджують, що кібербезпека є високим пріоритетом;
- 42% підприємств виявили хоча б одне порушення або напад протягом останніх 12 місяців, що не нижче, ніж у 2017 році;
- майже в 17% випадках ці підприємства витратили добу чи більше, щоб відновитись після атаки;
- 70% підприємств вважають, що персонал, що займається кібербезпекою, має можливість ефективно керувати ним, у порівнянні з 81% середніх та великих підприємств [4].

На сайті CERT Australia є дані щодо відсоткового співвідношення країн, що постраждали від кібератак в період з 2015 до 2017 року. Цілями цих атак були як державні, так і приватні установи. За цими даними, Україна займає п’яте місце.

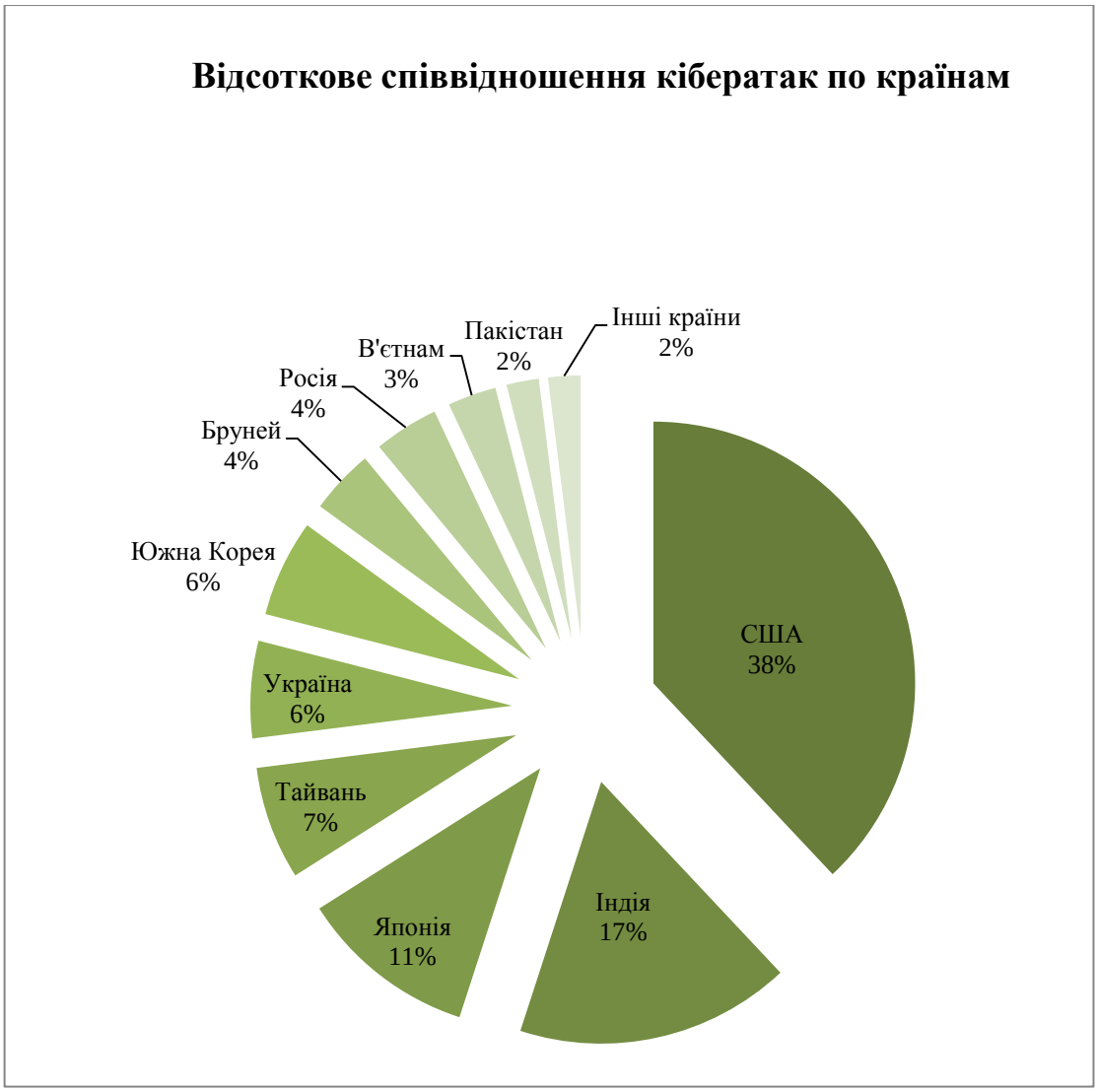

Рисунок 1.2 – Відсоткове співвідношення кібератак по країнам

На інтернет-ресурсі Habr кожний квартал публікують звіт Центра моніторингу інформаційної безпеки. Відповідно до даних звіту за перше півріччя 2018 року, було зафіксовано 112 млн. подій безпеки, що в два рази менше, ніж у попередньому півріччі та підтверджено 434 інцидентів.

Джерелами подій виступають мережеві і хостові IDS, мережеві пристрої, сканери захищеності, антивірусні рішення і honeypot'и.

В рамках внутрішньої обробки Центр класифікує інциденти в залежності від порушених ресурсів:

- висока критичність – інциденти, пов'язані з ключовими ресурсами серверного сегмента або з критичними ресурсами призначеного для

користувача сегмента (ресурси, що є критичними з точки зору бізнесу, фінансів або законодавства про інформацію);

- середня критичність – інциденти, пов'язані з некритичними ресурсами серверного сегмента;

- низька критичність – інциденти, пов'язані з некритичними ресурсами призначеного для користувача сегмента (рядовий користувач).

Рисунок 1.3 – Зафіксовані події ІБ

Серед виявлених 434 інцидентів:

Таблиця 1.2 – Зафіксовані інциденти ІБ

Клас інциденту	Низька критичність	Середня критичність	Висока критичність	Всього інцидентів	Частка інцидентів
Зловмисне ПЗ	3	75	101	179	41%
Атаки і спроби експлуатації вразливостей	4	68	57	129	30%
Підбір паролів	2	27	35	64	15%
Порушення політики ІБ	6	32	6	44	10%
DDoS	3	5	10	18	4%

За найбільшим класом - шкідливе ПЗ, спостерігаються наступні тенденції:

1. Чим більше вузлів на моніторингу - тим більше інцидентів з шкідливим ПЗ.

2. Як і в другому кварталі 2017 року тривають зараження шкідливими програмами WannaCry і Petya / notPetya. Незважаючи на загальне висвітлення цієї проблеми, все одно залишається дуже багато вразливих вузлів.

3. Більшість знайдених шкідливих файлів є ПЗ для майнінгу криптовалют. Тобто зловмисники намагаються заробити на ресурсах користувачів.

4. Також часто знаходимо рекламне потенційно-небажане ПЗ. В основному користувачі скачують його разом з зламаними або безкоштовними програмами і при установці ПЗ для швидкого пошуку драйверів, наприклад, DriverPack і аналоги.

У першому півріччі 2018 року найбільш часто піддавалися небажаному впливу саме призначені для користувача АРМ. Це 60% від усіх інцидентів на контрольовані ресурси. На другому місці розташувалися атаки на web-сервери і інші сервіси.

Необхідність забезпечення кібербезпеки на комерційних підприємствах зумовлено фактом, що протягом останніх років все ширше використання перспективних ІТ-технологій зумовило не лише численні переваги, а й цілу низку проблем. Зокрема, істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових загроз інформаційної безпеки, таких як нові форми кібератак [20].

Наведені дані свідчать про використання інформаційних технологій з метою здійснення зловмисної діяльності та унеможливлюють ігнорування питань в сфері кібербезпеки.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберзлочин – це суспільно небезпечне винне діяння у

кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [24];

Відсутність заходів, спрямованих на збереження інформації на підприємстві, де циркулює інформація, що не є власністю держави, впливає на ймовірність реалізації існуючих інформаційних загроз, що спричиняють матеріальні збитки.

Стає очевидним, що питання кібербезпеки мають бути у порядку денному кожного підприємства незалежно від його масштабів, рівня складності і характеру комерційної діяльності, а також усвідомлені усіма співробітниками підприємства. Зазначається, що, як правило, більшу ініціативу щодо зниження ризиків, які надходять від кіберзагроз, проявляють великі міжнародні компанії, хоча ті самі загрози та ризики рівною мірою поширюються також на представників малого бізнесу [22].

1.2 Дослідження теоретичної бази у сфері управління інформаційними ризиками підприємств

У зв’язку з тим, що останнім часом збільшується кількість незаконних фінансових операцій, крадіжок та шахрайства в мережі Інтернет, несанкціонованого використання чи модифікації програмного забезпечення, під час оцінки надійності систем інформаційної безпеки, мають бути змінені пріоритети від забезпечення традиційної інформаційної безпеки до кібербезпеки.

Управління інформаційною безпекою на підприємстві – це процес розробки, впровадження, моніторингу, підтримки та вдосконалення системи інформаційної безпеки.

Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового

комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [24];

Задачі забезпечення захисту інформації в куберпросторі виходять далеко за межі централізованого віддаленого управління антивірусами та іншими рішеннями. Вони становлять важливу частину менеджменту всієї організації, що забезпечує ефективність процесів і вирішення не тільки тактичних, а й стратегічних завдань.

Управління кібербезпекою - це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів по обробці ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг та аудит функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії [19].

Стандарт ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки» є українським стандартом, що заснований на міжнародному. Стандарт складається з рекомендацій щодо підвищення рівня кібербезпеки, розглядаючи різні аспекти цього питання та їхній зв’язок з іншими видами безпеки, зокрема: інформаційною безпекою; мережевою безпекою; Інтернет-безпекою; захистом інформаційної інфраструктури. У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі. Стандарт містить: огляд кібербезпеки; пояснення зв’язків між кібербезпекою та іншими видами безпеки; визначення зацікавлених сторін та їхньої ролі в кіберпросторі; настанова з вирішення основних питань кібербезпеки; способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки.

Міжнародний стандарт ДСТУ ISO/IEC 27032-2016 надає вказівки і перелік заходів щодо підвищення кібербезпеки в Інтернет, дотримуючись в цілому ризик-орієнтованого підходу в області інформаційної безпеки.

Використання рекомендацій стандарту, допоможе організаціям спланувати роботи по підвищенню рівня кібербезпеки ресурсів комп'ютерних систем, підключених до мереж загального доступу.

Специфічними особливостями стандарту можна назвати наступні:

- рішення задач підвищення готовності виключно шляхом протидії зловмисним загрозам,

- обмін інформацією та координація дій організацій є пріоритетним завданням забезпечення кібербезпеки.

Окрім того стандарт дає можливість встановити основні зв’язки між базовими поняттями кібербезпеки та основні зв’язки між ними. Вони зазначені на рисунку1.4.

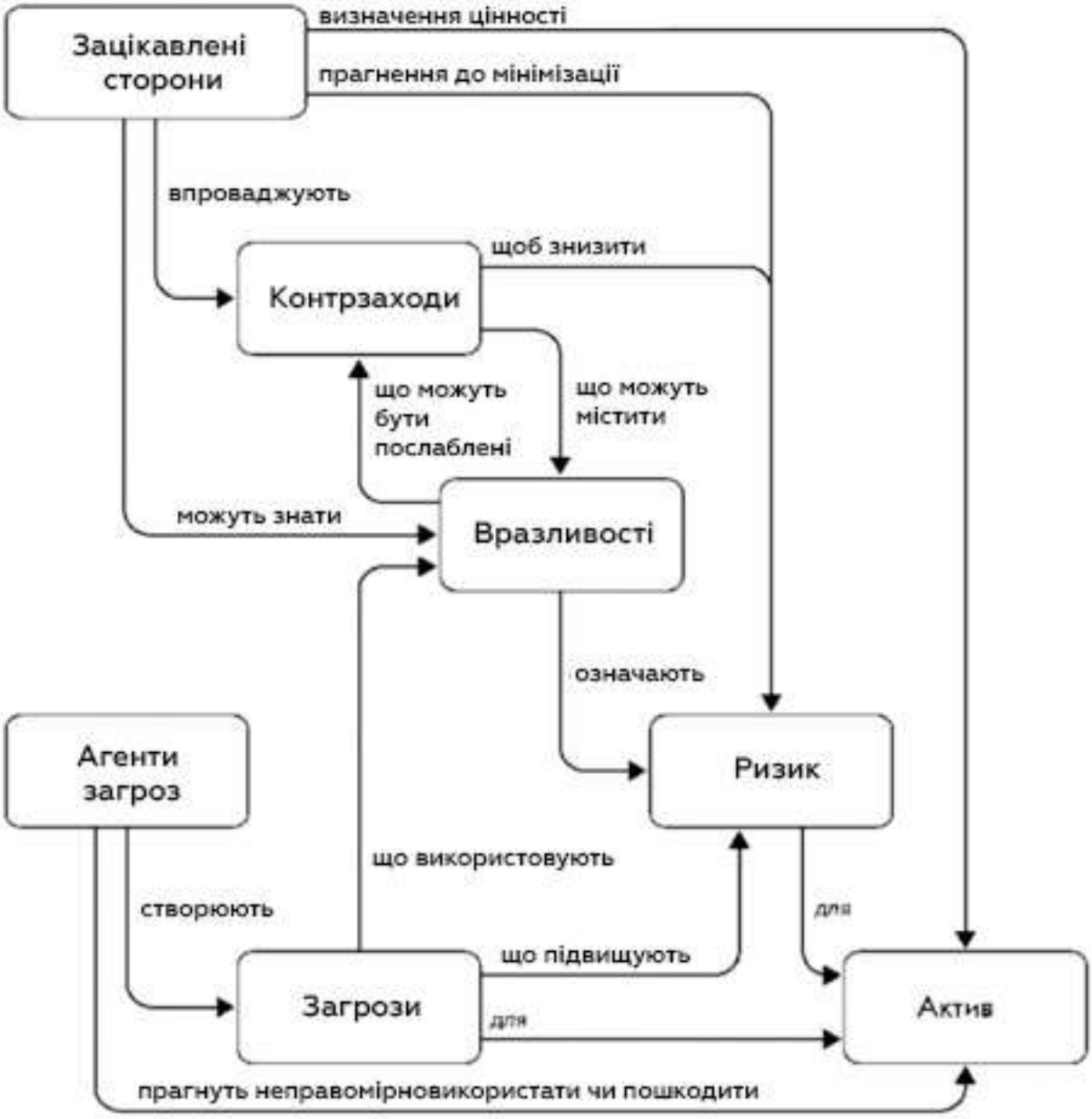

Рисунок 1.4 – Основні поняття кібербезпеки та характер зв’язків між ними

1.3 Особливості використання інформаційних технологій на малому комерційному підприємстві

Відповідно до Господарського Кодексу України, суб’єктами малого підприємництва є:

- фізичні особи, зареєстровані в установленому законом порядку як фізичні особи - підприємці, у яких середня кількість працівників за звітний період (календарний рік) не перевищує 50 осіб та річний дохід від будь-якої

діяльності не перевищує суму, еквівалентну 10 мільйонам євро, визначену за середньорічним курсом Національного банку України;

- юридичні особи - суб’єкти господарювання будь-якої організаційно-правової форми та форми власності, у яких середня кількість працівників за звітний період (календарний рік) не перевищує 50 осіб та річний дохід від будь-якої діяльності не перевищує суму, еквівалентну 10 мільйонам євро, визначену за середньорічним курсом Національного банку України [3].

Малі підприємства можна назвати найважливішим сектором сучасної ринкової економіки, адже вони найбільше розвиваються та впроваджують нові технології. Підприємства малого бізнесу в економічно розвинених країнах світу створюють від 50% до 70% від загального числа робочих місць.

В силу своєї масовості малий бізнес виступає одним з найважливіших споживачів комп'ютерних засобів і технологій. Велика потенційна місткість ринку збуту інформаційних технологій (IT) стимулює виробників розробляти спеціалізовані продукти, які враховують специфіку діяльності та особливості використання інформаційних технологій цією категорією суб'єктів економіки.

IT-інфраструктура - технічна основа для автоматизації процесів бізнесу. В останні десять років зробила величезний стрибок у своєму зміцненні і розвитку і продовжує діяти в цьому ж напрямку. До того ж одним з факторів, що сприяють освоєнню електронного бізнесу, є перехід до різної регламентованої електронної звітності, перш за все у сфері реєстраційної, митної і податкової системах.

Інформаційна підтримка для малого та середнього підприємництва стає найважливішим напрямком бізнесу. Якщо раніше впровадження інформаційних технологій було необхідно тільки для великих підприємств, то в даний час автоматизацію робочих процесів потребує і малий бізнес. Недостатня увага до розвитку на підприємстві інформаційної інфраструктури може призвести через деякий проміжок часу до великих неприємностей: починаючи від уповільнення робочих процесів до повної зупинки діяльності підприємства.

І керівники малих підприємств завжди бачать необхідність у застосуванні інформаційних технологій, вважаючи це виправданими витратами. Хоча автоматизація має на увазі те, що застосування ІТ-процесів для кожного підприємства індивідуально і направлено на раціоналізацію всіх наявних у компанії коштів.

Так, впровадження інформаційних технологій може відбуватися на різному рівні, починаючи від звичайного обліку і ведення документообігу в організації до активної політики фірми в мережі Інтернет (реклама, підтримка інтернет-магазину тощо).

Для здійснення торгового і бухгалтерського обліку існує багато готових рішень. (1С-бухгалтерія для України, M.E.Doc, клієнт-банкінг і багато ін.). До головних вимог відносять: оперативне оформлення документів, зручний спосіб розрахунків з контрагентами, взаємодія з бухгалтерією та іншими підрозділами в залежності від діяльності, здійснюваної підприємством.

На малих підприємствах використовують мережу Інтернету та засоби електронної комерції. По-перше, це величезні ресурси інформації, які містяться в глобальній мережі. По-друге, це можливість повного або часткового переведення бізнесу в електронний варіант. Так, електронна комерція здатна здійснювати різні види угод безпосередньо через Інтернет, що дозволяє компаніям знизити собівартість, що вкрай необхідно для належного розвитку малого бізнесу. Серед основних переваг переходу до електронної комерції: економія на кадрах, на оренду офісного приміщення, надання більш повної інформації про товар, реклама, просування, витрати на які значно нижче.

Також на сучасних малих підприємствах використовують:

- представлення бізнесу в мережі Інтернет;
- інформаційні бази внутрішні;
- створення та управління корпоративними ресурсами;
- інструменти для просування бізнесу в мережі Інтернет;
- програмне забезпечення для управління проектами;
- хмарні технології для бізнесу;

- зберігання даних як сервіс;
- сервіси для безперебійної роботи корпоративної мережі;
- забезпечення безпеки IT-інфраструктури тощо.

Малі підприємства виступають одними з найважливіших споживачів комп'ютерних засобів і технологій. Велика потенційна місткість ринку збуту інформаційних технологій стимулює виробників розробляти спеціалізовані продукти, які враховують специфіку діяльності та особливості використання інформаційних технологій цією категорією суб'єктів економіки [39].

Зрілість IT-інфраструктури малих підприємств в значній мірі залежить від інформаційної насиченості бізнесу, чисельності працівників, зайнятих інформаційною роботою, кількості комп'ютерів і оргтехніки, ступеня формалізації процесів управління.

Проте, для таких підприємств здебільшого інформаційні технології не є основним видом діяльності і вони мають свої особливості: невелика чисельність інформаційних працівників, в більшості своїй не мають розвиненої організаційної структури і чіткого поділу функціональних обов'язків; функції з обслуговування і забезпечення працездатності технічних засобів, програмного забезпечення виконує тимчасовий співробітник, або один з працівників підприємства в режимі реагування на виникаючі проблеми. Рішення про закупівлю і модернізацію програмного забезпечення, апаратних засобів спонтанні і безсистемні, приймаються керівником без чітко обґрунтування потреб і розрахунку ефективності витрат. Управління IT-інфраструктурою як усвідомлений бізнес-процес відсутній, відсутні і стандартизація процесів управління, IT-інфраструктура не ефективна, ненадійна, має місце низький рівень IT-безпеки. В силу невисокої залежності бізнесу від ефективності інформаційної роботи, фінансові втрати від збоїв в роботі комп'ютерної техніки незначні в порівнянні з великими підприємствами, але дуже значущі в масштабах даного малого підприємства.

Однак, малі підприємства відчувають потреби в автоматизації тих же функцій обліку та управління, що і великі підприємства. Управління стратегією

розвитку, персоналом, економікою, фінансами, маркетингом, виробництвом, збутом, постачанням, організація системи управління і звітності - життєво необхідні функції для діяльності малого підприємства. Менший масштаб діяльності відбивається лише на глибині реалізації цих функцій. Отже, використання програмних рішень, орієнтованих на великий бізнес економічно (висока вартість) і функціонально (глибока реалізація облікових функцій з більш високою складністю) для малого бізнесу не доцільно.

Звідси можна припустити, що більш затребуваними з боку малого бізнесу повинні бути інтегровані рішення, побудовані за принципом «все в одному».

Перспективним напрямком у вирішенні проблеми формування зрілої IT-інфраструктури підприємств малого бізнесу бачиться використання «Хмарних сервісів»: інфраструктура як послуга (Infrastructure as a Service, скор. IaaS); програмне забезпечення як послуга (Software as a Service, скор. SaaS); комунікація як послуга (Communications as a Service, сокр.CaaS) та інші.

Важливою особливістю підприємств малого бізнесу є єдність права власності та управління», коли власники виконують керівні функції. Тому, чим більше обізнаним є керівник в області можливостей і конкурентних переваг застосування IT, чим вище інформаційна насиченість бізнесу і більше розмір підприємства, тим більше схильне воно до впровадження інформаційних технологій.

Такі особливості малого бізнесу як вузька спеціалізація і багатовекторність, високі ризики і схильність до швидкої зміни діяльності, створюють додаткові проблеми у формуванні цілісної інфраструктури підприємства в зв'язку з суперечливими вимогами, що пред'являються до інформаційних систем. Багатовекторність діяльності ускладнює використання комплексних інформаційних систем, що функціонують за принципом «все в одному», ускладнює інтеграцію прикладних рішень від різних розробників. А схильність до швидкої зміни діяльності тягне за собою високі ризики вкладення ресурсів у придбання спеціалізованих програмних засобів, які незабаром можуть втратити актуальність. Компромісним варіантом є розробка невеликих

додатків для автоматизації специфічних бізнес-процесів доступними інструментальними засобами (наприклад, MS Office). Малі підприємства в своїй діяльності використовують особливі режими оподаткування, при необхідності переходячи з однієї системи на іншу в наявному порядку. Це накладає вимоги гнучкості до інформаційних систем.

В таблиці 1.3 зазначені особливості використання інформаційних технологій на малому підприємстві.

У сучасних реаліях будь-яке мале підприємство не може існувати окремо від інформаційних технологій. Широко використовують ІТ для пересилання електронних повідомлень, пошук нових клієнтів і партнерів в мережі Інтернет, використання месенджерів та соціальних мереж для спілкування і, що найважливіше, використання клієнт-банкінгу для проведення фінансових операцій та програм бухгалтерського обліку і звітності.

Таке стрімке інтегрування ІТ в малий бізнес передбачає підвищення рівня існуючих інформаційних загроз та виникнення нових.

Щорічно кількість кіберзагроз росте в кількісному і якісному відношенні. За даними дослідження [36], щодня з'являється близько 200 тисяч нових зразків шкідливого коду, що можуть бути використані проти інформаційної системи малого підприємства.

Таблиця 1.3 – Особливості використання інформаційних технологій в малому бізнесі

Особливість малих підприємств	Специфіка використання інформаційних технологій
Малий масштаб діяльності при збереженні більшості функцій управління	Потреба в широких за функціями інтегрованих системах, побудованих за принципом «все в одному»
	Здебільшого відсутність окремого спеціаліста, обов’язки з управління інформаційною інфраструктурою підприємства перекладаються на одного з робітників

Продовження таблиці 1.3 – Особливості використання інформаційних технологій в малому бізнесі

Особливість малих підприємств	Специфіка використання інформаційних технологій
Обмеженість ресурсів	Складність створення цілісної IT інфраструктури.
	Обмеженість у використанні широкого спектра програмних засобів і труднощі розробки власних ІС.
	Обмежені можливості залучення висококваліфікованих фахівців для створення і обслуговування IT
Єдність права власності та управління	Висока обізнаність керівника в галузі використання IT та збільшення розміру підприємства підвищують сприйнятливість до впровадження інформаційних технологій
Вузька спеціалізація в купі з багатовекторністю малих підприємств	Потреба в реалізації різнопланових функцій обліку та управління.
	Складність використання комплексних ІС в зв'язку з різноплановістю реалізованих функцій
Вибір (зміна) схем оподаткування	Потреба в швидких змінах при зміні системи оподаткування
Галузева специфіка	Вимагає використання спеціалізованого програмного забезпечення з більш високою вартістю

1.3.1 Аналіз ландшафту загроз на малому комерційному підприємстві

Серед загроз для малого підприємства можна виділити:

– крадіжка конфіденційної інформації - тип атаки, при якій зовнішні порушники або незадоволені працівники крадуть інформацію, яка є важливою для компанії;

– дефейс сайту - тип атаки, при якій сторінка web-сайту замінюється іншою сторінкою, найчастіше містить рекламу, загрози або викликають попередження;

– фішинг - тип атаки, при якій зловмисник отримує важливу інформацію (наприклад, логіни, паролі або дані кредитних карт) шляхом підроблення повідомлень від довіреного джерела (наприклад, електронний лист, складене як

легітимне, обманом змушує одержувача перейти по посиланню в листі, яка встановлює шкідливе програмне забезпечення на комп'ютер);

– програма-вимагач – тип шкідливого програмного забезпечення, що блокує доступ до даних на комп'ютері, в результаті чого злочинці вимагають викуп за те, щоб розблокувати заблоковані дані. Втрата даних через природних явищ або нещасних випадків.

Не варто забувати і про внутрішні загрози: витік даних, вразливості в програмному забезпеченні, шпигунстві тощо. Весь спектр зовнішніх і внутрішніх загроз ставить перед невеликими компаніями непросте завдання по створенню системи IT-безпеки, яка дозволить ефективно протистояти сучасним загрозам.

До основних проблем забезпечення кібербезпеки на малому підприємстві можна віднести: відсутність кваліфікованого персоналу (зазвичай функції фахівця з кібербезпеки виконує досвідчений користувач з числа штатних співробітників або, в кращому випадку, системний адміністратор), такі організації не проводять оцінку ризиків та реагують на інцидент після заподіяння збитків. Відповідно до недавнього дослідження «Лабораторії Касперського» і «B2B International», 96% опитаних IT-фахівців невірно оцінюють швидкість появи нових загроз, лише 4% опитаних дали близьку до реальності оцінку [36].

В малих підприємствах гостро стає проблема відсутності коштів, що стає причиною використання неліцензійного програмного забезпечення, не оновлюванні антивірусні бази, відсутність навчання персоналу компанії основам роботи з IT-системами.

Наявність та виникнення перелічених загроз підштовхують малі підприємства до необхідності впровадження заходів щодо забезпечення кібербезпеки на підприємстві.

Рисунок 1.5 – Поширені контрзаходи, що застосовують на підприємствах

Відповідно до статистичних даних, можна зауважити, що більшість компаній недооцінює ризики пов'язані з кіберзагрозами.

Деякі з них незначною мірою починають інвестувати в навчання співробітників, поясняти базові правила безпечної роботи в мережі Інтернет, тим самим підвищуючи рівень обізнаності про нові загрози. Починають з'являтися грамотні користувачі на робочих місцях, як основа для системи інформаційної безпеки компанії. Та здебільшого, питання інформаційної безпеки для малих підприємств відходять на задній план або взагалі не вирішуються. Співробітники компаній мають права адміністратора, повний доступ до всіх пристроїв і систем, що викликає безконтрольне використання ресурсів організації. Окремий захист потрібний при роботі з системами онлайн-банкінгу та іншими платіжними системами, що дозволить не допустити перехоплення параметрів доступу до рахунків шкідливими програмами. Невеликим компаніям потрібно універсальне рішення за розумну вартість, що відрізняється простотою установки і управління, яке дозволить гнучко налаштувати використання ресурсів компанії, а так само забезпечить комплексний захист від усіх типів загроз.

Успішний підхід в сфері кібербезпеки виражається у вигляді багаторівневого захисту, що охоплює комп'ютери, мережі, програми або дані,

які необхідно захистити. Співробітники, робочі процеси і технології повинні доповнювати один одного в організаціях, щоб забезпечити ефективний захист від кібератак. Забезпечити кібербезпеку на малих підприємствах доцільно через організацію системи управління інформаційної безпеки, що базується на системному підході.

1.4 Застосування системного підходу до забезпечення кібербезпеки

Система управління інформаційною безпекою складається з усіх заходів, спрямованих на досягнення і підтримку відповідних рівнів конфіденційності, цілісності та доступності [19].

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності інформації, забезпечення неможливості несанкціонованого доступу до інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) та ряду інших цілей.

Досягнення цих цілей можливо в ході вирішення завдань, таких як визначення відповідальних за інформаційну безпеку, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, в тому числі методи їх оцінки, контролінг інформаційної безпеки на підприємстві.

Основні функції СУІБ - це:

- виявлення і аналіз ризиків інформаційної безпеки;

- планування і практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

- контролювання цих процесів;

- внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на наступних принципах:

- комплексний підхід - управління ІБ має охоплювати всі компоненти ІС і враховувати всі актуальні чинники, які діють в інформаційній системі підприємства і за її межами;

- високий рівень керованості;

- ефективність - оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

- безперервність управління;

- процесний підхід - зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримку нерозривного зв'язку між етапами циклу, що дозволяє зберігати і постійно підвищувати якість СУІБ.

Серед основ побудови СУІБ вділяють наступні:

- визначити область застосування і межі СУІБ на підприємстві;

- визначити політику щодо СУІБ на підприємстві. Дана політика повинна визначати цілі управління захистом інформації, враховувати законодавчі, нормативні вимоги, визначати стратегії управління інформаційними ризиками, а також визначати спосіб оцінки ризиків організації;

- визначити підхід до оцінки ризику в організації;

визначити методологію оцінки ризику, яка підходить для СУІБ, а також відповідає встановленим законодавчим та нормативним вимогам захисту інформації. Обрана методологія оцінки ризику повинна гарантувати, що оцінки ризику дають порівнянні та відтворювані результати;

- розробити критерії прийняття ризиків і визначити прийнятні рівні ризику;

- виявити ризики; активи в рамках галузі застосування СМЗІ, а також власників цих активів; загрози для цих активів; вразливі місця, які можуть бути використані загрозами;

- проаналізувати ризик і оцінити рівні ризику, визначити, чи є ризики прийнятними або вимагають обробки з використанням критеріїв прийняття ризику;

- виявити і оцінити можливості для обробки ризиків (застосування відповідних засобів управління; свідоме та об'єктивне прийняття ризиків, за умови, що вони чітко відповідають політиці організації і відповідають критеріям для прийняття ризиків; уникнення ризику; передача пов'язаних ділових ризиків іншим сторонам, наприклад, страховим агентам;
- вибрати цілі управління і засоби управління для обробки ризику.

Можна говорити, що СУІБ є частиною загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Процеси управління інформаційною безпекою мають ієрархічність, тобто підпорядковані один одному:

Основним принципом є залучення до процесу забезпечення ІБ всіх співробітників організації, що взаємодіють з інформаційними ресурсами. Не менш важливо і те, що в основі будь-якого планування заходів по ІБ повинна лежати оцінка ризиків. Відсутність в організації процесів управління ризиками призводить до неадекватності прийнятих рішень і невиправданих витрат. Іншими словами, оцінка ризиків є тим фундаментом, на якому тримається СУІБ.

В Українському законодавстві прийнято ряд стандартів, що засновані на міжнародних стандартах на які спирається СУІБ, серед них діє ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги». Цей стандарт є тотожний переклад ISO/IEC 27001:2015 Information technology — Security techniques -- Information security management systems — Requirements. Стандарт можуть застосовувати організації усіх типів (комерційні підприємства, державні установи, некомерційні організації), які мають на меті розроблення та впровадження системи управління інформаційною безпекою (СУІБ) в організації.

Даний документ абстрагований від конкретних заходів щодо захисту, визначає загальну стратегію управління захистом інформації організації [37].

Цей міжнародний стандарт був підготовлений для того, щоб надати модель для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані і поліпшення Системи управління інформаційної безпеки (СУІБ). Рекомендується, щоб прийняття СУІБ було стратегічним рішенням для організації [10].

Згідно з документом необхідно застосовувати процесний підхід до управління захистом інформації.

Цей міжнародний стандарт приймає процесний підхід для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані і поліпшення СУІБ організації.

Процесний підхід до менеджменту захисту інформації, представлений в даному міжнародному стандарті, допомагає користувачам підкреслити важливість наступного:

- розуміння вимог захисту інформації та потреби встановити політику і цілі для захисту інформації організації;
- засоби реалізації та управління для менеджменту ризиками організації, пов'язаними із захистом інформації, в контексті загальних ділових ризиків організації;
- постійний контроль і аналіз якості виконання та результативності СУІБ;
- безперервне поліпшення, засноване на основі об'єктивних вимірювань.

Цей міжнародний стандарт приймає модель «Plan-Do-Check-Act» (PDCA), яка застосовується для структуризації всіх процесів СУІБ [34,110].

Цикл Шухарта-Демінга або системний підхід PDCA. При розгляді ризик-менеджменту з точки зору процесу здійснюється його умовний розподіл на чотири етапи: планування, реалізація, перевірка, дія. Ці етапи взаємопов'язані так, що вхід одного є виходом іншого, утворюючи тим самим безперервний процес або цикл. Родоначальником даного циклу вважають Вільяма Шухарта.

У своїх роботах вчений виділяє три стадії управління якістю: розробка специфікації, виробництво продукції, контроль виробленої продукції. Шухарт стверджував, що необхідно постійно покращувати якість продукції. Для цього він запропонував також процесний підхід не тільки при контролі над якістю, а й при організації виробничих зав'язків від операції до операції, обґрунтував необхідність організації виробництва не за процесом виробництва. Концепція Шухарта при безперервному поліпшенні якості отримала розвиток в роботах Едварда Демінга, який запропонував використовувати цикл PDCA: планування (Plan), реалізація (Do), перевірка (Check), дія (Act). В наші дні цикл PDCA є поширеною моделлю безперервного поліпшення процесів і застосовується в різних областях діяльності. Зокрема, ідеї даного циклу лежать в основі процесу менеджменту ризиків інформаційної безпеки і його інфраструктури.

Частина, що описує створення і управління СУІБ містить чіткі рекомендації в області оцінки і управління інформаційними ризиками.

Стандарт рекомендує проводити постійний контроль результативності СУІБ, аналіз цілей управління, беручи до уваги результати аудиту і статистику виникнення порушень, а також аналізувати оцінки ризику із запланованою періодичністю і аналізувати залишкові ризики та

Документ визначає коригувальні та запобіжні дії в сфері забезпечення захищеності організації.

Стандарт встановлює загальні принципи ведення захисту організацій в інформаційній сфері. Він відходить від конкретних практичних реалізацій, розглядаючи загальні організаційні моменти управління інформаційною безпекою систем. Важливо відзначити, що управління захищеністю організації в стандарті, який планується як основа для серії стандартів в області інформаційної безпеки, стрижневим підходом є аналіз і управління ризиками. Документ визначає порядок проведення даного аналізу, загальний характер роботи щодо забезпечення інформаційної безпеки організації.

Можна зазначити, що СУІБ базується на управлінні ризиками та полягає в плануванні та підтримці комплексу регламентів і процедур, спрямованих на

мінімізацію ризиків порушення інформаційної безпеки. Тобто, за своєю суттю управління інформаційною безпекою є управлінням інформаційними ризиками, націленим на досягнення прийнятного рівня цих ризиків.

1.5 Аналіз рекомендацій та підходів до управління аналізу та оцінці ризиків (АОР)

Все вищезазначене підтверджує, що необхідність управління інформаційними ризиками є важливим етапом для ефективного забезпечення кібербезпеки підприємства [37].

Отже, управління інформаційними ризиками є значущою частиною загального процесу побудови системи управляння інформаційною безпекою.

Щоб сформувати в усіх організаціях і функціональних підрозділах, незалежно від типу та сфери діяльності, єдине розуміння понять і термінів стосовно керування ризиками, використовують стандарт ISO Guide 73:2013 (ISO Guide 73:2009, IDT) «Керування ризиком. Словник термінів». У цьому стандарті наведено словник термінів, він забезпечує послідовне розуміння і узгоджений підхід до концепції управління ризиками і містить визначення загальних термінів, пов'язаних з ідентифікацією, аналізом, моніторингом, оцінкою, управлінням ризиком, а також процесами і менеджментом ризиків в цілому. Даний посібник призначено для використання особами, відповідальними за управління ризиками в організаціях, експертами і фахівцями, які беруть участь в діяльності ISO і IEC, розробниками національних і галузевих нормативних документів, що стосуються менеджменту ризиків.

В цьому стандарті визначається поняття «ризик» та використовується в цьому значенні в стандартах серії ISO 2700. Ризик – це вплив невизначеності на досягнення цілей. Примітки:

1. вплив - це відхилення від очікуваного (позитивне або негативне);

2. невизначеність - стан браку інформації, пов'язаної з розумінням події або знанням про нього, його наслідків або ймовірності;

3. ризик часто характеризується зазначенням можливих подій і наслідків, або їх комбінації;

4. ризик часто виражається у формі комбінації наслідків події (включаючи зміни в обставинах) і пов'язаної з ним ймовірності виникнення;

5. в контексті систем менеджменту інформаційної безпеки, ризики інформаційної безпеки можуть бути виражені як вплив невизначеності на досягнення цілей інформаційної безпеки;

6. ризик інформаційної безпеки пов'язаний з імовірністю того, що загрози будуть реалізовуватися використанням уразливості інформаційних активів або груп інформаційних активів і, тим самим, завдавати шкоди організації.

У стандарті Cobit 5 for Risk ризик визначається не як комбінація ймовірності події та її наслідків. COBIT 5 for Risk визначає інформаційний ризик як бізнес-ризик, він пов'язаний із використанням, володінням, експлуатацією, участю, впливом та прийняттям інформаційних технологій в рамках підприємства. Інформаційний ризик складається з подій, пов'язаних з IT, які потенційно можуть вплинути на бізнес.

Відповідно до Cobit 5 for Risk, інформаційний ризик завжди існує, незалежно від того, визначається чи визнається підприємством.

В американському стандарті NIST SP 800-30, інформаційний ризик визначається , як ризик, пов'язаний з експлуатацією та використанням інформаційних систем, що підтримують місії та ділові функції своїх організацій.

В українському законодавстві необхідність аналізу ризиків зазначається в НД ТЗІ: 1.1-002-1999 зі змінами від 28.12.2012 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», 3.7-003-2005 зі змінами від 28.12.2012 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній

системі», 1.4-001-2000 зі змінами від 28.12.2012 «Типове положення про службу захисту інформації в автоматизованій системі» [35].

Відповідно до цих документів, при побудові системи захисту інформації, має відбутись аналіз об'єкта захисту і можливих загроз. На підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. Подальші етапи створення системи захисту інформації, проводяться на підставі існуючого аналізу ризиків ІБ

Аналіз ризиків, до якого входять вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін. і визначається перелік суттєвих загроз. На цьому етапі уточнюють результати аналізу можливості керування ризиками, які виконані на попередніх етапах. На основі цього аналізу відбувається розробка політики безпеки інформації в ІТС.

Аналіз ризиків передбачає вивчення моделі загроз для інформації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в АС. Під час проведення аналізу ризиків необхідним є виконання наступних робіт [34]: визначення компонентів і ресурсів АС; ідентифікація загроз з об’єктами захисту; оцінка ризиків, оцінювання величини можливих збитків, пов'язаних з реалізацією загроз; визначення вимог до заходів, методів та засобів захисту.

Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені АС (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості АС внаслідок реалізації загрози. Для одержання оцінки можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків - відсутня,

низька, середня, висока, неприпустимо висока).

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

«Ризик являє собою функцію ймовірності реалізації певної загрози, виду і величини завданих збитків. Величина ризику може бути виражена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.).» [33].

До теперішнього часу накопичено достатній досвід і знання з аналізу ризиків, в тому числі і інформаційних. Зазначена проблематика вивчення інформаційних ризиків досить нова в порівнянні з фінансовими, банківськими та іншими ризиками. Але значимість її підвищується в міру зростання залежності бізнесу від інформаційних технологій [19].

Процес менеджменту ризиків інформаційної безпеки складається з:

- встановлення контексту;
- оцінки ризику;
- обробки ризику;
- прийняття ризику;
- обмін інформацією щодо ризику;
- моніторинг та перегляд ризику.

Рисунок 1.6 – Процес менеджменту ризиків інформаційної безпеки

Управління ризиком можна охарактеризувати як сукупність методів, прийомів і заходів, що дозволяють певною мірою прогнозувати настання ризикових подій і вживати заходів до виключення або зниження негативних наслідків настання таких подій [37]. Управління ризиками повинно бути інтегровано в загально організаційний процес, повинно мати свою стратегію, тактику, оперативну реалізацію. Важливо не тільки здійснювати управління ризиками, а й періодично переглядати заходи та засоби такого управління.

В процесі управління ризиком інформаційної безпеки виділяють два основні елементи: оцінка ризику і обробка ризику. Процес оцінки ризику

інформаційної безпеки складається з аналізу ризику та оцінювання ризику, а аналіз ризику до того ж складається з ідентифікації ризику і кількісної оцінки ризику.

В обов'язок кожного підприємства входить визначення методології оцінки ризику, яка найкращим чином відповідає конкретному підприємству.

За цим має відбуватися розгляд загроз і вразливостей з метою сприяння вибору засобів контролю (захисних заходів), пропорційних оцінці ризиків.

Далі за оцінкою ризику повинні бути прийняті рішення по обробці ризику: слід запобігати, переносити, приймати або знижувати ідентифіковані ризики. У тих випадках, коли рішенням, що випливають з оцінки ризику, є зниження ризику, повинні бути визначені відповідні засоби контролю для зниження ризиків до прийнятного рівня.

Здебільшого, величина ризику розраховується шляхом множення ймовірності виникнення ризику на відповідні наслідки. Але ці розрахунки можуть змінюватися відповідно до обраної методики оцінки ризику.

Ключовим етапом управління ризиками вважається етап вибору методів та інструментів управління ризиком.

Для ідентифікації ризиків проводиться аналіз бізнес-процесів підприємства. Результатом даного процесу є класифікований перелік всіх потенційних ризиків.

У зв'язку з тим, що наслідки від різних загроз нерівноцінні, недостатньо ідентифікувати ризик. Необхідно також оцінити величину загрози і можливість реалізації ризику, наприклад, у вигляді збитків в грошовому вираженні, а також ймовірність реалізації ризику.

Мета процесу оцінки ризиків полягає у визначенні характеристик ризиків в інформаційній системі і її ресурсах. Основним результатом даного процесу є перелік всіх потенційних ризиків з їх кількісними і якісними оцінками збитків і можливості реалізації.

Всі дані, які важливі з точки зору управління ризиками, моделюються, з допомогою обраної методики. Процеси всередині компанії стають прозорими, а

дані по управлінню ризиками – загальнодоступними, що і допомагає співробітникам здійснювати постійний моніторинг існуючих ризиків і виявляти нові.

На основі таких даних обираються необхідні засоби управління інформаційною безпекою. Для нашого прикладу: якщо величина і можливість збитків для ризику «Витік інформації про клієнтів до конкурентів» досить велика, то доцільно спланувати заходи щодо мінімізації ризику (наприклад, планування процесу оперативного оновлення програмного забезпечення інформаційної системи, формування регламентів доступу до інформації про клієнтів, впровадження засобів захисту від витоків конфіденційних даних і т.д.).

За результатами моніторингу здійснюється постійне оновлення розроблених документів і впровадження додаткових організаційних заходів. Менеджмент ризику є постійною діяльністю. Для нових інформаційних процесів і систем, а також систем обробки інформації, які перебувають на стадії планування, менеджмент ризику повинен бути частиною проектування і розробки. Для існуючих інформаційних процесів і систем менеджмент ризику повинен бути введений в будь-який момент. Коли плануються істотні зміни інформаційних процесів і систем, менеджмент ризику повинен бути частиною цього процесу планування. Він повинен брати до уваги всі інформаційні активи, процеси і системи в організації, а не застосовуватися до будь-якого з них ізольовано.

Процес управління ризиками містить безпосередньо організаційні і технічні заходи, які впроваджуються в процеси організації. Для підтримки постійної захищеності об'єкта на належному рівні необхідно розглядати питання забезпечення безпеки як безперервний процес. У зв'язку з цим, в рамках даної роботи процес менеджменту ризиків розглядається як цикл.

На етапі планування визначається контекст менеджменту ризиків, здійснюється ідентифікація активів і їх вразливостей, загроз, наслідків, а також

впроваджених контрзаходів. Крім того, визначається цінність активів і розробляється план обробки ризиків.

Аналіз ризиків – процедури виявлення факторів ризиків і оцінки їх значимості, по суті, аналіз ймовірності того, що відбудуться певні небажані події і негативно вплинуть на досягнення цілей підприємства.

Аналіз ризиків включає оцінку ризиків і методи зниження ризиків або зменшення пов'язаних із цим несприятливих наслідків.

Заключним етапом аналізу ризику є кількісна оцінка рівня ризиків. Кількісну оцінку ризику організація повинна здійснювати на основі результатів ідентифікації ризику. Для отримання кількісної оцінки ризику повинні бути скомпоновані всі складові ризику: наслідки та ймовірності.

Може бути проведено попередній аналіз, щоб ризики, наслідки яких вважаються низькими, були виключені з докладного вивчення. Виключені ризики повинні бути внесені в список, щоб продемонструвати повноту оцінки ризику.

Оцінка ризиків – це визначення кількісним або якісним способом величини ризиків.

Аналіз ризиків можна поділити на три види: якісний; кількісний та змішаний.

Кількісний аналіз ризиків повинен дати можливість чисельно визначити розміри окремих ризиків і ризику підприємства в цілому. Кількісний аналіз ризиків передбачає чисельне визначення величин окремих ризиків. Цей тип аналізу базується на теорії ймовірностей, математичній статистиці, теорії досліджень операцій. Кількісна оцінка використовує числові значення для наслідків і ймовірностей, а не описові шкали, які використовуються в якісній оцінці. При цьому застосовуються дані з різних джерел, в тому числі і дані власної статистики організації про інциденти за минулий період. Якість аналізу залежить від точності, повноти числових значень і від коректності використовуваних моделей.

«Кількісний» означає, що ризик визначається кількісно чи вимірюється за певними числами, цифрами та відсотками. Ця методологія відповідає на запитання «Які фінансові наслідки цього ризику?» та «Скільки даних буде втрачено чи скомпрометовано, якщо цей ризик буде реалізований?».

Щоб почати з кількісного аналізу ризиків, команда з оцінки повинна спочатку визначити основні активи бізнесу. Ця методологія оцінки ризику IT включає в себе такі фактори, як IT-обладнання, системи обробки даних та об'єкти, а також менш очевидні активи, такі як працівники, мобільні пристрої та самі дані, що знаходяться в системі. Коли всі основні активи ідентифікуються, обчислити вартість кожного в доларах. Це може бути складно зробити для неоднозначних або нестабільних активів, але це не повинно бути ідеальною наукою; оцінки в порядку. Для кожного ризику визначте, на які активи він вплине, і скільки цього активу буде втрачено чи скомпрометовано у відсотках. Потім просто візьміть відсоток втрат, помножений на вартість активу, щоб отримати суму збитків у доларах США для цього конкретного ризику.

Після оцінки кожного сценарію ризику, на підприємстві складають звіт про те, які активи піддаються ризику і який фінансовий вплив буде, якщо ризик буде реалізований. Це дозволяє керівництву приймати обґрунтовані рішення при розгляді контролю та гарантій захисту різних активів: якщо витрати на контроль перевищують суму, яка втрачається за сценарієм ризику, це не має фінансового сенсу для здійснення контролю, незалежно від того, чи втрата насправді відбувається.

Якісний аналіз має на меті ідентифікувати чинники, області та види ризиків. Цей тип аналізу ризиків дозволяє виявити і ідентифікувати можливі види ризиків, а також визначити і описати причини і фактори, що впливають на рівень даного виду ризику. Крім того, необхідно описати і дати вартісну оцінку всіх можливих наслідків гіпотетичної реалізації виявлених ризиків і запропонувати заходи щодо мінімізації або компенсації цих наслідків, розрахувавши вартісну оцінку цих заходів. Цей тип оцінки полягає в тому, щоб отримати якісний погляд на ризик. Замість цифр і відсотків, якісний підхід

відповідає на питання «як команда постраждає від цього ризику?» та «як втрати вплинуть на рівень обслуговування?». Цей метод є дуже суб'єктивним, на відміну від кількісного аналогу.

Якісну методику оцінки ризику ІТ-безпеки набагато простіше виконати, ніж кількісний аналіз, але дані менш точні. Замість того, щоб запитувати «скільки грошей ви втратите в цій ситуації?», якісний підхід запитує: «як ця ситуація вплине на продуктивність вашої команди?» Наприклад, при оцінці ризику сервісного кластера, оцінювач може запитати «як зміниться продуктивність вашої команди, якщо вона не зможе отримати доступ до своєї веб-програми?».

Результати якісної методології оцінки ризиків інформаційної безпеки подаються в вигляді звіту про те, які активи та системи є найважливішими для різних частин бізнесу. Комітет з оцінки не обов'язково знає фінансовий вплив, якщо ці системи були скомпрометовані, але вони зрозуміють, які бізнес-одиниці будуть зачеплені, і наскільки продуктивність буде втрачена при різних сценаріях ризику.

Етапи якісного аналізу ризиків:

1. Визначення можливих ризиків;

2. Опис можливих наслідків (збитків) реалізації виявлених ризиків і їх вартісна оцінка;

3. Опис можливих заходів, спрямованих на зменшення негативного впливу виявлених ризиків, із зазначенням їх вартості;

4. Вирішення можливості управління ризиками.

Методи експертної оцінки включають комплекс логічних і математично-статистичних методів і процедур, пов'язаних з діяльністю експерта з аналізу і прийняття рішень інформації. Експерт - це фахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію і т.п.) для знаходження найбільш ефективного вирішення.

Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу ризиків: опитувальники; SWOT-аналіз; метод Дельфі.

Оцінювання ризику інформаційної безпеки проводиться після аналізу ризику і завершує етап оцінки ризиків.

Змішана оцінка використовує як кількісні так і я кісні методики.

Здійснюється оцінка ризиків, за результатами якої вибираються необхідні контрзаходи. Документуванню підлягають всі стадії даного етапу, в тому числі, обґрунтування вибору відповідних контрзаходів для нейтралізації загроз.

Можна стверджувати, що для підприємств є переваги ризик-орієнтованого підходу до ЗІ. Організації, що управляють інформаційними ризиками, разюче відрізняються від тих, хто не приділяє цьому належну увагу. При такому підході керівнику набагато простіше зрозуміти, чому потрібно щось робити, що саме потрібно робити і скільки це буде коштувати.

Застосування ризик-орієнтованого підходу дозволяє:

- обґрунтувати необхідність реалізації певних заходів щодо забезпечення інформаційної безпеки;

- оптимізувати час на реалізацію заходів щодо забезпечення інформаційної безпеки;

- своєчасно ідентифікувати нові загрози і вразливості;

- оцінювати економічну ефективність обраних контрзаходів;

- оптимізувати витрати на забезпечення інформаційної безпеки;

- оцінювати ефективність служби інформаційної безпеки за допомогою аналізу повернення інвестицій [31].

1.5.1 Аналіз основних стандартів з управління, аналізу та оцінки ризиків

Процес управління інформаційними ризиками відбувається з використанням міжнародних чи регіональних стандартів. Найбільш ефективними та визнаними є серія стандартів ISO/IEC, Cobit 5 for Risk, NIST Special Publications 800 Series, BSI Standard 200-3, ERM COSO.

До національних стандартів України, що стосуються управління інформаційними ризиками та засновані на міжнародних стандартах відносяться:

- ДСТУ ISO 31000:2014 (ISO 31000:2009, IDT) «Менеджмент ризиків. Принципи та керівні вказівки». Даний стандарт є практичним документом, який спрямований на надання допомоги організаціям в розробці їх власних підходів до управління ризиками. Впроваджуючи стандарт, організація може порівняти свою практику управління ризиками з міжнародним досвідом.

Цей документ містить принципи і загальні керівні вказівки щодо ефективного виявлення та управління ризиками, тобто зовнішніми і внутрішніми факторами, які вносять невизначеність у досягнення цілей організації. Положення стандарту можуть бути застосовані до будь-якого типу ризику незалежно від його походження, може бути використаний в організації в цілому або її окремих частинах і різних видах діяльності, включаючи стратегії і рішення, операції, процеси, функції, проекти, товари, послуги та активи.

Область застосування стандарту охоплює будь-які державні та комерційні підприємства, асоціації, групи і фізичні особи.

- ДСТУ IEC/ISO 31010:2013 (IEC/ISO 31010:2009, IDT) «Керування ризиком. Методи загального оцінювання ризику». Цей стандарт є перекладом IEC/ISO 31010:2009 Risk management — Risk assessment techniques. У стандарті наведено систематичні методи загального оцінювання ризику.

Цей стандарт призначено для того, щоб викласти належні сучасні методики вибирання та застосовування методів загального оцінювання ризику,

у ньому не розглядають нові чи розроблювані концепції, щодо яких ще не досягнуто задовільного рівня професійного консенсусу. Він має загальний характер, тому він може слугувати настановою для багатьох галузей і типів систем.

Стандарт призначений для: збільшення ймовірності досягнення мети; заохочення активного управління; інформування про необхідність виявлення і усунення ризиків в масштабах всієї організації; покращення виявлення можливостей і загроз; вдосконалення фінансової звітності; підвищення ефективності управління; підвищення рівня довіри зацікавлених сторін; створення надійної основи для прийняття рішень і планування; покращення контролю; ефективного розподілу і використання ресурсів для усунення ризику; підвищення оперативної ефективності і дій; підвищення здоров'я і техніки безпеки, охорони навколишнього середовища; ефективного запобігання втрат; мінімізації втрат; покращення корпоративного навчання; покращення корпоративної стійкості.

- ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки». Цей стандарт надає настанови для управління ризиками інформаційної безпеки. Також підтримує основні концепції, визначені в ISO/IEC 27001, і розроблений для сприяння задовільному впровадженню інформаційної безпеки на основі підходу з управління ризиками. Знання концепцій, моделей, процесів і термінології, описаних в ISO/IEC 27001 та ISO/IEC 27002, дуже важливо для повного розуміння цього стандарту. Зазначений стандарт можуть застосовувати організації усіх типів (наприклад, комерційні підприємства, державні агентства, неприбуткові організації), які мають намір управляти ризиками, які можуть скомпрометувати інформаційну безпеку організації.

Відповідно до аналізу усіх документів, можна виділити, що стандарти серії ДСТУ ISO/IEC виносять оцінку ризику на систематичний розгляд:

• збитку, який, імовірно, може бути результатом порушення безпеки, беручи до уваги можливі наслідки втрати конфіденційності, цілісності або доступності інформації та інших активів;

• реальної ймовірності такого порушення, який проявляється в світлі переважаючих загроз, вразливостей і засобів управління, що застосовуються в даний час [37].

Стратегії аналізу ризиків ґрунтуються на декількох підходах: базовий підхід, неформальний підхід, детальний аналіз ризиків, змішаний підхід. [7,12]

Крім того, всі стандарти ISO/IEC серій 27000, 20000, 31000 та інші, що описують правила створення систем управління процесами, доповнюються та поєднуються між собою. Вищезазначені стандарти використовують процесний підхід, який розглядає управління як процес, а саме як набір взаємозв'язаних безперервних дій. Такий підхід робить наголос на досягнення поставлених цілей, а також на ресурсах, що використані для цього. Окрім того, стандарти вказаних серій використовують модель PDCA як структуру всіх процесів системи управління.

CobiT 5 є продуктом незалежної міжнародної асоціації аудиту і управління інформаційними системами ISACA [37].

Асоціація розвиває свою концепцію управління інформаційними технологіями відповідно до вимог ІБ. На основі цієї концепції описуються елементи інформаційної технології, даються рекомендації щодо організації управління, забезпечення режиму ІБ.

Модель управління CobiT описує універсальну модель управління інформаційною технологією. У моделі присутні ресурси інформаційних технологій, які є джерелом інформації, яка використовується в бізнес-процесі.

Цей стандарт являє собою всеосяжну структуру загальноприйнятих принципів, практик, аналітичних інструментів і моделей, які можуть допомогти будь-якому підприємству ефективно вирішувати найважливіші питання бізнесу, пов'язані з керівництвом і управлінням інформацією і технологіями.

У 2013 році ISACA опублікувала керівництво Cobit 5 for Risk, що увібрало в себе кращі ідеї і моделі інших стандартів з управління ризиками. Розглядаються IT-ризики в зв'язці з ризиками бізнесу, процес управління ризиками взаємодіє з іншими процесами в організації.

У документі наведено 111 типових сценаріїв ризиків. На них періодично даються посилання, наводяться докладні таблиці відповідності. В описі IT-процесів також наведені практичні рекомендації з управління IT-безпекою.

Крім того, COBIT вводить цілий ряд показників (метрик) для оцінки ефективності реалізації системи управління IT, які часто використовуються аудиторами IT-систем. В їх число входять показники якості і вартості обробки інформації, характеристики її доставки одержувачу, суми, пов'язані з суб'єктивним аспектам обробки інформації (наприклад стиль, зручність інтерфейсів).

Управління по COBIT можна представити в наступному вигляді (по порядку реалізації):

• стратегії (вибудовування IT-процесу по бізнес-цілям, постановка задачі, цілі та створення концепції IT-процесу; відповідальні: керівництво бізнес-підрозділів);

• політики (методи досягнення цілей в рамках стратегій, наприклад: «довжина пароля регламентується»; відповідальні: керівництво IT-підрозділів);

• стандарти (метрики для політик-методів, наприклад: «довжина пароля повинна складати не менше 8 символів»; відповідальні: керівництво IT-підрозділів);

• процедури (регламенти робіт для застосування політик-методів з використанням стандартів-метрик, робочі інструкції для виконавців; відповідальні: керівництво IT-підрозділів).

Стандарт відповідає всім потребам практики, зберігаючи незалежність від конкретних виробників, технологій і платформ. При розробці стандарту була закладена можливість використання його як для проведення аудиту IT-системи компанії, так і для проектування IT-системи. У першому випадку COBIT

дозволяє визначити ступінь відповідності досліджуваної системи кращих зразків, а в другому - спроектувати систему, майже ідеальну за своїми характеристиками.

Незважаючи на те що більша частина компонентів COBIT 5 описана в рамках п'яти принципів, є публікації і інструменти, які підтримують дотримання цих принципів, в них не входять.

В першу чергу, це рекомендації по впровадженню, викладені в книзі COBIT 5 Implementation - першої з групи публікацій під загальною назву Professional guides. Книга містить детальні рекомендації щодо реалізації принципів COBIT на трьох рівнях - управління організаційними змінами, управління програмами та постійного вдосконалення.

Варто зазначити, що у 2019 році очікується вихід наступної версії стандарту – Cobit 2019. Він поєднує і інтегрує понад 25 років розвитку в цій галузі, не тільки включивши нові уявлення з науки, але і впроваджуючи ці розуміння як практику.

Впроваджуються нові поняття та пояснюється термінологія - основна модель COBIT та її цілі управління та управління 40 забезпечують платформу для встановлення вашої програми управління

Очікується, що впровадження COBIT 2019 тепер є більш гнучким з новим керівництвом, яке пропонує як цільові проектні заходи для конкретних ситуації вирішення проблем або всебічне використання – можливе налаштування правильного рішення, яке відповідає унікальним потребам підприємства.

NIST Special Publications 800 Series (NIST - National Institute of Standards and Technology - американський національний інститут стандартизації). У його складі функціонує центр з комп'ютерної безпеки США - CSRC, який об'єднує фахівців федеральних служб, університетів, найбільших IT-компаній США. Центр публікує з початку 1990-х років Стандарти (FIPS) і більш детальні роз'яснення / рекомендації (Special Publications) в області інформаційної безпеки. Рекомендаціями (Special Publications), створеним CSRC, присвоюється код 800.

При створенні системи управління ризиками, використовують стандарти: NIST SP 800-30, NIST SP 800-39.

Стандарт США NIST 800-30 «Керівництво з інформаційними ризиками IT- -систем» - керівництво з аналізу та управління ризиками був розроблений Лабораторією інформаційної технології (ITL) Національного інституту стандартів і технології (NIST) США і представлені рекомендації в керівництві з аналізу та управління ризиками.

Відповідно до NIST SP 800-30 Методологія оцінки ризику охоплює дев'ять основних етапів (табл. 1): характеристика системи; ідентифікація загрози; ідентифікація вразливості; аналіз заходів захисту; визначення правдоподібності; аналіз впливу; визначення ризиків; рекомендації до заходів захисту; документація результатів.

У кожному етапі на основі логіки зв'язків з певної вхідної інформації виходить вихідна [27].

Імовірність реалізації загрози і рівень впливу оцінюються за шкалою: «висока», «середня», «низька». Оцінка ризиків здійснюється на основі компіляції отриманих оцінок: ймовірності реалізації загрози і рівня впливу. Кожному рівню за шкалою ставитися у відповідність деяке число. Також обговорюються значення рівнів ризиків. Цей процес пропонується здійснювати за допомогою матриці ризиків (табл. 2.2).

Після побудови матриці ризиків здійснюється опис рівнів ризику. Причому, відповідно до керівництва, значення рівнів ризику повинні виражати величину збитку ІС від впливу, якщо дана уразливість була б використана джерелом загрози, і напрямки діяльності посадових осіб ІС для кожного рівня ризику.

Далі пропонується підхід зниження ризику, який включає: розташування по пріоритетам, оцінку і здійснення рекомендованих в процесі оцінки ризиків заходів захисту. Посадовим особам ІС, які беруть участь в процесі оцінки та нейтралізації ризиків, на основі підходу «найбільша ефективність - найменша вартість», необхідно визначити заходи захисту для зниження ризику до

прийнятного рівня. У керівництві також пропонуються деякі стратегії і методи зниження ризиків.

BSI Standard 200-3: Risk Analysis based on IT Grundschutz Version 1.0 - британський стандарт від 2017 року, що заснований на методиці базового захисту IT від Федерального відомства з інформаційної безпеки Німеччини. Базовий захист IT (IT-Grundschutz) – це підхід від Федерального відомства з питань інформаційної безпеки (FSI) Німеччини є методологією для ідентифікації та впровадження заходів комп'ютерної безпеки в організації. Метою є досягнення адекватного та відповідного рівня безпеки для IT-систем. Для досягнення цієї мети FSI рекомендує «добре перевірені технічні, організаційні, кадрові та інфраструктурні гарантії» [10].

За допомогою BSI Standard 200-3, BSI забезпечує просту та зрозумілу процедуру, що дозволяє організаціям цілеспрямовано контролювати свої інформаційні ризики. Процедура заснована на елементарних загрозах, описаних у методиці IT-Grundschutz.

Коли застосовується методологія відповідно до IT-Grundschutz, оцінка ризику здійснюється непрямим чином для областей з нормальними вимогами захисту від BSI під час складання модулів IT-Grundschutz. Розглянуто лише ті загрози, які мають таку високу частоту виникнення або такі серйозні наслідки, які потребують гарантії безпеки. Типові загрози, що кожен повинен захищати себе, включають, наприклад, шкоду, спричинену пожежею, водою, крадіжкою, зловмисним програмним забезпеченням або апаратні дефекти. Цей підхід має перевагу тим, що користувачі IT-Grundschutz не повинні виконувати окремий аналіз загрози та уразливості в основній частині інформаційної системи, оскільки ця оцінка вже була заздалегідь виконана BSI.

Цей стандарт можна використовувати, коли компанії чи державні установи вже успішно працюють з методологією IT-Grundschutz відповідно до BSI Standard 2002-2 і хотіли б безпосередньо додати аналіз ризиків до IT-Grundschutz. Залежно від основних умов організації та типу інформаційної системи, може бути доцільним використання іншої встановленої практики або

адаптованої методології аналізу інформаційних ризиків як альтернативи стандарту BSI Standard 200-3.

Цей документ описує методологію аналізу ризиків. Список елементарних загроз, що містяться в Комплекті IT-Grundschutz, використовується як допомога.

ERM COSO (Комітет організацій-спонсорів Комісії Тредвея (англ. The Committee of Sponsoring Organizations of the Treadway Commission, COSO) – є добровільною приватною організацією, створеною в Сполучених Штатах і призначеної для вироблення відповідних рекомендацій для корпоративного керівництва по найважливішим аспектам організаційного управління, ділової етики, фінансової звітності, внутрішнього контролю, управління ризиками компаній і протидії шахрайству.

Рамкова програма COSO була розроблена, щоб допомогти підприємствам створювати, оцінювати та вдосконалювати свій внутрішній контроль. Важливість внутрішнього контролю в операціях та фінансовій звітності суб'єкта господарювання не може бути надмірно наголошеною, оскільки існування або відсутність процесу визначає якість випуску, виробленого у фінансовій звітності. Діючий та діючий процес внутрішнього контролю надає користувачам «розумну впевненість» в тому, що суми, представлені у фінансовій звітності, є точними та можуть бути використані для прийняття обґрунтованих рішень.

Інтегрована система внутрішнього контролю COSO має три компоненти, які включають:

1. Контрольне середовище: середовище управління являє собою набір стандартів, процесів і структур, що є основою для здійснення внутрішнього контролю в організації.

2. Оцінка ризику: кожен суб'єкт господарювання стикається з різними ризиками від зовнішніх та внутрішніх джерел. Ризик визначається як можливість того, що подія відбудеться та негативно вплине на досягнення цілей. Оцінка ризику передбачає динамічний та ітераційний процес визначення

та оцінки ризиків для досягнення цілей. Отже, оцінка ризиків є основою для визначення того, як керувати ризиками.

3. Контрольні заходи - це дії, встановлені політикою та процедурами, які допомагають забезпечити виконання директив керівництва з метою пом'якшення ризиків для досягнення цілей. Контрольні заходи виконуються на всіх рівнях суб'єкта, на різних етапах бізнес-процесів та в технологічному середовищі.

Вісім компонентів управління ризиками включають попередні три компоненти концептуальних основ внутрішнього контролю розширених для задоволення зростаючого попиту на ризик управління: внутрішнє середовище, постановка цілей, визначення подій, оцінка ризиків, реагування на ризик, засоби контролю, інформація та комунікації, моніторинг.

У 2017 було представлено новий документ ERM Framework Update від Coso. «Концептуальні засади управління ризиками організації» COSO представляють собою один з найбільш відомих і часто використовуваних в світі документів, присвячених питанням управління ризиками. Новий документ «Концептуальні засади управління ризиками організації: інтеграція зі стратегією і управлінням діяльністю» COSO 2017 був підготовлений для того, щоб організації по-новому підходили до обговорення питань, пов'язаних з управлінням ризиками. На думку COSO зміщення фокусу з управління ризиками різних бізнес-функцій на підхід, який передбачає проактивне виявлення і використання нових можливостей на рівні організації, буде сприяти створенню додаткової цінності і підвищенню якості продуктів і послуг.

В оновленому документі визнається нова структура концептуальних основ: п'ять компонентів і 20 принципів, узгоджених з життєвим циклом бізнесу. Така структура дозволяє проводити більш зрозуміле обговорення ризиків в контексті діяльності організації.

1.6 Аналіз сучасних методик АОР

В зазначених стандартах з управління інформаційними ризиками відсутні вимоги щодо використання конкретних методик для оцінки та аналізу ризиків. До загальних вимог відносять: можливість виявлення критеріїв для прийняття ризика; можливість ідентифікації прийнятних ризиків; можливість проведення, ідентифікації та оцінки ризиків; перекриття всіх аспектів СУІБ.

На сьогоднішній день існує безліч інструментальних засобів і методик управління інформаційними ризиками, під якими мається на увазі визначення параметрів ризику, аналіз і оцінка ризику (АОР), а також визначення операцій над ризиками. Часто перед фахівцями компанії для підвищення ефективності вирішення завдань захисту інформації виникає питання про вибір відповідної методики, що задовольняє поточним вимогам інформаційної безпеки підприємства [29].

Актуальність кількісних методик обумовлена необхідністю вирішення різних оптимізаційних задач, які часто виникають в реальному житті. Суть цих завдань зводиться до пошуку єдиного оптимального рішення з безлічі існуючих.

На практиці такі методики управління ризиками дозволяють:

- створювати моделі інформаційних активів компанії з точки зору безпеки;
- класифікувати і оцінювати цінності активів;
- складати списки найбільш значущих загроз і вразливостей безпеки;
- ранжувати загрози і вразливості безпеки;
- обґрунтовувати засоби і заходи контролю ризиків;
- оцінювати ефективність / вартість різних варіантів захисту;
- формалізувати й автоматизувати процедури оцінювання та управління ризиками.

Процес оцінки ризику починається з інвентаризації інформаційних ресурсів. Переглядаючи інформаційні активи, організація може переглянути, які з них представляють найбільші ризики інформаційної безпеки.

Основа оцінки ризиків інформаційної безпеки полягає у визначенні впливу та ймовірності негативного впливу на дані. Незалежно від використання якісної чи кількісної методики, компанії повинні розглянути кожну виявлену загрозу, що стоїть перед кібербезпекою. Після визначення загроз, роблять інвентаризацію інформаційних активів, щоб визначити, який вплив має порушення.

Наприклад, анонімне порушення бази даних може мати дуже незначний організаційний вплив. За відсутності інтелектуальної власності чи даних клієнта цей тип порушень не має фінансового впливу для компанії.

У 2006 році Агентство Європейського союзу з мережевої та інформаційної безпеки ENISA опублікувала список методів та інструментів доступний для оцінки ризиків, що найбільш широко використовуються.

Було розглянуто 17 методів, кожен метод був описаний за допомогою шаблону, що складався з 21 атрибута, які найбільше описують характеристики методу.

Розглянуті методи були обрані спеціальною робочою групою ENISA з технічних та політичних аспектів оцінки ризиків та управління ризиками ENISA-WG. Членами робочою групи були експерти з восьми держав-членів ЄС. Вони розглянули тільки найбільш відомі методи, тому даний аналіз не містить повного списку методів та стандартів, що стосуються ризиків IT. Специфічні методи були навмисно виключені з опитування:

- довідкові документи на високому рівні, такі як Довідник ISO 73;
- методи, які не класифікуються як методи оцінки та аналізу ризиків, відповідно до визначень, що використовуються;
- невідомі методи, які методи не можуть бути досліджені, оскільки відповідні документи не були доступні членам робочої групи;

- методи, орієнтовані на загальне керівництво та корпоративне управління (наприклад, Cobit 5, Basel II).

Більшість з цих 17-ти методів припинили оновлення та їх використання у сьогоденні є недоцільним. Однак, декілька з них мають своєчасну підтримку та постійне оновлення, а саме:

- методика, що розроблена Форумом інформаційної безпеки ISF Methods. Відповідно до звіту ENISA, ISF Methods глибоко охоплює всі аспекти (ідентифікація ризиків, аналіз ризиків, оцінка ризиків, оцінка ризиків, ліквідація ризику, прийняття ризиків, передача ризиків);
- Mehari, розроблена Clusif Club de la Security de l'Information Francais.

Беручи до уваги вищезазначені проблеми, що мають малі комерційні підприємства, для них доцільно використовувати кількісну методику оцінки ризиків. Така методика, з використанням програмного забезпечення, полегшує здійснення кількісних розрахунків для оцінки ризиків буде ефективнішою та просторішою в використання на малих підприємствах. Адже, кількісні оцінки забезпечують чіткі дані, що полегшують прийняття рішень.

За допомогою результату в цифровому вигляді, підприємство може вирішувати як виконувати контроль над ризиком, та чи є контрзаходи доступними і економічно ефективними. Ці цифри дозволяють провести дуже простий аналіз витрат для кожного контрзаходу та загрози активу.

Тому надалі будуть розглядатися лише методики кількісного аналізу інформаційних ризиків.

Нижче наведені короткі описи поширених методик кількісного аналізу ризиків. Серед найбільш ефективних, що використовуються на практиці виділяють наступні: RiskWatch, Mehari, FAIR, CIS RAM, IRAM2, Mitre.

Характеристики обраних методик:

1. У 1993 році американська компанія **RiskWatch** почала розробку спеціалізованого програмного забезпечення для оцінки ризиків і відповідності вимогам, яке може використовуватися для забезпечення фізичної безпеки, інформаційної безпеки, відповідності FFIEC, HIPAA тощо.

Сьогодні компанія пропонує три продукти, що забезпечують розширену оцінку ризику і захист від динамічного ландшафту загроз. У сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки. Воно включає в себе наступні засоби аудиту та аналізу ризиків: SecureWatch, ComplianceWatch та CyberWatch.

SecureWatch дозволяє керувати ризиками, проводити моніторинг та підтримку безпеки. ПЗ дозволяє налаштовувати свої критерії оцінки та показники для стандартизації, а також виконання оцінки фізичної безпеки.

Використання продукту відбувається в декілька кроків:

• визначення предмета дослідження, організація об’єктів захисту: фізичні об'єкти інформаційної діяльності, інформаційні активи, постачальники тощо. Пропонується заповнити опитувальники та контрольні списки, ідентифікувати активи, заповнити інформацію про злочини та інциденти для сприяння аналізу ризиків. На даному етапі описуються параметри організації - тип організації, склад досліджуваної системи, базові вимоги в області безпеки. Далі кожен з обраних пунктів описується детально. Для полегшення роботи аналітика в шаблонах даються списки категорій ресурсів, втрат, погроз, вразливостей і заходів захисту. З них потрібно вибрати ті, що реально присутні в організації. Для виявлення можливих вразливостей використовується опитувальник, база якого містить більше 600 питань. Питання пов'язані з категоріями ресурсів. Допускається коригування питань, виключення або додавання нових. Здається частота виникнення кожної з виділених загроз, ступінь уразливості і цінність ресурсів. Все це використовується в подальшому для розрахунку ефективності впровадження засобів захисту;

• кількісна оцінка ризиків: визначення оцінки ризику на основі показників і вразливостей безпеки / відповідності, виявлених в ході опитувань. Спочатку встановлюються зв'язки між ресурсами, втратами, загрозами і уразливими, виділеними на попередніх етапах. Додатково розглядаються сценарії «що якщо ...», які дозволяють описати аналогічні ситуації за умови впровадження засобів захисту. Порівнюючи очікувані втрати за умови впровадження захисних

заходів і без них, можна оцінити ефект від таких заходів. В якості критеріїв для оцінки і управління ризиками використовуються прогнозування річних втрат (Annual Loss Expectancy, ALE) і оцінка повернення від інвестицій (Return on Investment, ROI). Для розрахунку річних втрат використовується формула:

ALE = Цінність ресурсу * Фактор експозиції * Частоту.

- створення плану дій для відстеження та управління ризиками;
- генерація звітів за допомогою інструменту звітності, що створює призначені для користувача звіти з повною інформацією про організацію. Панелі звітів автоматично генеруються разом з даними, що були введені. Проводиться візуалізація ризиків всієї організації за допомогою оціночної карти ризику. Після проходження цих кроків, для аналітиків в звіті надається наступна інформація: діаграма відповідності вимогам стандарту, діаграма яким саме вимогам не відповідає дані відповіді на запити, таблиця детального уявлення відповідності і невідповідності вимогам стандарту, діаграма втрат.

Типи звітів:

- короткі підсумки;
- повні і короткі звіти про елементи, описаних на стадіях 1 і 2;
- звіт про вартість ресурсів, що захищаються і очікуваних втрат від реалізації загроз;
- звіт про загрози та заходи протидії;
- звіт про результати аудиту безпеки.

ComplianceWatch використовується для проведення аудиту, аналіз на відповідність нормативним вимогам та для виявлення вразливостей. Це ПЗ є інструментом оцінки відповідності до вимог міжнародних стандартів. Він підходить для компаній, чиї потреби зосереджені на обов’язковому дотриманню нормативних вимог.

Доцільним для забезпечення кібербезпеки є використання ПЗ CyberWatch.

CyberWatch – рішення з управління ризиками інформаційної безпеки, що оцінює кіберризики шляхом створення реєстрів ризиків для активів задля зменшення вірогідності настання кібератак. Для роботи з ПЗ необхідно:

- визначити область оцінки;
- визначити і додати активи організації, загрози для активів організації та вразливості, що існують;
- створити сценарії загрози на основі активів, загроз та вразливостей організації;
- обрати контрзаходи для керування ризиками.

Панель інструментів дозволяє оцінити кіберризик в різних областях організації, визначити, які області високого ризику вимагають додаткової оцінки.

CyberWatch допомагає оцінити ефективність існуючих контрзаходів, а Cyberwatch's Threat Framework миттєво створює сценарії загроз з притаманними ризиками для кожного нового активу, який був доданий в програмне забезпечення.

Недоліки продуктів RiskWatch:

- для комплексного керування та проведення АОР на підприємстві необхідно придбати три види ПЗ та оновлювати бази кожного окремо;
- такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних і адміністративних чинників;
- отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпує розуміння ризику з системних позицій - метод не враховує комплексний підхід до інформаційної безпеки;
- програмне забезпечення RiskWatch існує тільки англійською мовою.

2. Методологія **Mehari** була розроблена французькою некомерційною організацією CLUSIF (Club De La Securite De L'information Francais), мета якої здійснення обміну досвідом між фахівцями сфери безпеки інформаційних технологій.

Методика Mehari має відкриту архітектуру і складається з декількох документів-модулів: модуля оцінки ризиків, модуля аналізу та класифікації можливих втрат, оцінки сервісів безпеки, впроваджених в організації і бази знань загроз. У сукупності ці модулі дозволяють не тільки здійснювати оцінку ризиків, але і управління ними відповідно до вимог міжнародних стандартів. Методологія Mehari надає собою структурований підхід до оцінки ризиків. Вона дає можливість якісно і кількісно оцінити фактори ризику і УР.

Для оцінки пропонуються два основні варіанти - використовувати бази Microsoft Excel, OpenOffice або ПЗ Risicare яке забезпечує більш багатий користувальницький інтерфейс, а також дозволяє моделювати, візуалізувати і оптимізувати отримані результати.

ПЗ для моделювання ризиків Risicare є також продуктом CLUSIF, що розроблений для методики Mehari. Risicare розраховує ризики, проводить імітацію реалізації сценарія ризиків та перевіряє ситуації «що буде, якщо».

Risicare розглядає комбінацію аналізу ставок, класифікацію активів, аналіз уразливості і вивчення ситуацій ризику для виявлення ризиків у відповідності зі способом Mehari.

Підхід до аналізу ризиків, який використовується Risicare, заснований на базі знань про загрозу в і автоматизованих процедурах оцінки факторів зниження ризику.

Оцінка ризику: Risicare полегшує виконання розрахунків для оцінки ризиків і дає оцінку серйозності ризику (з комбінацією потенційності і впливу).

Оцінка ризику: Risicare аналізує кілька ситуацій загрози (з набором сценаріїв), щоб визначити серйозність кожного ризику для кожного активу і вказати найбільш серйозну для організації.

Risicare може відображати фази зниження ризику на основі запланованих поліпшень і цільових термінів їх досягнень.

Risicare генерує:

- детальні звіти
- графіки

- короткострокові і довгострокові плани безпеки

Останнє оновлення ПЗ проводилось у 2007 році, тому можна зазначити, що наразі Risicare має морально застарілий інтерфейс [12].

У методиці Mehari використовується структурована модель ризику, яка враховує «фактори зниження ризику». Процес АОР реалізується в 9 етапів: ідентифікація ризику; оцінка впливу; оцінка стримуючих чинників; оцінка захисних, паліативних та рекуперативних чинників; оцінка потенційності; оцінка впливу; оцінка впливу після вжиття заходів щодо зниження і показників скорочень впливу; глобальна оцінка ризиків; прийняття рішення про прийнятність або неприйнятність ризику.

Для кожного етапу надані прикладні засоби Mehari: практичні рекомендації, таблиці, розрахункові формули, та шкали оцінок. Супутня документація містить інструкції та поради щодо ефективного використання бази знань (подана у форматі Excel), а також теоретичні відомості щодо управління ризиками ІБ. Метод Mehari використовує трьохфакторну модель ризиків ІБ, елементами якої є: імовірність реалізації загрози, рівень вразливості активу до цієї загрози та цінність втраченого активу.

У методі Mehari запропоновано використовувати метод сценаріїв. Іншою перевагою Mehari є наявність шкал оцінювання та способу детермінованого визначення залишкових ризиків ІБ.

Рисунок 1.7 – Модулі Mehari та чотири підходи до проведення оцінювання ризиків ІБ

Крім цього, у Mehari визначено підхід до класифікації активів різних типів та запропоновано таблицю відповідності кращих практик з Mehari до заходів, що визначені у стандарті ISO/IEC 27002 (наявність такої можливості є безумовно важливою, враховуючи широке застосування ISO/IEC 27002 у сучасній практиці з організації захисту інформації).

В 2010 році вийшло оновлення Mehari і керівництво до методу було запропоновано на двох мовах: англійській та французькій. Ця версія методу:

- забезпечує повну модель управління ризиками, що відповідає вимогам ISO 27005;

- включає класифікацію активів, ймовірність виникнення загроз, рівень вразливостей;

- аналізує список сценаріїв ризику і забезпечує рівні серйозності для кожного сценарію;

- дозволяє оптимально обирати контрзасоби;

- дає додаткову оцінку відповідності організації стандартам ISO 27002: 2013 і процесу ISMS,

- розглядається як інструмент для АОР та УР шляхом автоматичного використання формул.

У Mehari 2010 процес оцінки сервісу безпеки здійснюється шляхом поширення серед підрозділів спеціальних анкет дозволяють оцінити якість рішень, спрямованих на зниження ризику. Опитувальники заповнюються аудитором в процесі інтерв'ювання персоналу підрозділу.

Виділяється три показника продуктивності сервісу безпеки:

- ефективність;
- надійність;
- сталість.

Якість сервісу безпеки оцінюється за шкалою від 0 до 4, що відображає складність порушення працездатності сервісу.

Надалі керівництва з оновленням методу тільки французькою мовою:

- Mehari Pro 2014 року для організацій малого і середнього бізнесу;
- Mehari 2017 року для організацій середнього та великого розміру.

У порівнянні з такими відомими програмними методиками, як RiskWatch або OCTAVE, Mehari є декілька важливих переваг:

– детальний опис методу дозволяє менеджерам по оцінці ризиків чітко уявляти внесок різних факторів в кінцеву оцінку;

– відкрита архітектура дозволяє адаптувати метод під специфіку організації та проводити індивідуальну оцінку ризиків.

3. CIS RAM Метод оцінки ризиків інформаційної безпеки Центру інтернет-безпеки, який допомагає організаціям впроваджувати й оцінювати свою безпеку щодо передових методів кібербезпеки CIS Controls. CIS RAM надає інструкції, приклади та шаблони для проведення оцінки кіберризику.

CIS RAM відповідає встановленим стандартам оцінки безпеки інформаційної безпеки, таким як ISO 27005, NIST SP 800-30, OCTAVE і RISK IT. CIS RAM доповнює ці популярні стандарти, надаючи докладні інструкції і

шаблони для швидкого проектування і впровадження оцінки ризику інформаційної безпеки.

Принципи методу CIS RAM:

- аналіз ризиків повинен враховувати інтереси всіх сторін, які можуть постраждати від ризику;
- ризики повинні бути зведені до рівня, який зацікавлені сторони знайдуть за потрібне;
- контрзаходи не повинні бути дорожче, ніж втрати від можливої реалізації ризику.

Для подолання аналізу ризиків інформаційної безпеки з дотриманням законодавчих і нормативних вимог CIS RAM ґрунтується на декількох класичних концепціях аналізу ризиків. Обчислення ризику включає в себе множинні впливу. У CIS RAM використовується класичний розрахунок оцінки ризику «Risk = Impact x Likelihood» з декількома змінами. Найбільш важливо, ризик розраховується шляхом множення значення ймовірності на множинні значення впливу. Ці множинні впливу включають вплив на цілі організації, її місію та зобов'язання щодо захисту інших. Організації повинні бути інформовані про багатьох способах, якими ризик інформаційної безпеки може завдати шкоди. Розрахунок ризику, який використовується CIS RAM, схожий на наведену нижче структуру:

«Ризик = Максимум (вплив місії, вплив цілей, вплив зобов'язань) * Імовірність».

В інструкціях до методу, чітко описується, як необхідно проводити цей розрахунок. Ефективність і масштаб впливу вказані в якісній і кількісній формі, щоб легко повідомляти рівні ризику всім зацікавленим сторонам і таким чином, що це важливо для кожної сторони. Схвалення ризиків чітко визначено. CIS RAM надає організаціям чітке керівництво для визначення прийнятного ризику, який видається прийнятним для влади і зацікавлених сторін, і який може послідовно застосовуватися до всіх ризиків інформаційної безпеки.

Допустимий ризик включається в себе поняття «відповідний» (всі потенційно порушені сторони погодяться з тим, що ризик є прийнятним) і чи є рекомендована захист «розумної» (вона не створює більшого навантаження, ніж ризик, який вона захищає від). Розширюючи визначення прийняття ризику цими двома факторами, організаціям легко приймати обґрунтоване рішення для прийняття ризику або для визначення пріоритетності неприйнятного ризику.

У CIS RAM відсутня спеціально розроблене програмне забезпечення для АОР, але є докладний посібник з використання методу з його детальним описом. Приклади використання методу представляються в таблицях Office Excel.

У CIS RAM містяться посилання на методі FAIR, оскільки він забезпечує послідовний метод оцінки інформаційного ризику, заснований на характеристиках компонентів інформаційних ризиків.

Управління та оцінка ризику CIS RAM представляється частиною загальної концепції CIS Controls V7 з побудови кібербезпеки.

Тобто тільки повне використання продуктів CIS може забезпечити систематичний підхід до управління та оцінки ризику для організації.

4. Організацією **Mirte** була запропонована концепція управління ризиками при побудові різних систем, в тому числі і інформаційних. Mirte безкоштовно розповсюджує простий інструментарій на базі електронної таблиці, призначений для використання на етапі ідентифікації та оцінки ризиків, вибору можливих контрзаходів відповідно до цієї концепції – «RiskNav».

У даній концепції ризик не поділяється на складові частини (загрози і вразливості), що в деяких випадках може виявитися більш зручним з точки зору власників інформаційних ресурсів. В даний час на етапі аналізу ризиків досить поширене побудова моделі порушника з прямою експертною оцінкою ризиків. З цієї причини найпростіші методики і інструменти типу «RiskNav» найбільш затребувані на ринку.

Перший крок – Ідентифікація ризика є найважливішим першим кроком в процесі управління ризиками. Його метою є рання і постійна ідентифікація ризиків, в тому числі всередині і поза проектом інженерної системи.

Другий крок – Оцінка ризика та оцінка наслідків. На цьому етапі проводиться оцінка впливу кожної події ризику на систему. Як правило, це включає в себе те, як подія може вплинути на вартість, графік або технічні результати. Вплив не обмежується тільки цими критеріями. Додаткові критерії, такі як політичні або економічні наслідки, також можуть зажадати розгляду. Крім того, робиться оцінка ймовірності (випадковості) кожної події ризику.

Третій крок – пріоритизація ризиків. На цьому етапі загальний набір ідентифікованих подій ризику, їх оцінки впливу та ймовірності їх виникнення «обробляються» для отримання найбільш важливого для найменш критичного ранжирування певних ризиків. Основна мета для визначення пріоритетності ризиків полягає у формуванні основи для розподілу критично важливих ресурсів.

Останній крок – планування зниження ризиків включає розробку планів зниження, спрямованих на управління, усунення або зниження ризику до прийнятного рівня. Як тільки план реалізується, він постійно контролюється, щоб оцінити його ефективність з наміром переглянути курс дій, якщо це необхідно.

У здійсненні управління ризиками беруть участь два інших етапу: розробка підходу і плану і вибір інструментів управління ризиками. Підхід до управління ризиками визначає процеси, методи, інструменти та командні ролі і обов'язки для конкретного проекту. У плані управління ризиками описується, як управління ризиками буде структуровано і виконано в рамках проекту. Інструменти управління ризиками підтримують впровадження та виконання управління програмними ризиками в програмах системного проектування. При виборі відповідних інструментів команда проекту розглядає такі фактори, як складність програми і доступні ресурси.

RiskNAV є надійним інструментом для полегшення процесу ризику. RiskNav дозволяє збирати, аналізувати, визначати пріоритети, контролювати та візуалізувати інформацію про ризик. Цей інструмент забезпечує графічне представлення трьох вимірів: пріоритет ризику, вірогідність та ступінь зменшення / управління.

RiskNav представляє простір ризику в табличній та графічній формі. Це ПЗ використовує модель, яка обчислює загальну оцінку для кожного виявленого ризику. Пріоритет ризику - це середнє значення середнього періоду часу, ймовірність виникнення та вплив.

RiskNav візуалізує простір ризику, який показує пріоритет ризику та стан зниження.

5. IRAM2 (Методологія оцінювання інформаційного ризику – 2), була розроблена британською організацією Information Security Forum (ISF) на основі бізнес-орієнтованого практичного посібника для ідентифікації та управління ризиками інформаційної безпеки в організаціях «The Standard of Good Practice for Information Security 2018».

IRAM 2 має шість фаз:

- огляд;
- оцінка впливу для бізнесу;
- аналіз загроз;
- оцінка вразливостей;
- розрахунок величини ризику;
- обробка ризику.

Величину інформаційного ризику можна розглядати як величину негативного впливу на бізнес, ризик розраховується за формулою:

Ризик = Ймовірність * Вплив.

Як основна технологія управління інформаційним ризиком, IRAM2 допоможе організаціям:

- застосовуйте простий, практичний, але суворий підхід: зосередьтеся на простоті та практичності, в той час як вбудовуючи суворість протягом

всього процесу оцінки. Це дає змогу проводити послідовні результати та глибину аналізу, що покращує процес прийняття рішень в бізнесі;

- зосередити увагу на бізнес-перспективі: керівництво інформаційним ризиком аналізу практиків, з тим щоб оцінювати ризики інформації з точки зору бізнесу. Кінцевий результат - це профіль ризику, який відображає точку зору інформаційного ризику в комерційних цілях;
- отримати більш широке охоплення ризиків: надавати більш широкий і більш всеохоплюючий охоплення ризиком, таким чином зменшуючи шанс, що значний ризик буде недоотриманий;
- зосередити увагу на найбільш значущих ризиках: дозволити ключовим зацікавленим компаніям та компаніям отримати чітке уявлення про те, звідки зосереджуватися ресурси, щоб вирішувати інформаційні ризики, які є найбільш значними для організації;
- взаємодіяти з ключовими зацікавленими сторонами: надавати можливість фахівцям із ризику інформування зацікавлених сторін із ключовими зацікавленими сторонами бізнесу, ризиків та технологій організованою та корпоративною поведінкою.

6. FAIR (факторний аналіз інформаційних ризиків) – це міжнародний кількісний метод оцінки інформаційного ризика.

Посилаючись на основні підходи до менеджменту інформаційними ризиками, що прописані в стандартах Cobit v.5.0, NIST SP 800-30, серію ISO/IEC 27000, методика факторного аналізу інформаційних ризиків FAIR, передбачає найбільш повне врахування факторів виникнення інформаційних ризиків [30]. FAIR дозволяє отримати опис достатньої кількості факторів, що впливають на оцінку ризику та конкретні значення ризику, яким би могли оперувати керівники підприємств.

Основою методики FAIR є аналіз факторів, що впливають безпосередньо на ризик. Аналізуються фактори, що мають вплив на компоненти, що є складовими ризику. Відповідно до зазначеної методики, головними складовими ризику є частота появи інциденту (LEF) та величина збитків від настання

зазначеного інциденту (LM) [6]. Кожна з цих складових поділяється на інші фактори: частота появи загрози, вразливість, первинні та вторинні збитки.

Відповідно до методики FAIR, основним принципом ефективного керування кіберризиками є кількісний аналіз ризиків.

Рамки FAIR визначають необхідні складові для реалізації ефективних програм управління кіберризиками. В основі будь-якої такої програми лежить здатність кількісно оцінювати кіберризики.

Система управління ризиками FAIR складається з наступних елементів:

- ризик – функція загроз, активів, контролю та факторів впливу, які впливають на збитки;
- управління ризиками, що складається з прийняття рішень та їх виконання;
- цикл зворотного зв'язку – показники, пов'язані з інформацією про загрозу та збитки та дані аналізу основних ризиків.

Використання FAIR передбачає проведення декількох етапів.

Спочатку необхідно визначити область аналізу і що є його метою. Для точного аналізу важлива чітко визначена область. Першою ціллю є визначення сценаріїв ризику, оскільки це є основою для структурування подальшого належного аналізу. Для визначення сценарію, необхідно: провести опис активу (ідентифікація об’єктів оцінки), загрози (частота появи інциденту) і ефекту (стосовно конфіденційності/цілісності/доступності), пов'язаного з аналізованих сценарієм.

Тобто, на першому етапі проводиться ідентифікація активів, загрози (з визначенням її групи та типу), оцінюється ефект загрози, що може бути застосований до інформаційної системи підприємства. Дані фіксуються в таблицю.

Наступний крок – оцінювання кожного зі сценаріїв. До цього етапу входять аналіз частоти появи загрози, існуючих вразливостей та кількісна оцінка факторів можливих збитків.

Частота появи загрози вимірюється з використанням факторів: «мінімальне значення», «найбільш ймовірне значення» та «максимальне значення»

Для оцінки найгіршого варіанту необхідно виконати наступні пункти:

– визначити дію загрози, яка напевно буде результатом найгіршого випадку;

– оцінити величину кожного виду втрат, пов’язаних з дією загрози;

– підсумувати величини всіх видів втрат.

Останнім етапом є розрахунок величини ризику, що відбувається через ідентифікацію сценарія з найвищім показником річних збитків. При розрахунку використовують метод Монте-Карло. Інтерпретація результатів проводиться відповідно до запропонованих таблиць методики.

Для проведення АОР, Інститут розробив ПЗ FAIR-U, що дозволяє вивчити основи методу, ввести дані про організацію, скористуватися вбудованим методом Монте-Карло для кількісного аналізу ризиків та згенерувати звіт.

Даний метод підтримують такі організації, як «Open Group» та «ISACA».

Методика FAIR являє собою детальний аналіз та оцінку ризиків, отриманий результат має конкретні значення ризику, а отже чіткий та доступний для використання.

1.7 Постановка задачі

В стандартах та нормативних документах зазначена необхідність впровадження системи управління інформаційною безпекою, що базується на системі управління ризиками.

Для використання ефективного управління ризиками підприємств, представників малого бізнесу, треба обмірковано та свідомо підходити до вибору методики оцінки ризиків, що впливає на один з основних етапів побудови СУІБ з використанням ризик-орієнтованого підходу.

Метою такого аналізу є надання загального уявлення про наявність потенційних загроз активам підприємства.

Сучасні методи управління інформаційними ризиками дозволяють оцінити існуючий рівень залишкових інформаційних ризиків на малих підприємствах. Це особливо важливо в тих випадках, коли до інформаційної системи компанії пред'являються підвищені вимоги в галузі захисту інформації та безперервності бізнесу.

Якісно виконаний аналіз інформаційних ризиків дозволяє провести порівняльний аналіз «ефективності вартості» різних варіантів захисту, обрати відповідні контрзаходи та засоби контролю, оцінити рівень залишкових ризиків. Крім того, інструментальні засоби аналізу ризиків, засновані на сучасних базах знань та процедурах логічного виводу, дозволяють будувати структурні та об'єктно-орієнтовані моделі інформаційних активів компанії, моделі загрози та моделі ризиків, пов'язані з окремими інформаційними та бізнес-транзакціями, і, отже, виявляти такі інформаційні активи компанії, ризик порушень захищеності яких є критичним, тобто неприйнятним. Такі інструментальні засоби надають можливість побудувати різні моделі захисту інформаційних активів компанії, порівнювати між собою за критерієм «ефективність» різні варіанти комплексів заходів захисту та контролю, а також вести моніторинг виконання вимог щодо організації режиму інформаційної безпеки вітчизняної компанії.

Постає необхідним розробити методику для вибору доцільного варіанту оцінки ризиків. Для цього необхідно розробити методичні вказівки для персоналу з інформаційної безпеки малого комерційного підприємства та шаблон таблиці, що включає критерії та їх метрики для вибору методики оцінки ризиків.

Надати обґрунтування та доцільність її використання для підприємств з чисельністю робітників від 10 до 50 та з річний доходом, що не перевищує суму, еквівалентну 10 мільйонам євро. Розробити рекомендації з використання методики для спеціаліста з ІБ.

Отже, для побудови такої системи, що буде найкраще підходити для певного підприємства, повинні бути проаналізовані й описані:

– критерії для порівняння та вибору методики оцінки ризиків для підприємства з урахуванням особливостей малого бізнесу;

– рекомендації з використання обраної методики для спеціаліста з кібербезпеки;

– проаналізувати практичну та економічну ефективності запропонованої методики.

1.8 Висновки

Впровадження в діяльність підприємства управління ризиками дозволяє забезпечити стабільність їх розвитку, підвищити обґрунтованість прийняття рішень щодо в ризиків і, тим самим, оптимізувати витрати на інформаційну безпеку. Рішення про вибір контрзаходів повинні враховувати співвідношення витрат і результату, однак проблеми можуть виникнути через людських помилок. У зв'язку з цим, питання впровадження ризик-орієнтованого підходу є актуальними, оскільки це збільшує ймовірність успіху і мінімізує ймовірність фінансових втрат.

Незважаючи на те, що процес менеджменту ризиків приносить важливі переваги, він має і певні обмеження. Наприклад, важливо розуміти, що персональне судження при прийнятті рішень може бути помилковим. Також для ефективного управління ризиками, важливо правильно підібрати методику оцінки ризику, що ідеально буде підходити до потреб конкретного малого підприємства.

Виходячи з результатів виконаного аналізу, було поставлено задачі на подальше дослідження.

РОЗДІЛ 2. РОЗРОБКА МЕТОДИЧНИХ РЕКОМЕНДАЦІЙ ДЛЯ ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ТА ОЦІНКИ РИЗИКІВ НА МАЛОМУ ПІДПРИЄМСТВІ

2.1 Визначення критеріїв обрання методу АОР

Для визначення найбільш ефективної методики для використання при управлінні ризиками на малому комерційному підприємстві необхідне проведення порівняльного аналізу.

Проведення порівняльної оцінки використання методів оцінки ризиків для малих підприємств необхідно для кожного підприємства окремо.

Наразі існують багато інструментів для вибору методики АОР, що планується використовувати на підприємстві. Великі комерційні підприємства розробляють власні інструменти, що дозволяє врахувати всі вимоги, які пред'являються. Серед великої кількості таких інструментів, найбільш поширеними та продуманими для використання є ті, що мають детальний опис використання, не є занадто складними та враховують фактори, необхідні для проведення обрання. Для виявлення кращої методики для конкретного підприємства можна використати вже існуючі засоби та шкали: атрибути ENISA; критерії авторів Корченко А.Г., Іванченко Е.В., Казмирчук С.В.; фактори, що впливають на вибір методів оцінки ризику стандарту ISO/IEC 31010.

Для опису та порівняння методів, робочою групою ENISA виділено 21 атрибут для опису характеристик методу, серед них:

- загальна та основна інформація;
- ідентифікація;
- дата першого видання, дата і номер фактичної версії;
- доступні мови, які підтримує цей інструмент;
- ціна;
- сфера застосування;

- цільові організації;
- рівень деталізації;
- вкажіть цільовий тип користувачів:
    - оперативний;
    - технічний;
- необхідні навики для користувачів;
- консультаційна підтримка;
- відповідність продукту міжнародним нормам (дотримання національного чи міжнародного стандарту);
- можливість пробної версії перед покупкою;
- інструменти та ПЗ, що підтримують метод;
- список засобів, які підтримують продукт;
- спеціальні допоміжні засоби можуть бути інтегровані з іншими інструментами.

Відповідно до стандарту ISO/IEC 31010, до факторів, що впливають на вибір методів оцінки ризику відносяться:

- значимість факторів, що впливають;
- можливість отримання кількісних вихідних даних.

Перший фактор поділяють на три пункти: ресурси і можливості, невизначеність та складність.

Дані вносяться в таблицю 2.1 та кожен метод пропонується оцінити за певною шкалою.

Значимість факторів, що впливають оцінюють за шкалою «Низька-Середня-Висока». Можливість отримання кількісних вихідних даних «Присутня-Відсутня».

Таблиця 2.1 – Порівняння методів відповідно до стандарту ISO/IEC 31010

Найменування методу оцінки ризику	Опис	Значимість факторів, що впливають			Можливість отримання кількісних вихідних даних
		Ресурси і можливості	Невизначеність	Складність	
…	…	…	…	…	…

В статті [28] пропонується для кожного методу складати десятикомпонентний кортеж <E, A, M, C, P, D, S, F, L, V>, що має в собі відомості щодо певних параметрів. Кожен з параметрів позначається латинською літерою:

E – подія;

A – дія;

M - міра ризику;

C – характеристика ситуації;

P – ймовірність;

D – небезпека;

S – ситуація вибору;

F – частота;

L – витрати і втрати;

V – відхилення від мети.

Даний метод інтегрованого представлення параметрів ризику (ІППР) є досить складним в використанні, адже для кожного параметру визначається різний степінь, деякі з них можливо відобразити безліччю ідентифікаторів. Слід зазначити, що коли виникають складнощі з отриманням статистичних даних, а так само для простоти інтерпретації величин, використовують логіко-лінгвістичний підхід та відображають цей компонент через лінгвістичну змінну.

Специфіка управління ризиками на малому підприємстві задає певні вимоги для методик з АОР, тому недоцільним виявляється використання

вищезгаданих методів та критеріїв порівняння. Адже, атрибути ENISA мають лише описовий характер, що не включає в себе важливі моменти, так само як і фактори стандарту ISO/IEC 31010 мають недостатньо критеріїв та інформації. А метод інтегрованого представлення параметрів ризику, незважаючи на отримання розгорнутої інформації в підсумку, виявляється занадто складним для використання на малих підприємствах.

Цей факт приводить до необхідності розробки відповідних до потреб малих підприємств критеріїв оцінки.

Таблиця 2.2 – Порівняння інструментів для вибору методу АОР

Існуючи інструменти	**Переваги**	**Недоліки**
фактори ISO/IEC 31010	Легкість у використанні, проведення аналізу не є трудомістким	Має недостатньо критеріїв для вибору, не враховує всі компоненти методик
атрибути ENISA	Легкість у використанні	Має лише описовий характер, відсутні чіткі вихідні дані
критерії автору Корченко А.Г.	Чіткість в отриманні статистичних даних, отримання розгорнутої інформації	Складний в використанні, відсутній розгорнутий опис використання.

2.2 Розробка інструменту для підбору методики АОР для малого комерційного підприємства

При розробці інструменту з набором критеріїв, відповідних до потреб малих підприємств, необхідно брати до уваги наступні особливості:

- через обмеженість ресурсів, на малих підприємствах немає можливості залучення висококваліфікованих ІТ-фахівців;
- характерні безсистемність і спонтанність рішень про модернізацію програмного забезпечення;

- необхідність гнучкості інформаційної системи через можливість переходу до іншої діяльності, можливий розвиток та збільшення масштабів підприємства, чи перехід на іншу систему оподаткування;
- залежність від власника, бо здебільшого, власники виконують керівні функції та висока обізнаність керівника в галузі використання ІТ підвищує сприйнятливість до впровадження інформаційних технологій;
- в процесах управління відсутні формалізація та стандартизація;
- недостатність фінансових ресурсів для придбання дорогого та вузькоспрямованого ПЗ. Тому є потреба в широкому за функціями ПЗ, що побудовано за принципом «все в одному»;
- зазвичай, на таких підприємствах наявна обмеженість комп'ютерної та оргтехніки, то складно створити цілісну ІТ інфраструктуру;
- вузька спеціалізація вимагає використання спеціалізованого ПЗ з більш високою вартістю;
- малий бізнес дуже інформаційно насичений і малі підприємства мають необхідність функцій обліку та управління, що і великі підприємства.

Враховуючи зазначені особливості інформаційної системи малого підприємства, його діяльності та організації, можна зазначити основні критерії, за якими варто обирати найбільш відповідний метод оцінки ризиків.

Критерії для порівняння та вибору методики оцінки ризиків для підприємства з урахуванням особливостей малого бізнесу:

К1 – Можливість отримання кількісних вихідних даних;

К2 – Відповідність вітчизняним та міжнародним стандартам;

К3 – Наявність детального керівництва з описом методики;

К4 – Наявність допоміжного ПЗ;

К5 – Оновлення та підтримка методики;

К6 – Доступність локалізованих версій;

К7 – Легкість у використанні;

К8 – Наявність діючої підтримки та супроводу.

Шкали для кожного критерію представлені в таблицях .

Таблиця 2.3 – Шкала оцінки для критерію К1

К1 – Можливість отримання кількісних вихідних даних	
2	Вихідні дані представлені кількісно
1	Змішаний тип
0	Вихідні дані представлені якісно

Таблиця 2.4 – Шкала оцінки для критерію К2

К2 – Відповідність вітчизняним та міжнародним стандартам	
2	Відповідає
1	Відповідає частково
0	Не відповідає

Таблиця 2.5 – Шкала оцінки для критерію К3

К3 – Наявність детального керівництва з описом методики	
2	Керівництво наявне
1	Керівництво представлене частково чи не детально
0	Керівництво відсутнє

Таблиця 2.6 – Шкала оцінки для критерію К4

К4 – Наявність допоміжного ПЗ	
2	Наявне офіційне ПЗ компанії-розробника методики, що оновлюється
1	Наявне офіційне ПЗ компанії-розробника методики, що є застарілим
0	Відсутнє офіційне ПЗ, необхідність в використанні стороннього ПЗ.

Таблиця 2.7 – Шкала оцінки для критерію К5

К5 – Оновлення та підтримка методики	
1	Оновлювалось за останні три роки
0	Не оновлювалось більш як три роки

Таблиця 2.8 – Шкала оцінки для критерію К6

К6 – Доступність локалізованих версій	
2	Методика доступна українською чи російською мовами
1	Методика доступна англійською мовою
0	Методика доступна на інших мовах

Таблиця 2.9 – Шкала оцінки для критерію К7

К7 – Легкість у використанні	
1	Для використання методики робітник повинен мати вищу освіту в галузі інформаційних технологій чи здобути відповідну кваліфікацію.
2	Для використання методики робітник повинен мати освіту в галузі, що є спорідненою з галуззю інформаційних технологій. Методика є інтуїтивно зрозумілою.
3	Для використання методики робітник не повинен мати освіту в галузі інформаційних технологій чи спорідненою з нею. Методика є інтуїтивно зрозумілою.

Таблиця 2.10 – Шкала оцінки для критерію К8

К8 – Наявність діючої підтримки та супроводу	
2	Наявний діючий центр підтримки
1	Центр підтримки наявний, але тимчасово чи повністю не функціонує
0	Центр підтримки відсутній

Для виокремлення найбільш вагомих та важливих критеріїв, встановлено вагові коефіцієнти для критеріїв. Інтегральна оцінка методу розраховується за формулою:

$$IO = \Sigma^{8}_{i=1} a_i * K_i; \quad (2.1)$$

де

К1…К8 – критерії для порівняння та вибору методики оцінки ризиків;

$a1 \ldots a8 \in \{1\ (\text{низький});\ 2\ (\text{середній});\ 3(\text{високий})\}$ – вагові коефіцієнти рівня впливу відповідного критерій на загальну оцінку.

Значення вагових коефіцієнтів встановлюється за результатами виконаного аналізу.

Дані аналізу пропонується використати допоміжний інструмент для вибору методики оцінки ризиків, дані заносяться у таблицю, що підраховує підсумок балів за критеріями.

Використовуючи запропонований метод порівняння методик оцінки інформаційних ризиків, можна точніше підібрати методику відповідно до особливостей окремого малого підприємства.

2.3 Визначення відповідного методу АОР для типового українського підприємства

Визначення кращої методики для малого підприємства пропонується з використанням відомостей про типове мале комерційне підприємство України.

За даними Державної статистичної служби України [40], кількість зареєстрованих малих підприємств, станом на 2015 рік, налічує 327814, що є 95,5% до загального показника відповідного виду діяльності. Виокремлено п’ятнадцять основних видів діяльності таких підприємств, основними є:

- оптова та роздрібна торгівля, ремонт автотранспортних засобів і мотоциклів (90823 одиниць);
- сільське, лісове та рибне господарство (44182 одиниць);
- промисловість (37640 одиниць).

В середньому, на підприємстві працює 17 осіб, що свідчить про невеликий штат працівників. Через брак кваліфікованих кадрів з ІБ, таким робітникам важлива наявність детального керівництва з описом методики оцінки ризиків та легкість у впровадженні цієї методики, адже важливо, щоб для використання методики робітник не повинен мати освіту в галузі інформаційних технологій чи спорідненою з нею та щоб методика є інтуїтивно зрозумілою. Спираючись на ці твердження слід зауважити важливість наявності офіційної підтримки від розробника.

Зазвичай, управління типового малого підприємства залежить від однієї-двох осіб, що є його власниками. Стратегічне планування зазвичай не

здійснюється через значний обсяг поточної роботи, що припадає на кожного співробітника. Більшість власників малих підприємств відчувають дефіцит широкого діапазону навичок, за допомогою яких вони повинні точно аналізувати діяльність і стрімко маневрувати своїми обмеженими ресурсами, щоб максимізувати швидкість і гнучкість управління, що негативно позначається на управління ІБ. Малі підприємства частіше від інших використовують неофіційні методи управління, обходячи складне планування і методи управління, необхідні для належного обґрунтування рішень. На малих підприємствах, де існує планування та управління на основі визначених методів, вони зазвичай охоплюють короткі терміни часу, є неофіційними, нерегулярними і невичерпними.

Типові підприємства не показують високий рівень прибутку, більшість за них працюють з негативними показниками сальдо, з цього можна зробити висновок, що такі підприємства будуть прагнути до мінімізації витрат на вузько направлене ПЗ. В інтересах таких підприємств використовувати вільне допоміжне ПЗ, що розроблене компанією, що пропонує методику.

З використанням вищезазначених критеріїв та беручі до уваги особливості малої підприємницької діяльності, що описана в першому розділі можна провести аналіз та обрати найбільш відповідну методику оцінки ризиків для типового українського підприємства.

Для виокремлення найбільш вагомих та важливих критеріїв, застосовуються вагові коефіцієнти для критеріїв: можливість отримання кількісних вихідних даних; наявність детального керівництва з описом методики; наявність допоміжного ПЗ; доступність локалізованих версій; легкість у використанні.

Всі вищезазначені методики оцінки інформаційних ризиків були проаналізовані перевірені на відповідність всім критеріями, відповідно до зазначених шкал; результати внесені в таблицю 2.11.

Таблиця 2.11 – Вихідна таблиця інструменту вибору методики оцінки ризиків

Критерії	**Найменування методу оцінки ризику**					
	RiskWatch	Mehari	FAIR	CIS RAM	Mitre	IRAM2
Можливість отримання кількісних вихідних даних	2	1	2	2	2	2
Відповідність вітчизняним та міжнародним стандартам	2	2	2	2	2	2
Наявність детального керівництва з описом методики	0	1	2	1	2	2
Наявність допоміжного ПЗ	2	0	2	0	1	0
Оновлення та підтримка методики	1	1	1	1	1	1
Доступність локалізованих версій	1	0	1	1	1	1
Легкість у використанні	3	2	3	3	1	2
Наявність діючої підтримки та супроводу	2	1	2	2	0	2
Підсумок балів	23	13	**29**	20	20	21

За результатами проведеного дослідження, більш відповідним для використання на малому комерційному підприємстві є метод FAIR.

Задля ефективного використання методу FAIR на малому підприємстві, постає необхідність в розробці методичних рекомендацій з використання методики FAIR. Перш за все, розробка має базуватися на розумінні етапів та складових частин обраного методу.

2.4 Розробка методичних рекомендацій для використання методу FAIR на малому підприємстві

FAIR (факторний аналіз інформаційних ризиків) – це міжнародний метод кількісної оцінки інформаційного ризика. Посилаючись на основні підходи до менеджменту інформаційними ризиками, що прописані в вищезазначених стандартах, методика факторного аналізу інформаційних ризиків FAIR, передбачає найбільш повне врахування факторів виникнення інформаційних

ризиків [29]. FAIR дозволяє отримати опис достатньої кількості факторів, що впливають на оцінку ризику та конкретні значення ризику, які б могли використовувати на підприємствах. Основою методики FAIR є аналіз факторів, що впливають безпосередньо на ризик. Аналізуються фактори, що мають вплив на компоненти, що є складовими ризику. Відповідно до зазначеної методики, основними складовими ризику, що поділяються на інші фактори, є частота появи інциденту (LEF) та величина збитків від настання зазначеного інциденту (LM) [6]. Кожен з цих компонентів поділяється на інші фактори: частота появи загрози, вразливість, первинні та вторинні збитки. Описана модель має структуру, що представлена на рисунку 2.1.

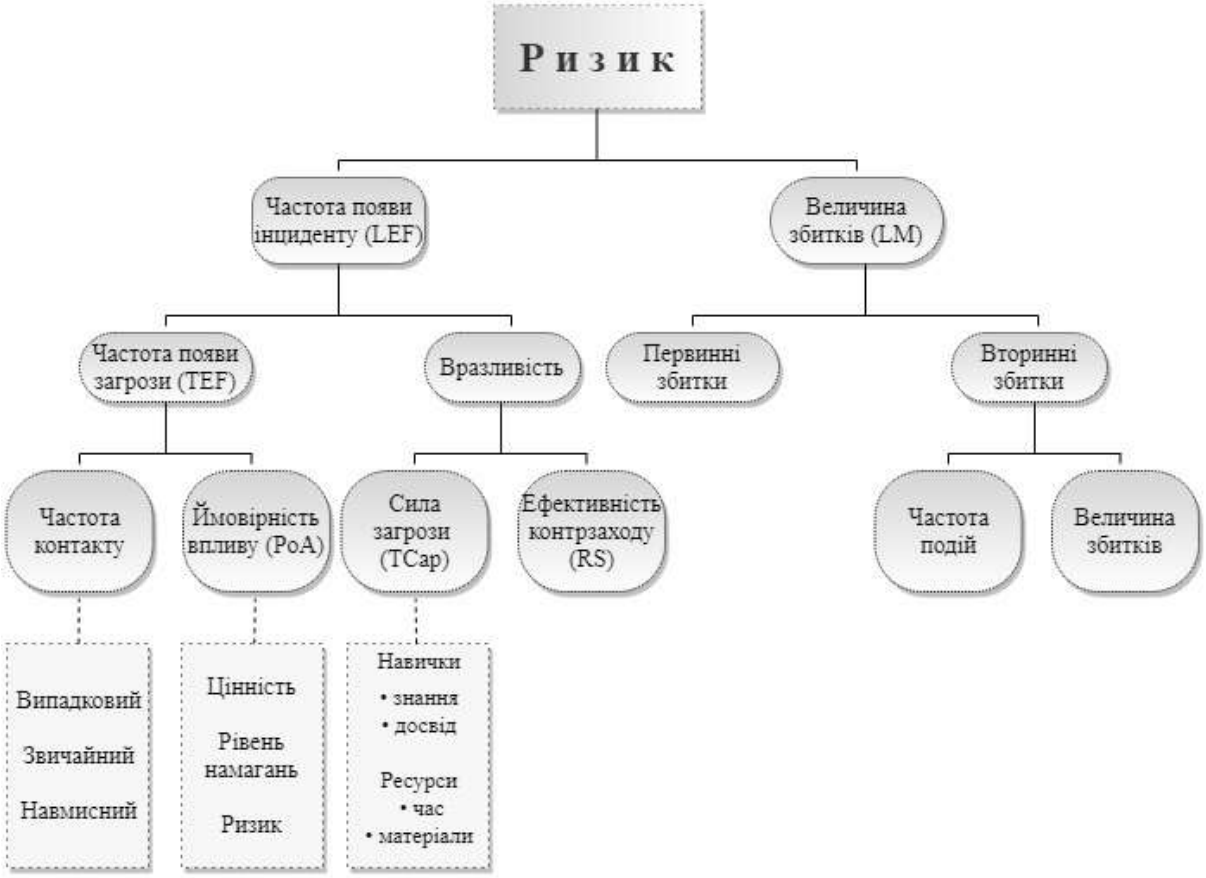

Рисунок 2.1. – Складові ризику за методом FAIR

Використання FAIR передбачає проведення декількох етапів. Спочатку необхідно визначити область аналізу і що є його метою. Для точного аналізу важлива чітко визначена область. Першою ціллю є визначення сценаріїв ризику, оскільки це є основою для структурування подальшого належного аналізу. Для визначення сценарію, необхідно: провести опис активу

(ідентифікація об’єктів оцінки), загрози (частота появи інциденту) і ефекту (стосовно конфіденційності/цілісності/доступності), пов'язаного з аналізованих сценарієм.

Тобто, на першому етапі проводиться ідентифікація активів, загрози (з визначенням її групи та типу), оцінюється ефект загрози, що може бути застосований до інформаційної системи підприємства. Дані фіксуються в таблицю, що формується з використанням спеціально розробленого інститутом FAIR, програмного забезпечення за назвою FAIR-U. Це ПЗ доступно для безкоштовно для учасників методу на сайті розробника.

Наступний крок – оцінювання кожного зі сценаріїв. До цього етапу входять аналіз частоти появи загрози, існуючих вразливостей та кількісна оцінка факторів можливих збитків. Частота появи загрози вимірюється з використанням факторів: «мінімальне значення», «найбільш ймовірне значення» та «максимальне значення».

Для оцінки найгіршого варіанту необхідно виконати наступні пункти:

– визначити дію загрози, яка напевно буде результатом найгіршого випадку;

– оцінити величину кожного виду втрат, пов’язаних з дією загрози;

– підсумувати величини всіх видів втрат.

Останнім етапом є розрахунок величини ризику, що відбувається через ідентифікацію сценарія з найвищім показником річних збитків. Розрахунок проводиться ПЗ автоматично, з використанням методу Монте-Карло. Інтерпретація результатів проводиться відповідно до запропонованих таблиць методики.

Методичні рекомендації мають за мету прискорювати та полегшувати використання методу FAIR робітниками малого підприємства. Вони розроблялись на основі офіційної інформації інституту FAIR та виконують наступні функції:

– несуть інформативний характер для робітників: дають визначення основних понять в сфері управління ризиками, описують етапи методу та інформацію щодо використання ПЗ FAIR-U;
– являються покроковим керівництвом з використанням методу FAIR.

Методичні рекомендації складаються з 4 етапів, у яких зазначені основні кроки проведення оцінки ризиків обраним методом: визначення активів підприємства; визначення загроз активам, що розглядаються; виявлення вразливостей, проведення оцінки сили загрози та ефективності контрзаходу, отримання даних частоти появи інциденту, оцінка величини збитків.

Дані методичні рекомендації являють собою детальне керівництво з використання методу FAIR працівником малого підприємства.

Розроблені методичні рекомендації наведені в додатку Б

2.5 Висновки

В другому розділі були виконані поставлені задачі, а саме:

– проаналізовані та сформовані критерії для вибору методів оцінки ризиків, розроблені методичні вказівки для персоналу з інформаційної безпеки малого комерційного підприємства та шаблон таблиці, що включає критерії та їх метрики для вибору методики оцінки ризиків;

– доведено доцільність використання методу FAIR для малих комерційних підприємств. Методика FAIR являє собою детальний аналіз та оцінку ризиків, отриманий результат має конкретні значення ризику, а отже чіткий та доступний для використання;

– наведено детальний опис етапів методу FAIR;

– описані рекомендації з використання обраної методики для спеціаліста з кібербезпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Характеристика підприємства

ОІД виступає ІТС НВП ТОВ «Аксіома», що розміщене в офісному приміщенні за адресою: м. Дніпро, вул. Каштанова, 15. Підприємство займається електромонтажними роботами та надає послуги за проектування та монтажу:

1) охоронної сигналізації з підключенням на пульт охорони (в тому числі бездротова);

2) пожарної сигналізації;

3) відеоспостереження;

4)системи обмеження та контролю доступу (турнікети, замки, відеодомофони);

5) АТС, пульти зв’язку, переговорні пристрої;

6) інтеграція системи «Розумний дім» для котеджей та офісів;

7) мережі: комп’ютерні, телефонні.

Форма власності: приватна власність.

На підприємстві працюють висококваліфіковані спеціалісти з вищою освітою в сфері економіки, обліку та аудиту і проектування. Кількість робітників налічує 12 осіб, серед яких є спеціаліст з управління кібербезпеки.

3.2 Розрахунок витрат на проведення АОР на підприємстві

Метою даного розділу є обґрунтування економічної доцільності застосування запропонованих методичних рекомендацій та методу FAIR на малому комерційному підприємстві з метою ідентифікації та оцінки існуючих ризиків.

Для визначення ефективності необхідно розрахувати:

1) капітальні (фіксовані) та поточні (експлуатаційні) витрати на проведення АОР на підприємстві методом FAIR з використанням запропонованих в дипломній роботі методичних рекомендацій;

2) визначити оцінку величини збитків від атаки та загальний ефект від проведення АОР з використанням методики та рекомендацій;

3) визначити показники економічної ефективності.

3.2.1 Розрахунок капітальних витрат на проведення АОР на підприємстві

До капітальних (фіксовані) витрат відносяться витрати на навчання та освоєння робітником методу FAIR:

– перегляд вебінару;

– ознайомлення з методичними рекомендаціями, що розроблені в дипломній роботі.

Таблиця 3.1 – Зарплати робітників за місяць

Посада	**Розмір заробітної плати, грн.**	**Кількість співробітників,чол.**	**Витрати на заробітну плату за місяць, грн.**
Директор	9000	1	9000
Головний бухгалтер	8500	1	8500
Бухгалтер	8000	1	8000
Інженер-проектувальник	8500	2	17000
Спеціаліст з управління кібербезпеки	8000	1	8000
Монтажник	7500	6	45000
Загалом ($З_с$):			95500

$$К = З_{зп} + З_{мч}, \quad (3.1)$$

де $З_{зп}$ – заробітна плата робітника, грн;

$З_{мч}$ – вартість витрат машинного часу, що необхідне для навчання, грн.

$$З_{зп} = t * З_{пр}, \quad (3.2)$$

де t – загальна тривалість навчання, годин;

$З_{пр}$ – середньогодинна заробітна плата робітника з нарахуваннями, грн/год.

$$З_{мч} = t * С_{мч}, \quad (3.3)$$

де $С_{мч}$ – вартість 1 години машинного часу, грн/год

t – загальна тривалість навчання, год;

$$С_{мч} = Р * С_{е} + (Ф_{зал} * Н_{а} /F_{р}) + (К_{лпз} * Н_{апз} /F_{р}), \text{ грн} \quad (3.4)$$

де Р – встановлена потужність ПК кВт;

$С_{е}$ – тариф на електричну енергію, грн/кВт*год;

$Ф_{зал}$ –залишкова вартість ПК на поточний рік, грн;

$Н_{а}$ – річна норма амортизації на ПК, частки одиниць;

$F_{р}$ – річний фонд робочого часу;

$К_{лпз}$ – вартість ЛПЗ, грн;

$Н_{апз}$ – річна норма амортизації на ПЗ, частки одиниць;

$$t = t_{в} + t_{омр}, \quad (3.5)$$

де $t_{в}$ - час просмотру вебінару;

$t_{омр}$ - час ознайомлення з методичними рекомендаціями.

t = 1,4 год + 0,30 год = 1,7 год

$З_{зп}$ = 1,7 * 50грн/год = 85,00 грн

$С_{мч}$ = 0,4 * 1,68 грн/кВт *год + (1200 грн * 3000грн / 1920 год) = 6,94 грн

$З_{мч}$ = 1,7 * 6,94 грн = 11,80 грн

Таким чином, капітальні витрати на навчання робітника складають:

К = 11,80 + 85,00 = 96,80 грн

3.2.2 Розрахунок експлуатаційних витрат на проведення АОР на підприємстві

Поточні річні витрати складаються з:

$$С = С_{ел} + С_{з} + С_{єсв} + С_{тос}; \quad (3.6)$$

Проведення АОР відбувається чотири разі на рік одним спеціалістом, на що він витрачає 8 год в процесі одного аналізу, тому:

$С_{ел}$ = 4*(0,4 кВт * 8 год * 1,68 грн/кВт *год) = 21,52 грн

$С_{з}$ = 4* ($З_{год}$ *8 год) = 4* 50 * 8 = 1600 грн

$С_{єсв}$ = $С_{з}$ * 22% = 352 грн

$С_{тос}$= К * 2% = 96,80 * 0,02 = 1,94 грн

С = 1975,46 грн

3. 3 Визначення оцінки величини збитків від атаки та загальний ефект від проведення АОР з використанням методики та рекомендацій

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки ($П_{п}$).

Час простою внаслідок атаки 4 години:

$П_{п}$ = (95500/176)*4 = 2170,45 грн

Витрати на відновлення працездатності системи включають кілька складових:

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

$П_{пв}$ – витрати на відновлення системи, грн;

$П_{зч}$ – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ = 16 год:

$П_{ви}$ = (50500/176)*16 = 4590,90 грн

Витрати на відновлення системи визначаються часом відновлення після атаки $t_в$ = 4 год і розміром середньогодинної заробітної плати спеціаліста:

$П_{пв}$ = (8000/176)*4 = 181,82 грн

Витрати на відновлення працездатності системи:

$П_в = П_{ви} + П_{пв} + П_{зч}$ = 4590,90 + 181,82 + 0 = 4772,72 грн

О = 45000 грн - річний обсяг продажів підприємства.

Втрати від зниження працездатності атакованої системи:

V = О/2080 * (4+16+4) = 45000 /1920 * 24 = 562,50 грн

Таким чином, загальний збиток від атаки на ІТС підприємства при реалізації загрози складе:

$В = П_п + П_в$ + V = 4590,90 + 4772,72 + 562,50 = 9882,85 грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням В – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; С – щорічних витрат на експлуатацію системи інформаційної безпеки.

Відповідно до результатів оцінки ризиків, ймовірність реалізації загроз – 42,68%.

Загальний ефект від впровадження системи інформаційної безпеки:

$E = B \cdot R – C$ = (9882,85* 42,68%)/100 - 1975,46 = 2242,54 грн

Рисунок 3.1 – Результат аналізу ризиків за методом FAIR

3.4 Розрахунок показників економічної ефективності

Визначення та аналіз показників економічної ефективності:

Оцінка економічної ефективності здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій То.

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

Коефіцієнт ROSI розраховують за допомогою показників:

$$ROSI = E/K \text{ , частки одиниці,} \quad (3.7)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

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

$$ROSI = 2242,54 / 96,80 = 23,17$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження системи ЗІ.

$$To = 1 / 23,17 = 0,04 \text{ роки.}$$

3.5 Висновки

В розділі проаналізована доцільності використання методу FAIR за методичними рекомендаціями, що розроблені в дипломній роботі. Визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Розраховані капітальні витрати становлять 96,80 грн.

Експлуатаційні витрати становлять 1975,46 грн.

Загальний збиток від реалізації існуючих загроз складає 9882,85 грн.

Ефект від використання методу FAIR за методичними рекомендаціями становить 2242,54 грн.

Термін окупності капітальних інвестицій складає 14,6 днів.

Отже, економічна доцільність обґрунтована і використання методу FAIR за методичними рекомендаціями, що розроблені в дипломній роботі може бути ефективним та успішною.

ВИСНОВКИ

В ході виконання дипломної роботи було проведено аналіз факторів, що впливають на процедуру проведення аналізу та оцінки інформаційних ризиків на малому підприємстві та виконані всі поставлені завдання, а саме:

– розглянуті міжнародні та вітчизняні стандарти та була виділена необхідність впровадження системи управління інформаційною безпекою, що базується на системі управління ризиками;

– проведено аналіз існуючих загроз кібербезпеки, зазначено важливість проведення аналізу та оцінки інформаційних ризиків на малих підприємствах з урахуванням особливостей їх діяльності. Визначено основні характеристики типового малого підприємства України, як об`єкту інформаційної діяльності;

– розглянуто широковживані методи аналізу та оцінки інформаційних ризиків та інструменти для їх порівняння;

– розроблений інструмент для вибору доцільного варіанту оцінки ризиків, що включає вагомі для малого підприємства критерії, розроблені вказівки для малого комерційного підприємства з шаблоном інструменту, що містить критерії та їх метрики для вибору методики оцінки ризиків;

– з використанням запропонованого інструменту доведено доцільність використання методу факторного аналізу інформаційних ризиків для малих комерційних підприємств. Методика факторного аналізу інформаційних ризиків являє собою детальний аналіз та оцінку ризиків, отриманий результат має конкретні значення ризику, а отже чіткий та доступний для використання. Наведено детальний опис етапів методу FAIR;

– надано методичні рекомендації з використання методу факторного аналізу інформаційних ризиків для спеціаліста на малому комерційному підприємстві;

– обґрунтовано економічну доцільність застосування запропонованих методичних рекомендацій до методу FAIR на малому комерційному підприємстві з метою оцінки існуючих ризиків.

Отже, запропоновано інструмент з вибору відповідної методики для використання на типовому малому комерційному підприємстві та розроблено методичні рекомендації з використання методу FAIR.

ПЕРЕЛІК ПОСИЛАНЬ

1. A Guide to risk assessment and safeguard selection for Information Technology Systems, [Электронный ресурс] / MG-3, Government of Canada, Communications Security Establishment (CSE) P.O., Terminal, Ottawa, Ontario, Canada, K1G 3Z4 – 1996, P. 73 – Режим доступа: http://www.cse-cst.gc.ca.

2. BSI-Standard 100-3: Risk analysis based on IT-Grundschutz // Bundesamt für Sicherheit in der Informationstechnik. – 2008. – version 2.5.

3. CIS RAM Puts the CIS Control into Action [Електронний ресурс]. – Режим доступу: https://www.cisecurity.org/blog/cis-ram-puts-the-cis-controls-into-action

4. Cyber Security Breaches Survey 2018 [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

5. ENISA Threat Landscape Report 2017 [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport

6. Freund J., Jones J. Measuring and managing information risk. A FAIR approach [Текст]: Jack Freund, Jack Jones. – Oxford:Butterworth of Elsevier, 2017. - 391 с.

7. Information Risk Assessment Methodology 2 (IRAM2) [Електронний ресурс]. – Режим доступу: https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/

8. ISF Methods - ENISA [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_isf_methods.html

9. ISO/IEC 27005 Информационные технологии – Методы защиты – Менеджмент рисков информационной безопасности. BS ISO/IEC 27005:2008. – 2008. – Технический перевод v.2.6 от 4.02.2011.

10. IT-Grundschutz. bsi.bund.de. BSI. Retrieved 29 November 2013

11. John Wiley & Sons (US), John Wiley & Sons, Inc. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams, 2010, for ISACA

12. Mehari - ENISA [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

13. Mehari – Overview // Club de la Securit ´ e de l'Information Franc¸ais ´(CLUSIF). – 2010.

14. NIST 800 – 30 Risk Management Guide for Information Technology Systems.

15. Performance And Analysis Of Risk Assessment Methodologies In Information Security [Електронний ресурс]. – Режим доступу: http://www.ijcttjournal.org/Volume4/issue-10/IJCTT-V4I10P157.pdf

16. Risk Assessment Methods [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

17. Risk Management | The MITRE Corporation [Електронний ресурс]. – Режим доступу: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management

18. RiskWatch - Risk & Compliance Management Software & Services [Електронний ресурс]. – Режим доступу: https://www.riskwatch.com

19. Варфоломеев А.А. - Управление информационными рисками: Учеб. пособие. – М.: РУДН, 2008. – 158 с.: ил.

20. Вітер С.А., Світлишин И.И.- Захист облікової інформації та кібербезпека підприємства [Електронний ресурс]. – Режим доступу: http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf

21. Господарський кодекс України від 16.01.2003 р. №436-IV [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/436-15

22. Дикий А.П. - Організація бухгалтерського обліку як інструмент забезпечення економічної безпеки підприємств: дис. канд. екон. наук: 08.00.09 / А.П. Дикий. – Житомир, 2009. – 172 с

23. Добринін І.С., Мальцева Н.О. - Вдосконалення методики факторного аналізу інформаційних ризиків - Харківський національний університет радіоелектроніки, Харків

24. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241

25. Кибербезопасности и антивирусная защита «Лабораторія Касперського» [Електронний ресурс]. – Режим доступу: https://www.kaspersky.ru/

26. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2010. – №3. – С. 5-10.

27. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

28. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1. – С. 96-101.

29. Луцкий М.Г Современные средства управления информационными рисками / Луцкий М.Г., Иванченко Е.В., Казмирчук С.В., Охрименко А.А.// Науково-практичний журнал «Захист інформації» №1, 2012 – 13с. [007]

30. Луцкий М.Г. Базовые понятия управления риском в сфере информационной безопасности / Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – 194 с.

31. Макеев А. С. Менеджмент рисков информационной безопасности как непрерывный процесс // Молодой ученый. — 2016. — №10. — С. 62-66. — URL https://moluch.ru/archive/114/29934/ (дата обращения: 13.11.2018).

32. Методика факторного аналізу інформаційних ри-зиків An Introduction to Factor Analysis of Information Risk (FAIR) [Електронний ресурс]. – Режим доступу: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf.

33. НД ТЗІ 1.1-002-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

34. НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Типове положення про службу захисту інформації в АС;

35. НД ТЗІ 3.7-003-2005 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС;

36. Особенности обеспечения информационной безопасности малого и среднего бизнеса [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/Small_Business_Security

37. Остапенко А.Г. Математические основы риск-анализа : учеб. пособие / А.Г. Остапенко, М.В. Бурса. – Воронеж : ФГБОУ ВПО «Воронежский государственный технический университет», 2013. – 63с.

38. Отчёт Центра мониторинга информационной безопасности за I полугодие 2018 года - Habr [Електронний ресурс]. – Режим доступу: https://habr.com/company/pm/blog/424475/

39. Провалів В.С. - Інформаційні технології в малому бізнесі: особливості використання // Природні і математичні науки в сучасному світі: зб. ст. по матер. XIX міжнар. наук.-практ. конф. № 6 (18). - Новосибірськ: СібАК, 2014.

40. Сайт Державного комітету статистики України [Електрон. ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/

41. Сучасні підходи до оцінки ризиків інформаційних технологій. [Електронний ресурс]. – Режим доступу: http://www.auditagency.com.ua.

42. Хмелюк А. В. Статистична оцінка діяльності підприємств малого бізнесу: проблеми інформаційного забезпечення - Ефективна економіка № 12, 2013 [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=2612

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	62	
6	А4	2 Розділ	13	
7	А4	3 Розділ	6	
8	А4	Висновки	2	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	10	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Дипломна робота – Зубенко ОВ – 125м-17-2.docx – Пояснювальна записка.
2. Презентація – Зубенко ОВ.pttx – Презентація
3. Інструмент для обрання методики АОР – Зубенко ОВ.xlsx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник : _____ к.е.н.,доц. Пілова Д.П.

(підпис)

ДОДАТОК Г. Відгук від керівника дипломної роботи

ВІДГУК

на дипломну роботу магістра

студентки групи 125м-17-2

Зубенко Ольги Володимирівни

на тему: «Використання методики факторного аналізу інформаційних ризиків в процесі забезпечення кібербезпеки малих комерційних підприємств»

Метою дипломної роботи є впорядкування процедури проведення аналізу та оцінки інформаційних ризиків на малому підприємстві.

Тема дипломного проекту безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в дипломному проекті вирішуються наступні задачі: аналіз теоретичної бази в сфері управління ризиками; досліджено існуючі кількісні методи оцінки ризиків; наведено три інструменти для порівняння запропонованих методів оцінки ризиків в метою вибору відповідної для використання на підприємстві.

Розроблено інструмент порівняння, що враховує вимоги, відповідно до особливостей малого бізнесу. Розроблені методичні рекомендації для використання методу FAIR. Практичне значення результатів дипломного проекту полягає у розробці інструменту для вибору відповідної методики оцінки ризиків для малого комерційного підприємства.

Перевагою дипломного проекту є розробка методичних рекомендацій щодо використання методу FAIR на малому комерційному підприємстві.

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

За час дипломування Зубенко О.В. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння звання магістра та кваліфікації професіонала з організації інформаційної безпеки.

Дипломна робота заслуговує оцінки «відмінно»

Керівник дипломної роботи д.ф.-м.н., проф. Кагадій Т.С.

Керівник спец. розділу ст. викл. Тимофєєв Д.С.

ДОДАТОК Д. Методичні рекомендації з використання методу FAIR

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

з використання методу FAIR для проведення оцінки ризиків на малому комерційному підприємстві

Аналіз та оцінка ризиків з використанням методу FAIR складається з чотирьох етапів, що містять десять кроків:

Етап I – Визначення сценаріїв

1. Визначити активи підприємства.

2. Визначити загрози активам, що розглядаються.

Етап II – Визначення частоти появи інциденту (LEF)

3. Оцінити частоту появи загрози (TEF)

4. Виявлення вразливостей (Vulnerability)

5. Оцінка сили загрози (TCap)

6. Оцінка ефективності контрзаходу (RS)

7. Отримання даних частоти появи інциденту (LEF)

Етап III – Оцінка величини збитків (LM)

8. Оцінка втрат від реалізації найгіршого сценарію

9. Оцінка найбільш ймовірних втрат

Етап IV – Визначення величини ризиків

10. Отримання вихідних даних

Варто зазначити, що для кожної загрози треба проводити процедуру аналізу с початку.

Перед початком використання методу необхідно створити обліковий запис на сайті інституту FAIR https://www.fairinstitute.org/fair-u. Це надасть доступ до ПЗ FAIR-U.

Етап I – Визначення сценаріїв

Всі дані першого етапу позначаються у вкладці «Scope». Для початку прописується мета проведення АОР в графі «Analysis Purpose».

1. Визначити активи підприємства.

Для того, щоб скласти можливі сценарії, до яких застосовують фактори методу, необхідно провести ідентифікацію інформаційних активів підприємства. Розглядаються цінні інформаційні активи, вплив на які буде мати негативний результат. Також визначаються цінність (вартісні характеристики)

активу та вимоги до захисту (конфіденційність, цілісність та доступність). Активи позначаються в графі «Asset(s)».

Після проведення класифікації інформації, дані регіструються з використанням таблиці 1.

Таблиця 1 – Класифікація інформації

№ п/п	Опис	Детально	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
…	…	…	…	…	…	…	…

Таблиця 2 – Інвентаризаційна відомість інформаційних активів підприємства

	Інформація про актив						
№ п/п	Назва актива	Тип інформ. активу	Персональні дані (Т/Н)	Дані про клієнтів (Т/Н)	Власник активів	Термін зберігання даних	Поточний рівень захисту
…	…	…	…	…	…	…	…

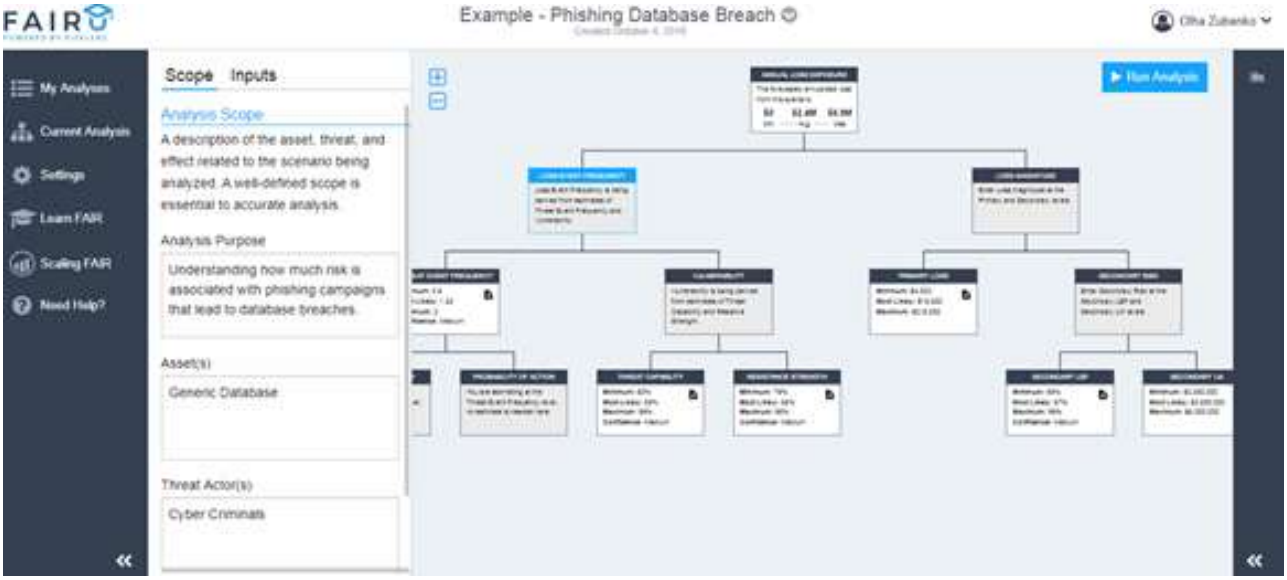

Рисунок 1 – ПЗ для методу факторного аналізу інформаційних ризиків

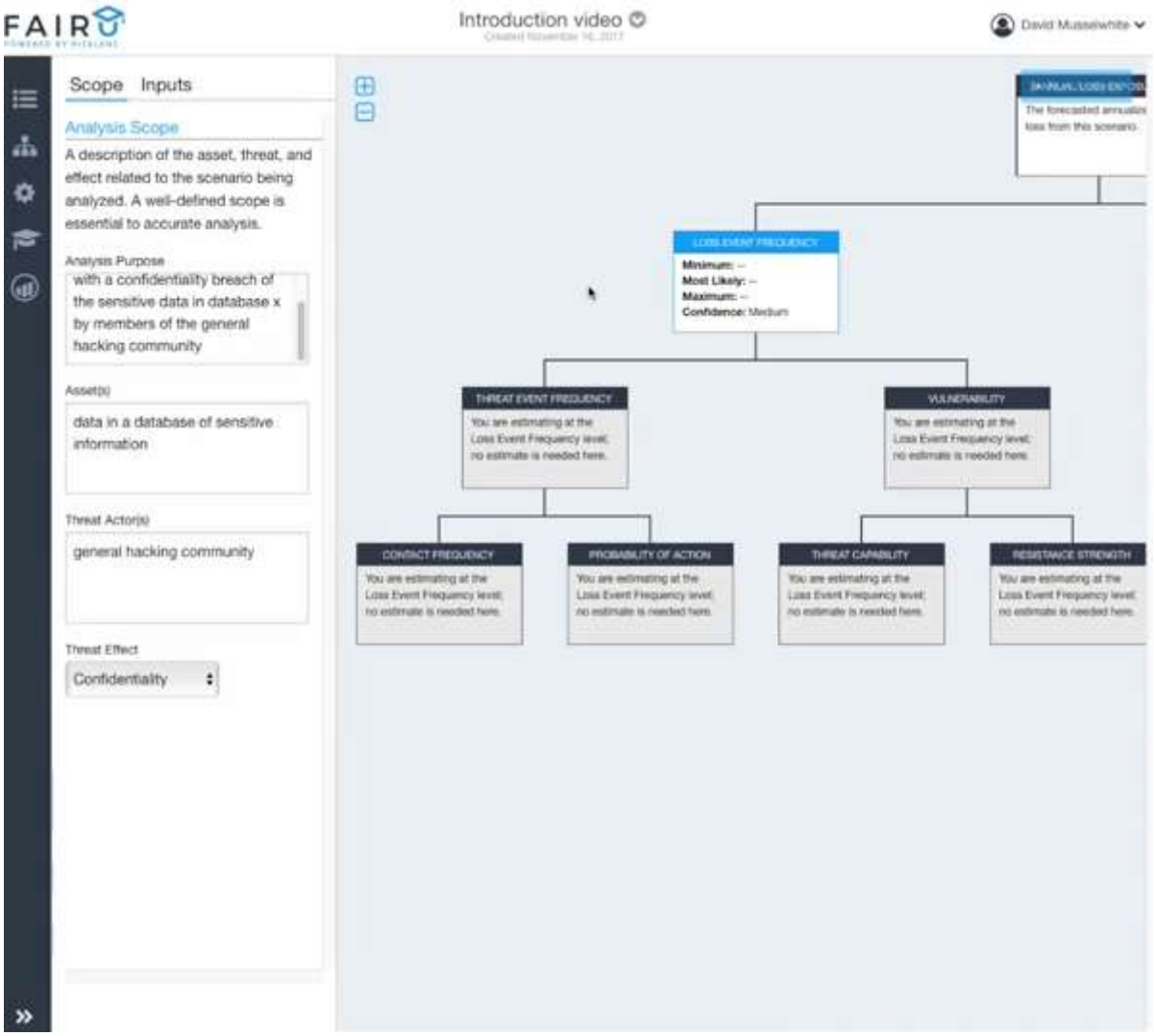

Рисунок 2 – Введення даних першого етапу

2. Визначити загрози активам, що розглядаються.

За результатами впливу на інформацію та систему її обробки, загрози поділяються на чотири класи:

Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам розмежування доступу до інформації.

Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформації в результаті некоректних дій адміністраторів, технічного обслуговуючого персоналу.

Втрата спостережності (керованості системою) (С) - порушення процедур

ідентифікації та автентифікації адміністраторів або процесів і надання їм повноважень, втрата контролю за їх діяльністю, можливість відмови від отримання або пересилання повідомлень.

Загрози потенційно можуть завдати шкоди інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам. Загрози можуть бути навмисними (Н), випадковими (В), природними (П). Повинні бути ідентифіковані як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

За походженням загрози поділяються на випадкові та навмисні. Випадкові загрози спричиняються помилками у програмному забезпеченні, збоями та відмовами апаратури та систем забезпечення, помилками персоналу тощо. Випадкові загрози, спричинені стихійними лихами (повінь, землетрус, пожежа тощо) розглядаються окремо. Навмисні загрози зумовлені цілеспрямованими діями порушників.

Для кожного активу визначаються групи загроз, що можуть мати на нього вплив. В зазначених групах наводиться більш чіткий опис загрози з зазначенням вимоги до захисту, що може бути порушена.

Загрози позначаються в графі «Threat Actor(s)».

Етап ІІ – Визначення частоти появи інциденту (LEF)

Дані другого етапу позначаються у вкладці «Inputs».

3. Оцінити частоту появи загрози (TEF)

Враховується ймовірна частота появи загрози, що буде впливати на зазначені активи протягом одного року. Період часу, що зазначається може змінюватися аналітиком за необхідністю. Відповідаючи на питання «Скільки разів протягом наступного року відбудеться загроза, що приведе до збитків?», зазначаються у відповідних графах мінімальну кількість, максимальну та найбільш ймовірну кількість. Зазначають також конфіденційність активу за шкалою «висока-середня-низька». За необхідністю заповнюють дані з обґрунтуванням чи додатковою інформацією.

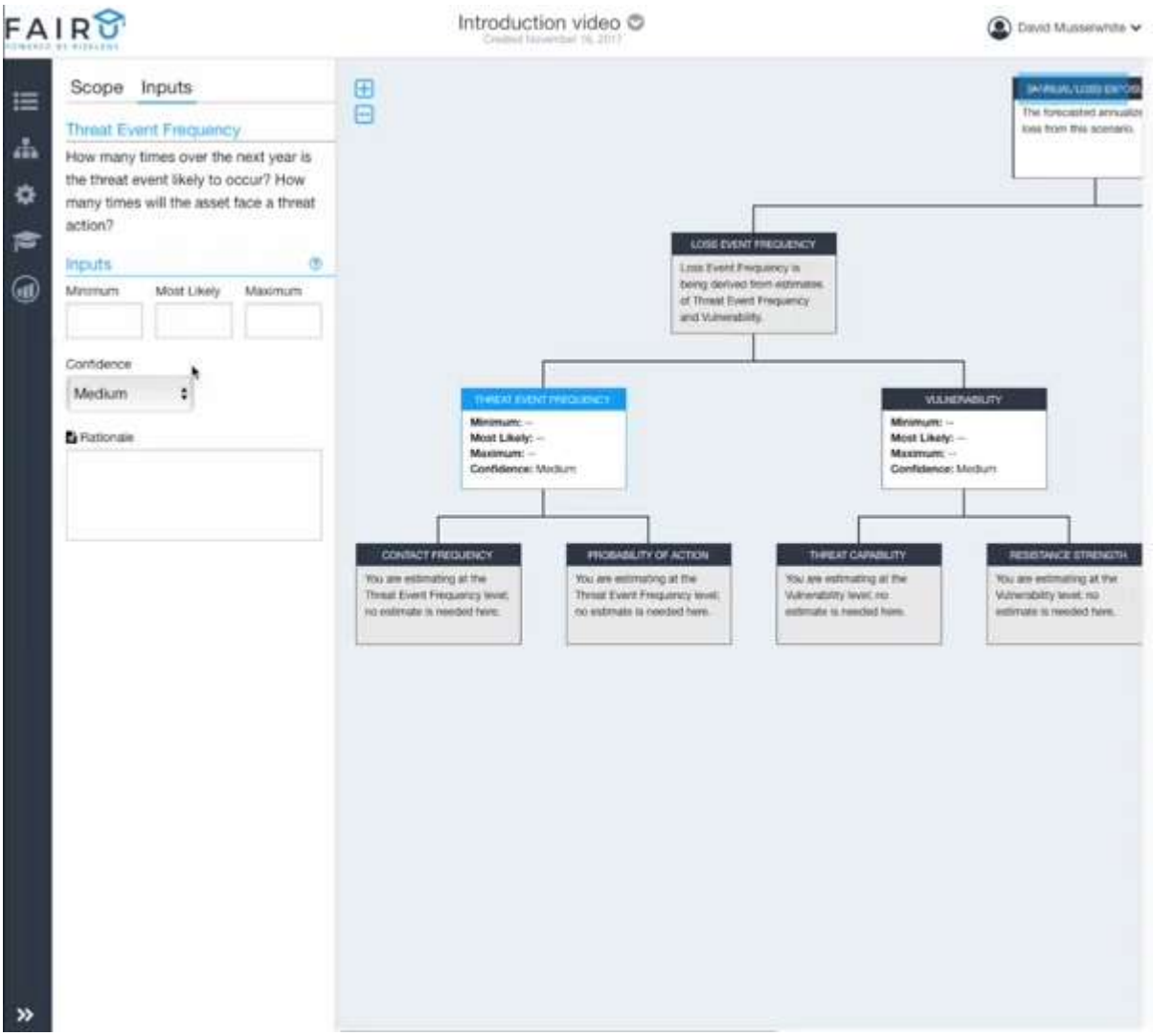

Рисунок 3 – Поле введення даних частоти появи загрози

4. Виявлення вразливостей (Vulnerability)

До кожної загрози прописують існуючу вразливість, що може стати причиною реалізації загрози. Позначають відсоток подій, пов'язаних із загрозою, що можуть призвести до втрат. Так само зазначають у відповідних графах мінімальну кількість, максимальну та найбільш ймовірну кількість. Дані щодо ймовірність того, що актив з використанням котрзаходів не зможе протистояти діям загрози розраховується програмою на основі наступних кроків.

5. Оцінка сили загрози (TCap)

Оцінюється ймовірний рівень сили, який загроза здатна застосувати до активу. Дані подаються у відсотках, з вказанням мінімальної, максимальної та найбільш ймовірної величини.

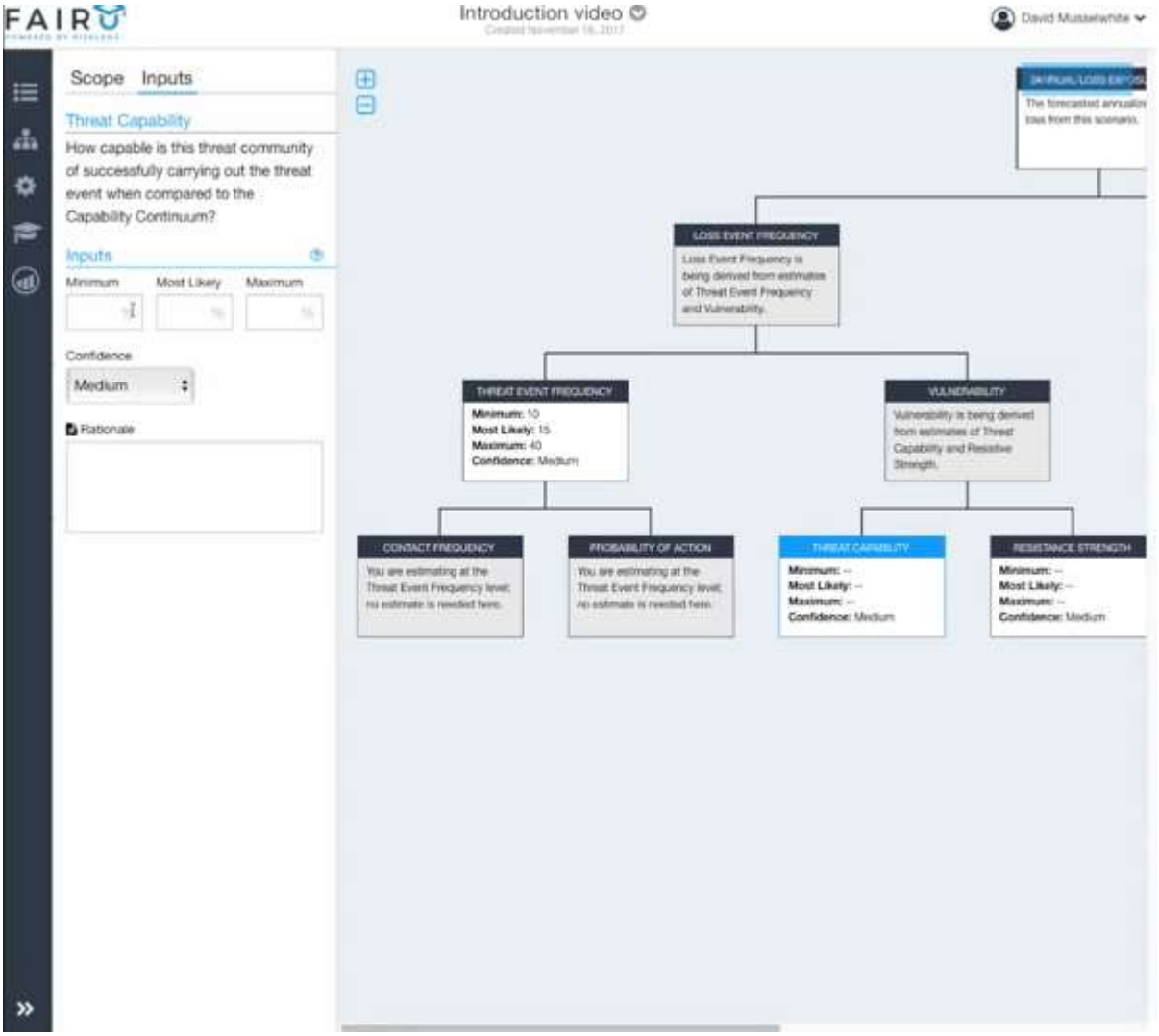

Рисунок 4 – Поле введення даних сили загрози

6. Оцінка ефективності контрзаходу (RS)

Розраховується Очікувана ефективність існуючого контрзаходу протягом певного періоду часу. Дані подаються у відсотках, з вказанням мінімальної, максимальної та найбільш ймовірної величини.

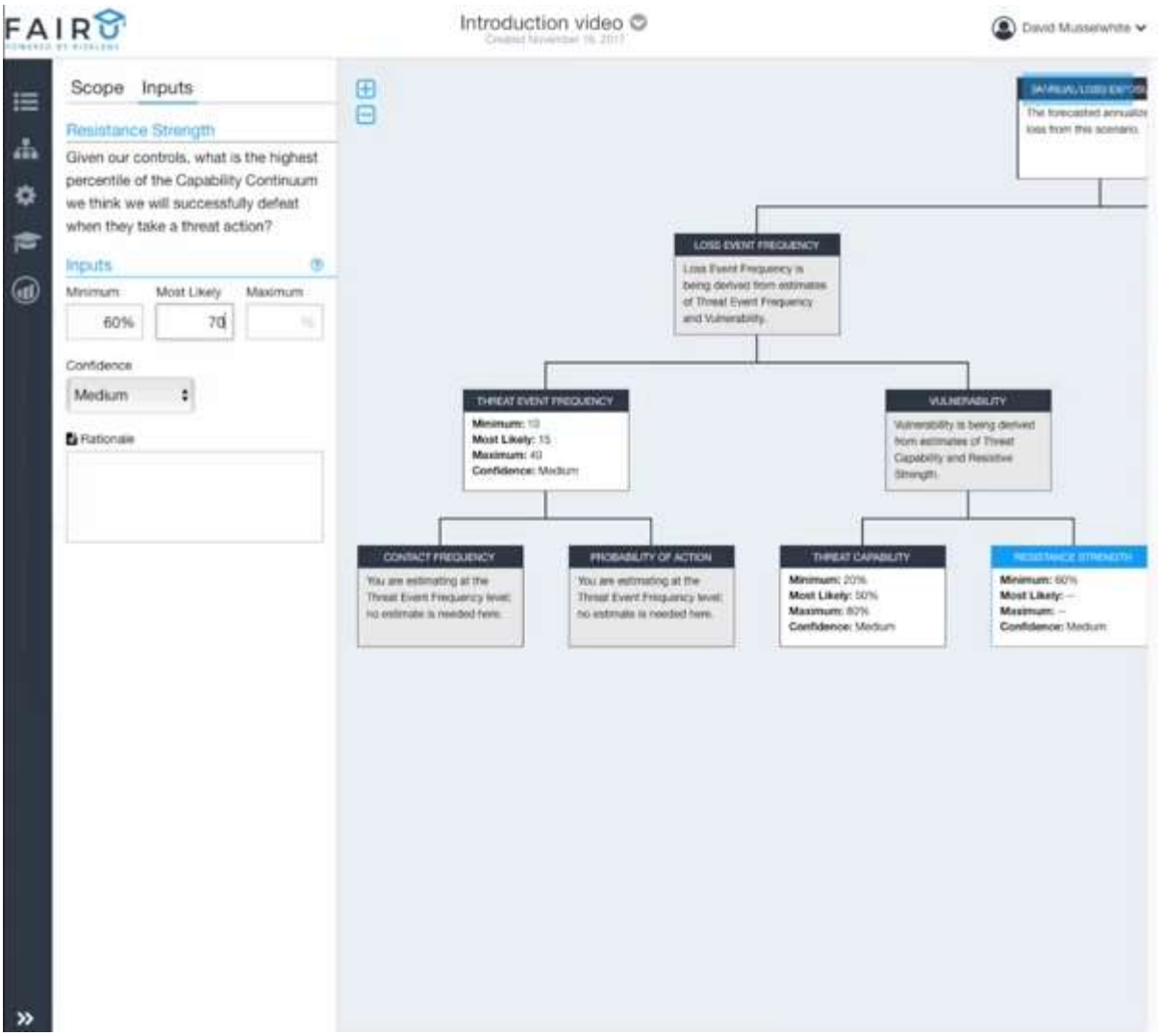

Рисунок 5 – Поле введення даних ефективності контрзаходів

7. Отримання даних частоти появи інциденту (LEF)

Ймовірна частота появи інциденту протягом певного періоду часу, розраховується програмою автоматично.

Етап III – Оцінка величини збитків (LM)

8. Оцінка первинних збитків

Задля даної оцінки необхідно відповісти на питання «Скільки грошей підприємство втратить від реалізації існуючої загрози?». Для оцінки найгіршого показника: визначають загрозу, яка, швидше за все, призведе до найгіршого результату; оцінюють величину для кожної форми втрат, пов'язану з цією загрозою. Дані найбільших, найменших та найімовірніших втрат

вказують в грошових одиницях для таких складових: продуктивність, заміна активу, репутація, штрафи.

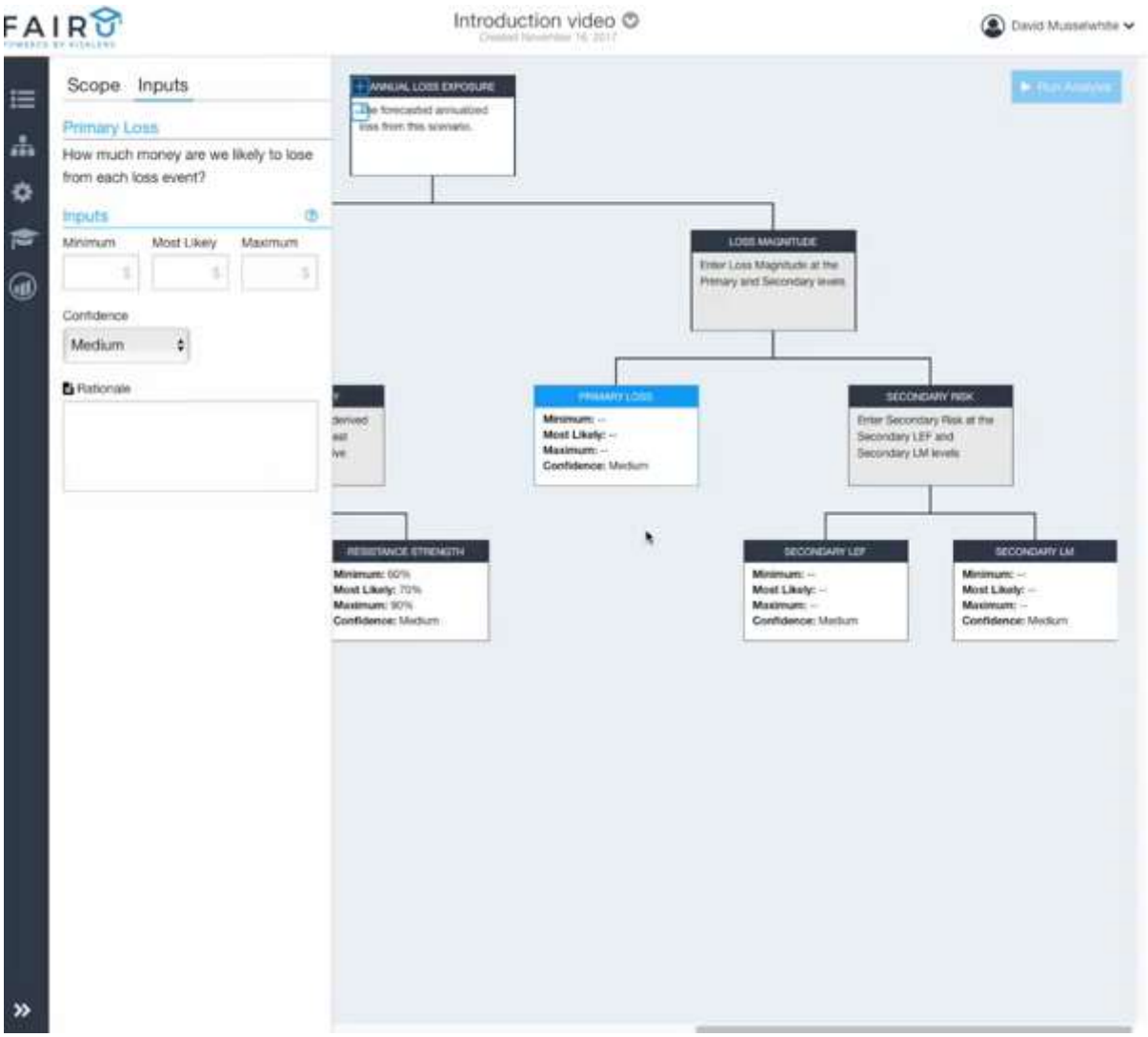

Рисунок 6 – Поле введення даних для оцінки первинних збитків

9. Оцінка вторинних збитків

Цей пункт відповідає на питання «Який відсоток подій первинного збитку, ймовірно, призведе до появи вторинних втрат?». Дані позначають у відсотках. Вторинні витрати розраховуються за складовими, що вказані в попередньому кроці. Тут необхідно оцінити скільки збитків підприємство зазнає внаслідок реакції вторинних зацікавлених сторін на первинну втрату.

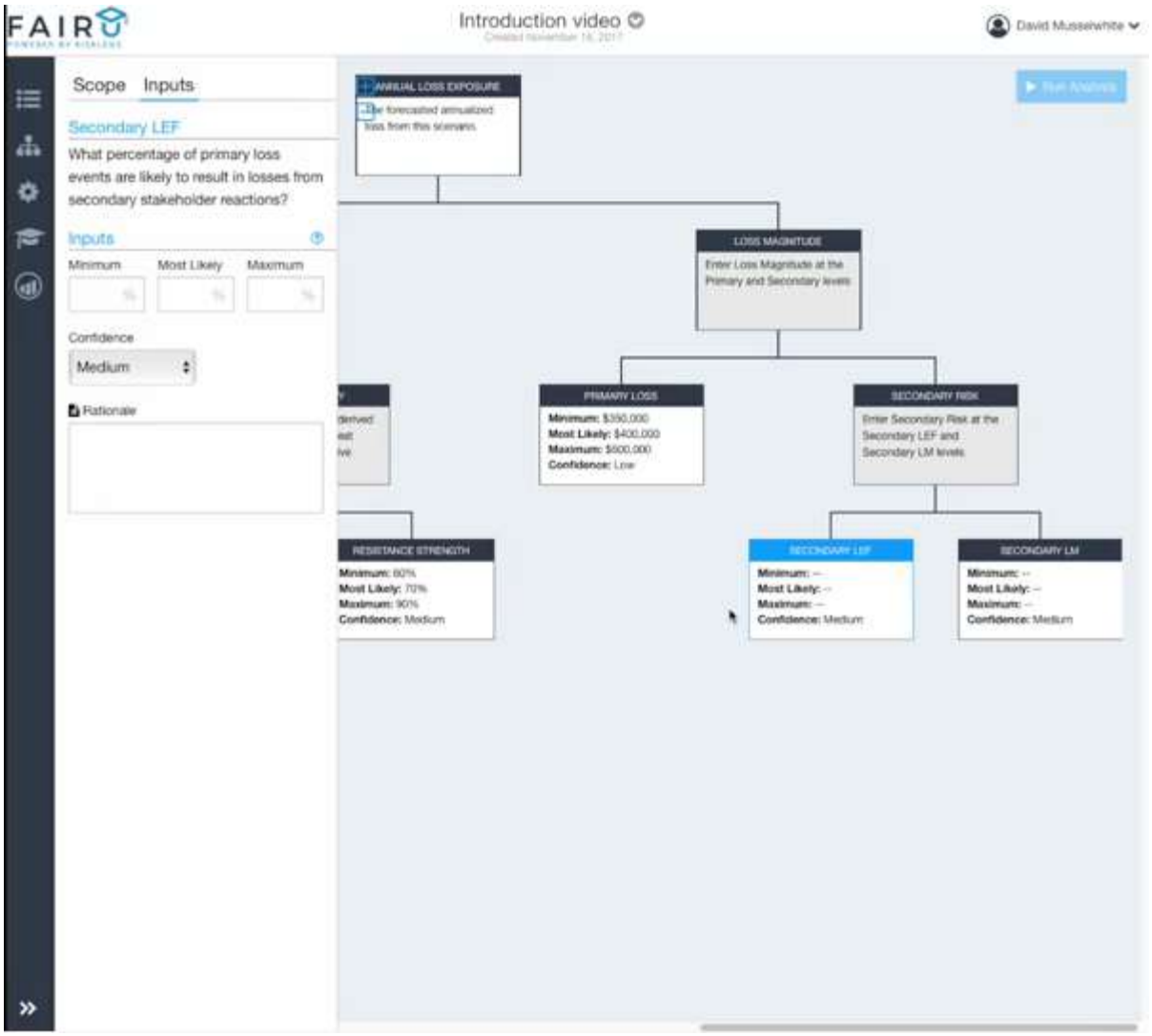

Рисунок 7 – Поле введення даних для оцінки вторинних збитків

Етап IV – Визначення величини ризиків

10. Для отримання вихідних даних пропонується «Провести аналіз», натиснувши на відповідну кнопку. З використанням методу Монте-Карло, ПЗ підраховує величини ризиків.

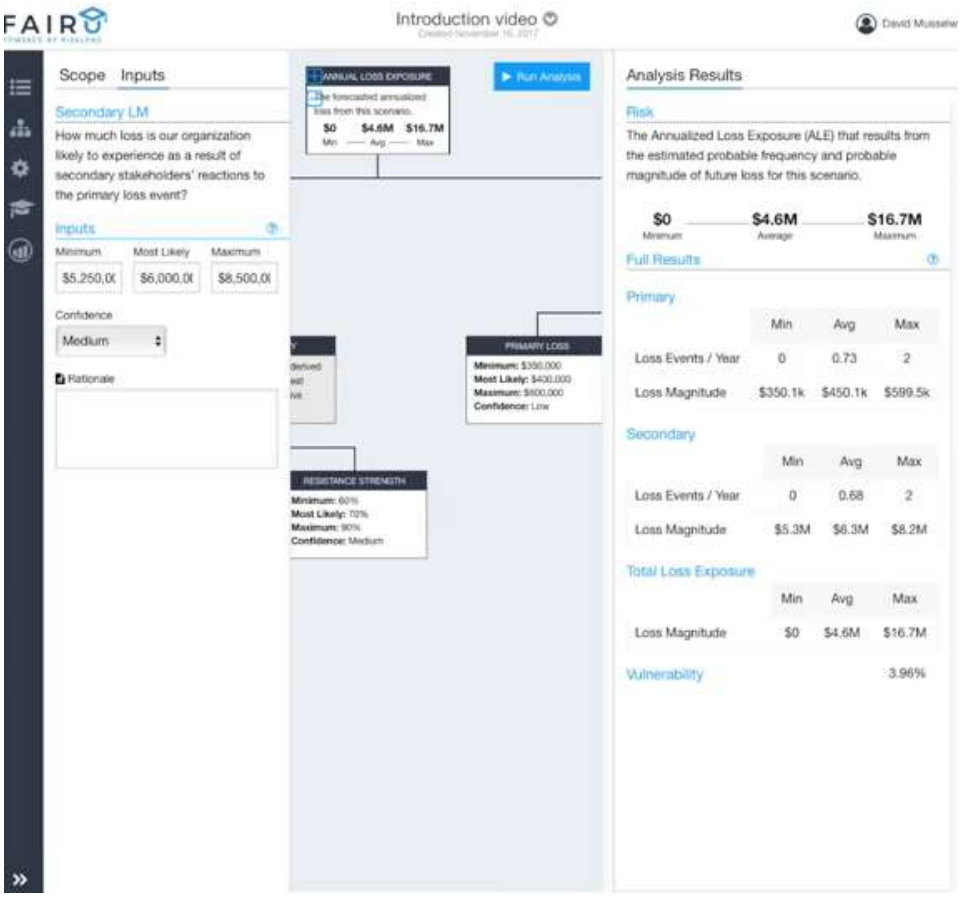

Рисунок 8 – Проведення аналізу ризиків

Рисунок 9 – Результат аналізу ризиків за методом FAIR