МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ЕТИЧНІ НОРМИ І ЗАСОБИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ І РИЗИКАМИ ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

_____ Ігор КУДІН
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Ігор КУДІН
Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ
Рецензент:
к.т.н.,
доцент: Юрій ПЕПА

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_____ Світлана ЛЕГОМІНОВА

“____”_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Кудіну Ігорю Валерійовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Етичні норми і засоби управління інформаційними інцидентами і ризиками ”

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.

(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека, управління інцидентами, корпоративна та професійна етика, етичні вимоги і стандарти, етичні кодекси кібербезпеки, наукова та технічна література*

4. Перелік питань, які потрібно розробити:
   1. Здійснити аналіз наукової літератури та публікацій, пов'язаних із застосуванням етичних методів і засобів управління інцидентами і ризиками інформаційної безпеки.
   2. Проаналізувати світовий досвід застосування етичних методів в управлінні інформаційними інцидентами і ризиками.
   3. Розробити методику застосування етичних норм і засобів в управлінні інцидентами та ризиками
   4. На основі аналізу розробити рекомендації щодо практичного застосування етичних норм і засобів в управлінні кібербезпекою.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання “02” жовтня 2023 р.

7.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Аналіз літератури та джерел щодо етичних аспектів управління інформаційними інцидентами і ризиками	27.10.2023	
4.	Дослідження основних етичних вимог та норм, які стосуються управління інформаційними ризиками	10.11.2023	
5.	Аналіз світового досвіду застосування етичних кодексів у кібербезпеці.	15.11.2023	
6.	Розробка методики застосування етичних норм в управлінні ризиками та інцидентами інформаційної безпеки	22.11.2023	
7.	Розробка пропозицій з практичного застосування етичних норм та засобів в управлінні інцидентами та ризиками	29.11.2023	
8.	Оформлення роботи.	04.12.2023	
9.	Оформлення презентації.	14.12.2023	
10.	Отримання рецензії на роботу.	18.12.2023	
11.	Захист в ДЕК.	__.01.2024	

Здобувач вищої освіти _____ Ігор КУДІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня магістра

Направляється здобувач Кудін І.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

Освітньо-професійної програми Управління інформаційною безпекою
(назва)

на тему: "Етичні норми і засоби управління інформаційними інцидентами і ризиками "
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **КУДІН Ігор** у кваліфікаційній роботі дослідив сучасний стан застосування сучасних етичних норм в управлінні кібербезпекою, визначив основні етичні виклики та проблеми управління інцидентами і ризиками, розробив зразок застосування моделі штучного інтелекту для аналізу та оцінювання інцидентів і ризиків. Удосконалив методику та відпрацював пропозиції з її застосування. Розроблені рекомендації разом із міжнародними стандартами забезпечать попередження інцидентів та вразливостей систем інформаційної безпеки організацій, дозволять керівниками організацій правильно організувати заходи кібербезпеки при здійсненні управлінської діяльності. **КУДІН Ігор** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **КУДІНА Ігоря** на оцінку "добре" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"_____" ____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кудін І.В. допускається до захисту роботи в екзаменаційній комісії

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Кудіна Ігоря Валерійовича
на тему “ ЕТИЧНІ НОРМИ І ЗАСОБИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ І РИЗИКАМИ ”

Актуальність

Актуальність обраної теми полягає в тому, що ефективне управління інцидентами вимагає постійного вдосконалення етичних методів та засобів, спостерігається зростання кількості інформаційних інцидентів, таких як кібератаки, витоки даних та інші. Етичні проблеми виникають як в процесі запобігання, так і в управлінні наслідками цих інцидентів і потребують проведення наукових досліджень.

Позитивні сторони

У роботі доцільно зосереджена увага на важливості забезпечення етичних норм в управлінні кібербезпекою з урахуванням міжнародних стандартів, такі як GDPR, ISO/IEC. Зроблений аналіз їх впливу на етичні аспекти управління інцидентами і ризиками дозволив зосередити увагу на удосконаленні методики їх аналізу та оцінки. Розроблений проект моделі виявлення, аналізу та оцінки інцидентів дозволяє керівникам структурних підрозділів інформаційної безпеки адаптувати її під особливості функціонування конкретних проблем кожної організації. Розробка методики внесли вагомий внесок у розуміння та практичне застосування етичних принципів управління інцидентами і ризиками.

Проведене комплексне дослідження етичних норм світових стандартів в управлінні кібербезпекою та визначені шляхи впровадження етичних норм в процеси управління кібербезпекою і розроблені підходи можуть бути використані в процесі планування та реалізації системи управління кібербезпекою організацій та підприємств.

Недоліки

Лістинг програми запропонованої моделі на основі штучного інтелекту доцільно було винести у додатки разом із навчальним і контрольним набором даних. Однак, зазначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «добре» а її автор Кудін Ігор Валерійович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач кафедри
Робототехніки та технічних
систем
к.т.н., доцент _____ Юрій ПЕПА
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 65 стор., 16 рис., 4 табл., 63 джерел.

Метою роботи є дослідження етичних норм та стандартів управлінні інцидентами та ризиками інформаційно безпеки та розробка методик і практичних рекомендацій для застосування способів та засобів в управлінні інцидентами та ризиками.

Об'єктом дослідження є процес управління інформаційними інцидентами та ризиками.

Предмет дослідження – етичні методи управління інформаційними інцидентами та ризиками.

*Методи дослідження***.** Аналіз при дослідженні нормативної бази та міжнародних стандартів, узагальнення і синтез існуючих підходів до застосування етичних норм в управлінні інцидентами і ризиками, моделювання при формуванні методики та оцінювання її ефективності, системний аналіз інтеграції етичних стандартів у корпоративні практики управління інцидентами і ризиками.

Короткий зміст роботи. Визначені та досліджені етичні принципи управління інформаційними інцидентами, а також проведено аналіз ризиків і етичних конфліктів в управлінні кібербезпекою та вплив. Визначені параметри та інструменти для оцінки ризиків з використанням етичного аналізу знайшли своє втілення в моделі та удосконаленій методиці виявлення, аналізу та оцінки інцидентів та ризиків інформаційної безпеки.

Галузь застосування. Результати дослідження можуть бути використані в процесі планування та реалізації системи управління інцидентами і ризиками організацій та підприємств, застосуванні етичних норм у корпоративних кодексах.

КЛЮЧОВІ СЛОВА: УПРАВЛІННЯ ІНЦИДЕНТАМИ І РИЗИКАМИ, КІБЕРБЕЗПЕКА, КОРПОРАТИВНА КУЛЬТУРА, ЕТИКА КІБЕРБЕЗПЕКИ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: 65 pages, 16 figures, 4 tables, 63 sources.

The purpose of the work is the study of ethical norms and standards for the management of incidents and risks of information security and the development of methods and practical recommendations for the use of methods and means in the management of incidents and risks.

***The object* of the study** is the process of managing information incidents and risks.

The subject of the research is ethical methods of managing information incidents and risks.

Research methods. Analysis during the research of the regulatory framework and international standards, generalization and synthesis of existing approaches to the application of ethical norms in incident and risk management, modeling in the formation of the methodology and evaluation of its effectiveness, systematic analysis of the integration of ethical standards into corporate incident and risk management practices.

Brief content of the work. Ethical principles of information incident management have been identified and researched, as well as an analysis of risks and ethical conflicts in cyber security management and impact. The defined parameters and tools for risk assessment using ethical analysis found their embodiment in the model and improved methodology for identifying, analyzing and evaluating information security incidents and risks.

Field of application. The results of the study can be used in the process of planning and implementation of the incident and risk management system of organizations and enterprises, the application of ethical norms in corporate codes.

KEYWORDS: INCIDENT AND RISK MANAGEMENT, CYBER SECURITY, CORPORATE CULTURE, CYBER SECURITY ETHICS.

ЗМІСТ

ВСТУП

Актуальність теми. Інформаційні технології швидко розвиваються, що призводить до появи нових інформаційних загроз і ризиків. Ефективне управління інцидентами вимагає постійного вдосконалення етичних методів та засобів. Спостерігається зростання кількості інформаційних інцидентів, таких як кібератаки, витоки даних та інші. Етичні питання виникають як в процесі запобігання, так і в управлінні наслідками цих інцидентів.

Ризик – неминучий супутник будь-яких відкриттів, технологічних проривів, вдалих інноваційних та управлінських дій. Ризики є невід'ємним елементом розвитку суспільства: ризикує кожен, хто до вирішення наявних проблем підходить творчо, мислить нестандартно, експериментує, діє не за шаблоном.

Інциденти та ризики є взаємопов'язаними концепціями в контексті управління інформаційною безпекою. Ризик може призвести до інцидентів, і управління ризиками спрямоване на мінімізацію ймовірності виникнення подібних інцидентів та зменшення їхніх наслідків. Разом з тим, процес створення загальної теорії ризиків носить нерівномірний, переривчастий характер.

Об'єктивна умова виникнення будь-якого ризику полягає у існуванні апріорної невизначеності: або відносно розвитку подій для певної ситуації, або щодо вибору дії в умовах наявності кількох можливих варіантів дій.

Сучасний соціально-політичний стан України призвів до істотних змін у виробничо-господарській діяльності, а також актуалізував необхідність перегляду ставлення до ризиків, формування нових концептуально-теоретичних уявлень про їх природу, функції, прояви, привернув увагу до питань практичного дослідження ризиків, їх ідентифікації, оцінювання, технологій управління ризиками.

Перелічені фактори зумовили актуальність теми дослідження.

Мета дослідження: дослідити етичні аспекти управління ризиками

інформаційної безпеки та розробити пропозиції по застосуванню етичних методів в управлінні інформаційною безпекою.

Для досягнення цієї мети в роботі виконані наступні завдання:

- здійснений аналіз наукової літератури та публікацій, пов'язаних із застосуванням етичних методів і засобів управління інцидентами і ризиками інформаційної безпеки;

- проаналізований світовий досвід застосування етичних методів в управлінні інформаційними інцидентами і ризиками;

- розроблена методика застосування етичних норм і засобів в управлінні інцидентами та ризиками;

- на основі аналізу розроблені рекомендації щодо практичного застосування етичних норм і засобів в управлінні кібербезпекою.

Об'єктом дослідження є управління інформаційними інцидентами і ризиками,

Предметом дослідження є етичні методи і засоби управління інцидентами і ризиками інформаційної безпеки.

Методи дослідження: з метою вирішення вище вказаних наукових завдань у даній роботі застосовані методи аналізу і синтезу, системного аналізу для виконання огляду в науковій літературі основних принципів застосування етичних норм в управлінні інцидентами, метод Кейс-стаді при аналізі впровадження ISO 27001 в інформаційно-технологічній компанії, моделювання при формуванні методики застосування етичних норм в управлінні.

Наукова новизна одержаних результатів полягає в тому, що вперше запропоновано застосування штучного інтелекту для виявлення, аналізу та оцінки інцидентів і ризиків та створена модель на мові програмування Python для комплексного виконання цих процедур, удосконалена методика з урахуванням визначених параметрів та інструментів для оцінки ризиків, проведено комплексне дослідження етичних норм світових стандартів в управлінні кібербезпекою та визначені шляхи

впровадження етичних кодексів в процеси управління кібербезпекою. Розроблена удосконалена методика може бути використана в процесі планування та реалізації системи управління кібербезпекою підприємства.

Практичне значення одержаних результатів. Застосування здобутих результатів дасть змогу автоматизувати процес збору аналізу та оцінювання інцидентів і ризиків, здійснити розробку або вдосконалення етичного кодексу компанії, який враховує світові стандарти та етичні норми в кібербезпеці, у відповідності до цілей бізнесу, корпоративних можливостей та ресурсів в сучасних умовах.

Апробація результатів кваліфікаційної роботи: було оприлюднено на науковій конференції:

Щавінський Ю. В., Кудін І. В., Порохницький О. А. Етичні методи та засоби управління інформаційними інцидентами і ризиками. Актуальні проблеми кібербезпеки : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 369–372.

РОЗДІЛ 1
ОСНОВИ ЕТИЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ І РИЗИКАМИ

1.1 Етичні принципи управління інформаційними інцидентами

У сфері досліджень роль етики з кожним роком зростає все більше і більше. Можливо, хтось здивується, але навіть у сфері технологій експертам необхідно розуміти та впроваджувати етичні принципи. Саму етику можна розуміти як кодекс або моральний спосіб, за яким людина живе і працює. Але в галузі інформаційних технологій та досліджень кібербезпеки існує ймовірність, що навіть найбільш технічно відповідне рішення може бути неузгоджено з етичними принципами. Експерти повинні впроваджувати фундаментальні етичні принципи у свої технічні продукти, щоб не завдати шкоди або не мати будь-якого негативного впливу на своїх користувачів. Такі проблеми, як забезпечення конфіденційності користувачів, звітування та обробка випадкових знахідок, тестування технологічного продукту, пом'якшення упереджень тощо, можуть мати різні негативні наслідки для людей, якщо їх не вирішувати належним чином.

Етичні питання, які виникають у сфері кібербезпеки, різняться з точки зору діяльності, що реалізується зацікавленими сторонами, та законодавчих вимог щодо рівня безпеки. Також слід враховувати інтенсивність ризиків, які можуть виникнути для людей. З появою нових технологій етичні ризики, пов'язані з кібербезпекою, можуть виникати в будь-якій сфері повсякденного життя – економіці, охороні здоров'я, громадській безпеці, транспорті тощо та завдавати різного рівня шкоди людям.

Самі ризики мають різний вплив на них – деякі з них мають прямі наслідки для їхніх прав, такі як порушення їхнього приватного життя та гідності [1], інші можуть мати згубний вплив на їхню економічну діяльність,

наприклад, хакерство та інші види порушень безпеки [2]. Перш ніж будуть вжиті будь-які заходи щодо пом'якшення конкретного ризику, зацікавлені суб'єкти повинні добре ознайомитися з ним, щоб вони могли вжити найбільш відповідних заходів для його усунення та зменшення будь-якого шкідливого впливу, який може бути спричинений.

Ризик - це ймовірність виникнення події чи ситуації, яка може мати негативний вплив на досягнення цілей організації чи проекту. У контексті управління ризиками, ризик визначається як комбінація ймовірності виникнення події та впливу цієї події на організацію.

Основні компоненти ризику включають:

- ймовірність виникнення: визначає, наскільки ймовірно подія чи ситуація може виникнути, Ймовірність може бути високою, середньою або низькою.

- вплив (масштаб впливу): визначає, як великий може бути вплив події, якщо вона станеться. Вплив може бути високим, середнім або низьким. Співвідношення компонентів ризику показано таблиці 1.1.

Таблиця 1.1

Співвідношення компонентів ризику

Загальна серйозність ризику				
Втрати	ВИСОКІ	Посередня	Висока	Критична
	ПОСЕРЕДНІ	Низька	Посередня	Висока
	НИЗЬКІ	Відсутня	Низька	Посередня
		НИЗЬКА	ПОСЕРЕДНЯ	ВИСОКА
	Імовірність			

- заходи по зменшенню ризику: ризик може бути управляємий шляхом впровадження заходів по зменшенню ймовірності виникнення події або зменшення її впливу, а також інших стратегій управління ризиками;
- ризикова сприйнятливість: це готовність організації або особи приймати ризик. Деякі організації можуть бути більш ризикозатримуючими, тоді як інші можуть бути консервативними та бажаючими уникати ризику.

Для управління ризиками можуть бути використані різні стратегії:

- уникнення;
- зменшення;
- передачу;
- прийняття ризику тощо.

Управління ризиками полягає в ідентифікації, оцінці, виявленні та контролі ризиків з метою забезпечення досягнення цілей організації та максимізації можливостей, в той час як мінімізація загроз.

Етичні принципи управління інформаційними інцидентами – це набір вказівок, які допомагають гарантувати, що інциденти інформаційної безпеки розглядаються відповідально та етично. Ці принципи призначені для керівництва діями груп реагування на інциденти та безпеки, а також для забезпечення того, щоб вони діяли в найкращих інтересах своїх виборців і суспільства в цілому.

Концепція EthicsFIRST (FIRST- Форум інцидентів Групи реагування та безпеки) є одним із таких принципів, які містять вказівки щодо етичної поведінки для команд реагування на інциденти та безпеки. Рамкова основа включає принципи, сформульовані як заяви про відповідальність, засновані на розумінні того, що суспільне благо завжди є головним фактором. EthicsfIRST розроблено, щоб надихати та спрямовувати етичну поведінку всіх членів команди, включаючи нинішніх та потенційних практиків, інструкторів, студентів, впливових осіб та всіх, хто ефективно використовує комп'ютерні технології. Ця структура включає принципи, сформульовані як заяви про

відповідальність, засновані на розумінні того, що суспільне благо завжди є першочерговим фактором. Кожен принцип доповнюється рекомендаціями, які містять пояснення, щоб допомогти фахівцям з обчислювальної техніки зрозуміти та застосувати цей принцип.

Обов'язки представлені нижче, але не в порядку важливості. Ці обов'язки слід розглядати не як абсолютні вимоги, а скоріше як зазначено в RFC2119 IETF для визначення «ПОВИНЕН»: "Це слово або прикметник "РЕКОМЕНДОВАНО" означає, що за певних обставин можуть існувати поважні причини ігнорувати конкретні [обов'язки], але всі наслідки повинні бути зрозумілі та ретельно зважені, перш ніж вибрати інший курс". (IETF - англ. Internet Engineering Task Force – відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів, створене IAB в 1986 році, яке займається розвитком протоколів і архітектури Інтернету).

Довіра є основою багатьох відносин між командами і часто потрібна для того, щоб відбувся змістовний обмін інформацією. Спільнота FIRST побудована на цій довірі, і вона може продовжувати функціонувати таким чином лише за наявності розумного рівня довіри між командами.

Нижче наведено деякі з ключових принципів структури EthicsfIRST (рис.1.1).

Етика для команд реагування на інциденти та безпеки

1. Обов'язок надійності
2. Обов'язок скоординованого розкриття вразливостей
3. Обов'язок конфіденційності
4. Обов'язок визнати
5. Обов'язок авторизації
6. Обов'язок інформувати
7. Обов'язок поважати права людини
8. Обов'язок перед здоров'ям команди
9. Обов'язок перед командою
10. Обов'язок відповідального інкасації
11. Обов'язок визнавати межі юрисдикції
12. Обов'язок доказового обґрунтування

Рис. 1.1. Перелік етичних обов’язків команди на реагування

1.Обов’язок надійності: члени команди повинні брати лише ті зобов’язання, які вони можуть виконувати, поводитися передбачувано по відношенню до інших команд і підтримувати довірчі стосунки, які вони мають з іншими командами.

2.Обов’язок скоординованого розкриття вразливості: члени команди, які дізнаються про вразливість, повинні слідувати скоординованому розкриттю вразливості, співпрацюючи із зацікавленими сторонами для усунення вразливості системи безпеки та мінімізації шкоди, пов’язаної з розголошенням.

Члени команди, які дізнаються про вразливість, повинні стежити за скоординованим розкриттям вразливостей, співпрацюючи із зацікавленими сторонами, щоб усунути вразливість безпеки та мінімізувати шкоду, пов'язану з розкриттям. До зацікавлених сторін належать, зокрема, повідомник про вразливості, постачальники, яких це стосується, координатори, захисники, а також клієнти, партнери та користувачі.

Члени команди повинні координувати свої дії з відповідними зацікавленими сторонами, щоб узгодити чіткі терміни та очікування щодо оприлюднення інформації, надавши достатньо деталей, щоб користувачі могли оцінити свій ризик і вжити дієвих захисних заходів.

3.Обов’язок конфіденційності: члени команди зобов’язані зберігати конфіденційність, якщо це доречно.

Члени команд реагування на інциденти та безпеки (Teams) мають доступ до багатьох цифрових систем та джерел інформації. Їхні дії можуть змінити світ. Як представник цієї професії, член команди повинен усвідомлювати відповідальність перед своїм виборцем та іншими фахівцями з безпеки, а також перед суспільством в цілому. Людина також повинна усвідомлювати свою відповідальність за власне благополуччя. Члени команди зобов'язані зберігати конфіденційність, де це доречно. Запити на збереження певної інформації в таємниці можуть бути явними, наприклад, за допомогою Протоколу світлофорів (TLP). Члени команди повинні поважати такі

прохання, коли це можливо. Якщо неможливо зберегти інформацію в таємниці, наприклад, через конфлікт з вимогами місцевого законодавства, контрактів або обов'язком інформувати, член команди повинен негайно повідомити власника інформації про цей конфлікт.

Деякі обов'язки щодо конфіденційності ґрунтуються на законах, правилах або звичаях. Якщо під час реагування на інцидент деякі сторони пов'язані або очікують конфіденційності на основі таких міркувань, вони повинні зробити все можливе, щоб ці очікування були чітко виражені заздалегідь. У такому разі всі сторони повинні дотримуватися вищезазначеного очікування щодо збереження чіткого запиту щодо збереження інформації в таємниці, коли це можливо.

4. Обов'язок визнання. Команди отримують інформацію з багатьох різних джерел: дослідників, клієнтів, інших команд, державних установ тощо. Члени команди повинні своєчасно відповідати на запити, навіть якщо це лише для підтвердження того, що запит було отримано. Коли це можливо, члени команди повинні визначити очікування щодо наступного оновлення.

5. Обов'язок авторизації. Члени команди мають законну потребу та право розуміти свої зони відповідальності, діючи лише в системах, доступ до яких їм дозволено. Члени команди повинні усвідомлювати, як їхні дії можуть вплинути на їхніх виборців, і переконатися, що вони не завдають додаткової шкоди під час виконання своїх обов'язків. Там, де це можливо, слід проконсультуватися з виборцями, перш ніж вносити зміни до їхніх систем.

6. Обов'язок інформувати. Члени команди повинні вважати своїм обов'язком інформувати своїх виборців про поточні загрози та ризики безпеки. Якщо члени Команди мають інформацію, яка може негативно вплинути або покращити безпеку та захист, вони зобов'язані повідомити про це відповідні сторони або інших осіб, які можуть допомогти, доклавши відповідних зусиль, належним чином враховуючи конфіденційність, закони та правила конфіденційності та інші зобов'язання.

7. Обов'язок поважати права людини. Члени команди повинні

усвідомлювати, що їхні дії можуть вплинути на права інших людей через обмін інформацією, можливу упередженість у своїх діях або порушення прав власності. Члени команди мають доступ до широкого спектру особистої, чутливої та конфіденційної інформації під час роботи з інцидентами. З цією інформацією слід поводитися таким чином, щоб забезпечити дотримання прав людини.

Під час роботи з інцидентами рятувальники не повинні діяти упереджено та повинні зробити все можливе, щоб усунути упередженість у своїх процесах та прийнятті рішень, які виконуються відповідачами або вбудовані в алгоритми.

Для цілей цього принципу поняття «власність» (Декларація прав людини ООН: стаття 17) включає в себе нематеріальні активи, такі як інтелектуальна власність, а також ідеї та концепції в цілому, незалежно від того, чи захищені вони законом (наприклад, запатентовані).

8. Обов'язок перед здоров'ям команди. Команди несуть відповідальність за те, щоб продовжувати надавати послуги, які вони пообіцяли своїм виборцям. Ця відповідальність включає в себе фізичне та емоційне здоров'я Команди.

Для того, щоб поважати як особистостей членів, які складають Команду, і забезпечувати довгострокову життєздатність підтримки належного рівня обслуговування, Команда повинна прагнути підтримувати здорове, безпечне та позитивне робоче середовище, яке підтримує фізичне та емоційне здоров'я (всіх) її членів. Для того, щоб реагувати на кризу, «нормальні» операції повинні підтримувати емоційне здоров'я та зниження стресу.

9. Обов'язок перед командою. Управління інцидентами – це тема, що розвивається, яку члени команди повинні постійно вивчати. Команда повинна надавати ресурси своїм членам, щоб вони могли вивчати, застосовувати та просувати технологічні та наукові знання в межах своєї сфери відповідальності. Навчальні або освітні кредити CPE/CEU можуть зробити свій внесок, але простих вправ на відповідність недостатньо для виконання

цього обов'язку. Команда повинна підтримувати достатню технологічну інфраструктуру для надання послуг, включаючи адекватні заходи для захисту цієї інфраструктури від втручання зовнішніх сторін.

10. Обов'язок відповідального інкасації. Збір даних необхідний для реагування на інциденти, але слід дотримуватися балансу між метою реагування на інциденти та повагою до зацікавлених сторін даних.

Під час розслідування обсяг інформації, необхідної для збору, може змінюватися. Під час проходження інциденту члени команди повинні коригувати те, що вони збирають, відповідно до потреби. Дані, які безпосередньо не стосуються інциденту та його виправлення, повинні бути виключені зі звітності.

Зібрані та вилучені дані повинні оброблятися відповідно до чинного законодавства та з повагою до конфіденційності користувачів. Дозвіл слід запитувати перед збором та обробкою даних під контролем власника даних. Слід дотримуватися чинного законодавства та нормативних актів щодо обробки даних.

Дані, які можуть допомогти іншим групам реагування в їхніх зусиллях, пов'язаних з іншими інцидентами, повинні бути надані їм, можливо, у відредагованій формі. Конфіденційна та службова інформація повинна надаватися лише з відповідним захистом.

Перш ніж ділитися даними з третіми сторонами для пом'якшення наслідків, слід зважити ризики та переваги. Дані слід передавати лише в тому випадку, якщо користь явно переважає ризики. Конфіденційні дані повинні зберігатися таким чином, щоб їх можна було легко знищити після закриття інциденту. Зібрані дані повинні бути безпечно знищені відповідно до політики зберігання даних.

11. Обов'язок визнавати межі юрисдикції. Члени команди повинні визнавати та поважати межі юрисдикції, юридичні права, правила та повноваження сторін, які беруть участь у діяльності, пов'язаній з реагуванням на інциденти.

Закони, нормативні акти та інші правові питання, наприклад, пов'язані із захистом конфіденційності або повідомленнями про порушення даних, можуть відрізнятися в різних залучених юрисдикціях. Межі юрисдикції можуть визначатися фізичним місцезнаходженням залучених сторін, таким як їхні країни або місця проживання, а також іншими факторами, що стосуються цих сторін. Навіть у межах однієї країни закони та нормативні акти можуть відрізнятися між політичними регіонами (наприклад, між окремими штатами США) або між різними підприємствами, галузями чи секторами в межах цієї країни (наприклад, охорона здоров'я, фінансові послуги та державні установи). Національні CSIRT можуть мати визначені обов'язки та/або повноваження щодо діяльності за участю виборців у межах їхньої власної юрисдикції, а також вони можуть співпрацювати або «передавати» інформацію та діяльність іншим суб'єктам, які мають повноваження для юрисдикцій, які перетинають кордони.

Члени команди повинні знати про ключові питання, які впливають на залучені юрисдикції, включаючи, але не обмежуючись, правилами конфіденційності або вимогами щодо повідомлень про порушення даних. Оскільки закони та нормативні акти про кібербезпеку та конфіденційність розвиваються та продовжують оновлюватися в усьому світі, рекомендується проконсультуватися з поінформованим юрисконсультом для отримання вказівок, коли питання стосуються кількох юрисдикційних кордонів.

12. Обов'язок доказового обґрунтування. Команди повинні діяти на основі фактів, які можна перевірити. Під час обміну інформацією, такою як індикатори компрометації (МОК) або описи інцидентів, члени команди повинні прозоро надавати докази та обсяг. Якщо це неможливо, слід зазначити причини відмови від надання цих доказів та обсяг інформації.

Членам команди слід утримуватися від поширення чуток. Будь-яка гіпотеза повинна бути чітко визначена як така.

Прозорі процеси доказів та обґрунтування важливі навіть у разі автоматизованого обміну, наприклад, під час автоматизованого обміну

великими обсягами інформації. У цьому випадку опис процесу інтелектуального аналізу даних повинен бути переданий на зрозумілому рівні деталізації.

Члени команди часто опиняються в ситуації, коли, здається, жодна дія не задовольняє всім етичним принципам. У такій ситуації необхідно зробити вибір, яким принципам віддати пріоритет. У цій ситуації обробникам інцидентів рекомендується поміркувати про те, на яких зацікавлених сторін можуть вплинути їхні дії та як, бажано під час дискусії з колегою. Як правило, слід вибирати те рішення, яке мінімізує порушення цих етичних рамок. Іноді це може бути неможливо, наприклад, через зовнішній тиск. У такій ситуації рекомендується діяти, звертаючи увагу на етичну дилему, можливо, під знаком протесту. Детально описані обов'язки групи етичного реагування на інциденти у Проекті (додаток А).

1.2 Аналіз ризиків і можливих етичних конфліктів в управлінні кібербезпекою

Ефективне управління конфліктами, як зазначає переважна більшість наукових досліджень [3-13] полягає у здатності менеджера знаходити оптимальні шляхи їх вирішення, які можуть бути як функціональними, так і дисфункціональними та будуть впливати на діяльність організації у довгостроковій перспективі. Також необхідно наголосити на особливостях управління конфліктами, які спираються на концепцію корпоративної соціальної відповідальності та важливості ролі керівника в управлінні конфліктами.

Ризики та етичні конфлікти в управлінні кібербезпекою є важливими питаннями, які потребують уваги. Існує багато досліджень на цю тему, які можуть допомогти вам зрозуміти ці питання краще. Наприклад, дослідження, проведене в 2020 році, показало, що кіберзлочини коштують світову

економіку майже 1 трильйон доларів США [14]. Це свідчить про те, що кібербезпека є серйозним питанням, яке потребує уваги.

Щодо етичних конфліктів, то в управлінні кібербезпекою можуть виникати різні етичні питання, наприклад, пов’язані з приватністю, безпекою, свободою слова та іншими [15]. Ці питання можуть бути складними, і їх потрібно розглядати з увагою до деталей. Наприклад, дослідження, проведене в 2021 році, показало, що недостатня кількість даних про кіберризики становить серйозну проблему для зацікавлених сторін, які намагаються вирішити це питання [16].

Моральні цінності, якими керується поведінка людини, є найважливішим компонентом будь-якого ефективного підходу до захисту кібербезпеки. Без визначених етичних норм і керівних принципів експерти з кібербезпеки нагадують чорних злодіїв, від яких вони намагаються захистити системи та дані.

Канони етики кібербезпеки, які охоплює різноманітний спектр підходів і шкіл думки, не дають однозначного вирішення численних складних етичних дилем, з якими щодня стикаються IT-фахівці, керівники відділу інформаційної безпеки (CISO) та організації. Навіть найбільш етичні та технічно досвідчені команди з кібербезпеки не можуть перешкодити найрішучішим зловмисникам. Як наслідок, розумно ретельно планувати проблеми кібербезпеки. Для цього потрібен добре підготовлений план реагування на інциденти, який описує технічні факти, надає практичні рекомендації для виконавчої та юридичної команд, а також вирішує будь-які критичні етичні проблеми.

Розберемо низку ситуацій етичних конфліктів в управлінні кібербезпекою та запропонованих дій на прикладі Кодексу етики для команд реагування на інциденти та безпеки (EthicsfIRST). Ці тематичні дослідження мають на меті представити дилеми, з якими можуть стикатися команди безпеки. Для кожного з обов'язків є один приклад, який відображає відповідні аспекти цього обов'язку. Формат прикладу полягає в тому, що спочатку

контекст описується в розділі «Ситуація», потім описується запропонована дія, а потім Резолюція, що описує, як це збалансовує різні обов'язки, описані EthicsfIRST. Для зручності читання потрібно спростити та уточнити приклади. Конкретного прикладу обов'язку поважати права людини немає. EthicsfIRST дотримується визначень прав людини, викладених Організацією Об'єднаних Націй, і вони враховані у наведених нижче тематичних дослідженнях.

Обов'язок надійності.

Ситуація: шукач повідомляє про проблему безпеки в операційний центр безпеки (SOC) компанії X. Організація має SOC і групу реагування на інциденти безпеки продуктів (PSIRT). Кожна команда в компанії X має власні механізми прийому (наприклад, електронна пошта, веб-сайт) і керує власними комунікаціями, але ці окремі команди не є очевидними для шукача. SOC постійно ігнорує листування з шукачем, і той, хто шукає, засмучується. Розчарований, шукач звертається до соціальних мереж про невдалий досвід, який вони отримали з PSIRT організації.

Дія: Кожна команда в компанії X повинна розуміти масштаб і місію іншої команди, а також мати налагоджені процеси для маршрутизації завдань між ними. SOC повинен передати справу PSIRT або власнику продукту на випадок, якщо компанія X не має повного PSIRT, який потім зв'яжеться з шукачем. Якщо шукач є членом іншої компанії, яка має PSIRT, компанія X повинна координувати свої дії з PSIRT шукача, щоб усунути поганий зв'язок і проінформувати його про кроки, які вживаються для виправлення процесу. Шукач видаляє блог і твіти. В результаті компанія вдосконалює внутрішні процеси обробки вразливостей між SOC і PSIRT.

Розв'язання: Надання чіткого механізму зв'язку для тих, хто шукає, щоб повідомити правильну команду, зменшує ймовірність плутанини та втрати кореспонденції. Побудова довірчих відносин і репутації перед подією або взаємодією важлива для своєчасного вирішення проблем безпеки або інцидентів. Довіра формується між людьми з часом. Наявність налагодженої мережі довіри може допомогти деескалації та зменшити ризик пошкодження

бренду.

Обов'язок скоординованого розкриття вразливостей.

Ситуація: Академічний дослідник знаходить вразливість у певних типах обладнання. Ця проблема поширена у багатьох виробників, що дуже ускладнює для дослідника скоординоване розкриття вразливостей (CVD) у кількох організаціях.

Дія: Дослідник звертається до свого національного CSIRT. Ця організація може допомогти зв'язатися з найбільш поширеними постачальниками, попередивши їх про знахідку. Хоча важко знайти всіх постачальників у цьому просторі, національна команда CSIRT також звертається до інших CSIRT та команд постачальників, які можуть допомогти поширити цей звіт про CVD.

Резолюція: Діючи як сполучна ланка, національний CSIRT координує вирішення вразливості з виробниками/виробниками компонента та попереджає компанії, які його використовують. Вони здатні пояснити глобальний контекст CVD, навіть між постачальниками, які можуть відчувати, що їм не дозволено спілкуватися один з одним через захист ринку. Це призводить до скоординованої міжгалузевої співпраці для вирішення проблеми.

Обов'язок конфіденційності.

Ситуація: Ви отримуєте інформацію від групи X про інцидент, яка визначає джерело атаки як таке, що походить від іншого з ваших учасників.

Дії: Ви оцінюєте індивідуальні обставини ситуації та визначаєте, чи є необхідні дії на основі місцевого та міжнародного законодавства. Ви зв'язуєтеся з першим доповідачем, учасником X, і просите дозволу на координацію з учасником Y. Організація, що повідомляє, не дає вам явного дозволу на обмін своїми журналами або інформацією зі свого сайту з відповідними контактами в джерелі атаки Y.

Розв'язання: Якщо ви не отримали явного дозволу організації, що звітує, на ідентифікацію її або її уражених систем як джерела звіту, ви повинні

зберігати конфіденційність і ідентичність джерела звіту, повідомляючи відповідну контактну особу служби безпеки в джерелі атаки.

Обов'язок визнання.

Ситуація: команда PSIRT отримує повідомлення про вразливість, яка впливає на поточний підтримуваний продукт. Минув тиждень, а шукач досі не отримав підтвердження про те, що його звіт отримано. Ще один лист надіслано, але відповіді все одно немає. Шукач зв'язується з командою PSIRT іншої компанії, яка використовує продукт першої компанії, щоб повідомити про проблему (або шукач просто оприлюднює інформацію).

Дії: Групи реагування на інциденти завжди повинні підтверджувати отримання повідомлення якомога швидше. Після того, як вони підтвердять, що це вразливість, вони повинні попередити шукача про це та дії, які вони планують вжити (виправити це, а не виправляти, оскільки продукт більше не підтримується, виправити його наступну версію тощо).

Розв'язання: Щоб уникнути подібних ситуацій, групи реагування на інциденти повинні мати налагоджені процеси отримання та підтвердження повідомлень. Скоординоване розкриття вразливостей не є вулицею з одностороннім рухом. Якщо команди не визнають звіти, вони можуть виявити, що не отримують їх.

Обов'язок авторизації.

Ситуація: CSIRT має досліджувати кінцеву точку, на якій основний користувач проживає в країні, яка підпадає під дію GDPR.

Дія: Проконсультуйтеся з експертами-юристами, щоб оцінити вимоги щодо дотримання місцевого та внутрішнього законодавства. У координації з юридичними експертами визначте найкращий курс дій для конкретного випадку, пам'ятаючи, що всі дії повинні виконуватися відповідно до міркувань щодо захисту конфіденційності користувачів, збираючи лише те, що суворо необхідно для підтримки цілісності середовища.

Розв'язання: Служби реагування на інциденти діють у межах своїх повноважень – консультуються з виборцями та відповідними зацікавленими

сторонами, де це можливо, перед залученням.

Обов'язок інформувати.

Ситуація: CSIRT стає відомо про інцидент. У їхньому середовищі існують законодавчі обмеження на обмін даними (злам, вразливість, скомпрометовані системи) за межами свого виборчого округу. Їм потрібно вирішити проблему, але якщо це вимагатиме від клієнтів вжити заходів, їм потрібно буде повідомити про це своїх клієнтів. Якщо персональні дані зазнали впливу, то цих користувачів потрібно буде повідомити.

Дії: Після того, як сайт знайомств був зламаний, CSIRT вирішив не перевіряти розкриті дані для свого виборчого округу, оскільки це може викликати збентеження у користувачів та їхніх організацій. Необхідно оцінити, чи є конфуз більш-менш ризикованим для організації, ніж розслідування та повідомлення постраждалих користувачів.

Рішення: Користувачі мають право приймати рішення, засновані на ризиках, або вживати заходів для пом'якшення потенційних негативних наслідків у результаті витоку особистої інформації. Потенційним користувачам надається інформація для обґрунтування їхніх рішень щодо підписки.

Обов'язок перед здоров'ям команди.

Ситуація: За останні два роки кількість випадків захворювання зросла більш ніж на 100% у команді реагування на інциденти. Кожен член команди регулярно працює над кількома інцидентами. Вони виснажені і вже кілька місяців не мають перерви. Моральний дух значно знизився. Учасники починають залишати компанію, збільшуючи навантаження на команду, що залишилася.

Дії: Щоб уникнути цього, команди повинні переконатися, що учасники відновлюються, роблячи перерви та відключаючись від роботи. Якщо робоче навантаження не зменшується, керівникам слід подумати про те, щоб відстоювати додаткові можливості або змінити пріоритети командних обов'язків/послуг. Дотримуючись місцевого трудового законодавства та

вказівок, команди повинні враховувати гнучкий графік роботи та розумне пристосування.

Резолюція: Хоча команди час від часу матимуть раунд надзвичайних ситуацій, це не повинно бути повсякденними очікуваннями. Командам потрібен час, щоб відпочити та «відключитися», щоб залишатися ефективними, ефективними, щасливими та здоровими. Команди, які продовжують підштовхувати своїх членів до недостатнього балансу між роботою та особистим життям, можуть зіткнутися з високими показниками плинності кадрів, проблемами зі здоров'ям, пов'язаними зі стресом, і деморалізованою робочою силою.

Обов'язок перед командою.

Ситуація: Послуги команди запитує установча організація. Команда відправляє в запитуючу організацію двох членів: нового співробітника і більш досвідченого учасника. Обидва учасники мають потужну технічну підготовку, але новий співробітник не був навчений стандартним процедурам команди щодо обробки конфіденційної інформації.

Дії: Команди повинні переконатися, що всі учасники пройшли належну підготовку перед розгортанням на складовому об'єкті. Команди повинні подумати, скільки повністю навчених співробітників потрібно для задоволення потреб на місці, а потім додати нового працівника як учня до команди.

Резолюція: У цьому сценарії прийнятно проводити навчання на робочому місці для нового працівника за умови, що команда все ще може безпечно задовольняти потреби організації, що входить до його складу. Більш досвідчений член команди (члени) повинен забезпечити новому члену команди психологічну безпеку для постановки запитань («дурних питань не буває») і приділяти особливу увагу щоразу, коли обробляється конфіденційна інформація. Не слід очікувати, що нові члени команди «розберуться» на роботі.

Обов'язок відповідального інкасації.

Ситуація: CSIRT отримує юридичний дозвіл на збір інформації про цифрову криміналістику та мережеву діагностику від скомпрометованого хоста в межах своєї юрисдикції. CSIRT починає збір і починає розробляти інформацію про загрози на основі зібраних даних (хешів, мережевих адрес і зразків шкідливого програмного забезпечення для подальшого аналізу). У міру просування проекту команда продовжує збирати дані через кілька місяців після завершення розслідування. Команда збирає дані, перевищуючи початкову мету збору, що, можливо, наражає організацію на ризик порушення закону.

Дії: Щоб запобігти надмірному збору, команди повинні заздалегідь встановити чіткі правила збору та зберігання даних, які передбачають часові межі (дати початку та завершення збирання). Якщо кінцева дата досягнута до того, як цілі збору будуть досягнуті, CSIRT може продовжити дату закінчення збору даних з огляду на юридичний дозвіл, цільову мету та можливе розпорядження.

Розв'язання: Щоб уникнути цього ризику, CSIRT повинні гарантувати, що зібрані дані використовуються лише за призначенням (наприклад: цифрове криміналістичне реагування на інциденти, діагностика мережі, аналіз вразливостей або розробка розвідки загроз). Після того, як зібрані дані вичерпали свою корисність для цієї мети, з ними слід поводитися відповідно до встановленої політики зберігання даних в інтересах мінімізації ризику викриття або неправильного використання в майбутньому.

Обов'язок визнавати межі юрисдикції.

Ситуація: Провайдер веб-хостингу в країні А зазнав атаки невідомого кіберзлочинця. Злочинець здатний скомпрометувати сервіс і витягти дані клієнтів, включаючи клієнтів з країни Х. Команда дотримується вимог країни А, але пропускає дедлайн і вимоги щодо звітності для країни Х. Потім орган із захисту даних країни Х штрафує постачальника веб-хостингу за недотримання вимог щодо повідомлень про витік даних.

Дії: Команди повинні регулярно переглядати процедури інцидентів і

правила конфіденційності, щоб переконатися, що їхня практика відповідає відповідним законам і вимогам. Команди повинні співпрацювати зі своїми юридичними представниками та представниками з питань конфіденційності, щоб розробити відповідні плани та документацію для поширених сценаріїв. Якщо виникає нестандартна ситуація, команди звертаються до юридичного представництва для отримання консультацій щодо конкретної ситуації.

Розв'язання: Відповідач повинен знати процедури звітування, необхідні як для місцевої юрисдикції (країна A), так і для юрисдикції власника даних (країна X). Можуть виникати різні правила щодо повідомлень та обов'язків відповідального за інцидент. Якщо юрисдикційні норми суперечливі, команди повинні знати, до кого і як своєчасно звертатися за відповідною юридичною консультацією.

Обов'язок доказового обґрунтування.

Ситуація: Сервісну фірму, яка реагує на інциденти, просять провести оцінку стану кібербезпеки жертви після інциденту. Після завершення оцінки CSIRT сервісної фірми подає свої рекомендації організації-жертві. Через місяць організація-жертва заявляє, що виконала всі рекомендовані дії, і просить CSIRT надати «чистий звіт про стан здоров'я». CSIRT не впевнений, чи повинні вони надавати сертифікацію чи ні.

Дії: CSIRT повинен незалежно оцінити кібербезпеку організації-жертви після інциденту АБО не надавати жодних підтверджень без доказів, що підтверджують це.

Рішення: Сервісна фірма повинна заздалегідь повідомити, як буде проводитися оцінка і як будуть аналізуватися виправлення. Фірма не повинна надавати будь-яке схвалення оновленої позиції кібербезпеки організації-замовника без попереднього проведення власної оцінки, щоб довести, чи дійсно рекомендації були дотримані.

Необов'язкове пояснення: Результати оцінювання повинні ґрунтуватися на прозорих і точних міркуваннях, підкріплених доказами. Докази, а отже, і висновки, можуть змінюватися з часом. Оцінки повинні чітко вказувати на те,

які докази були зібрані, як вони були інтерпретовані, які докази можуть змінити оцінку, а також ступінь невизначеності у зборі, інтерпретації доказів та прогалинах.

Сучасні методи етичного нагляду щодо етики кібербезпеки є неадекватними. Ці методи зазнають невдачі принаймні у двох сферах: наукові розробки та в ширшій спільноті практикуючих експертів з кібербезпеки. У першому випадку проблеми пов'язані з недостатньою поінформованістю членів спільноти комп'ютерної безпеки та етичних комітетів щодо природи етичних проблем щодо кібербезпеки. В другому випадку проблеми широко відомі, але відсутність адекватного керівництва або підзвітності створює бар'єр на шляху до послідовної етичної практики. Разом з тим, поточні розробки або практика кібербезпеки є неетичними. Скоріше, точка зору полягає в тому, що ці практики значною мірою залишаються нерегульованими та некерованими, незважаючи на очевидну потенційну можливість завдати значної шкоди.

Висновок до першого розділу. Визначені та досліджені етичні принципи управління інформаційними інцидентами, а також проведено аналіз ризиків і етичних конфліктів в управлінні кібербезпекою. Висвітлення цих аспектів дозволило визначити важливі питання, пов'язані із забезпеченням етичного та відповідального управління інформаційними ризиками. Потрібно відзначити, що таким чином, необхідно більше оцінювати ризики, пов'язані з розвитком кібербезпеки, у комітетах з етичних перевірок та чітких кодексах поведінки для професійної спільноти, які охоплюють як розвиток, так і практику.

Проблема, що стоїть перед управлінням, полягає в тому, що існуючі структури в університетах та інших формальних дослідницьких середовищах можуть бути недостатньо гнучкими у визнанні етичних питань, порушених у цьому документі. Це ілюструє перший випадок, в якому кілька Рад з дослідницької етики (REB) не змогли захистити інтереси суб'єктів дослідження в тому, що було очевидно сумнівним з етичної точки зору

дослідженням. З іншого боку, там, де дослідження проводяться за межами цих середовищ, як правило, в приватному секторі, відсутні структури управління, що ставить перед дослідниками ще складніше завдання, коли вони шукають етичний внесок для керівництва своїми дослідженнями.

РОЗДІЛ 2
ЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

2.1 Етичні вимоги до ризик-менеджменту

Етичні міркування стають все більш важливими у сфері управління ризиками. Зараз організації визнають необхідність заохочувати етичне лідерство та прийняття рішень на основі цінностей для управління складними нематеріальними ризиками

Науковці у своїх дослідженнях [17-20] визначили етичні вимоги до ризик-менеджменту, норми та принципи, які слід враховувати при виявленні, оцінці та управлінні ризиками в організації. Загальні етичні принципи, які можна застосовувати до ризик-менеджменту, включають (рис.2.1):

- прозорість: забезпечення відкритості та доступу до інформації про ризики для всіх зацікавлених сторін, включаючи співробітників, інвесторів, клієнтів та інші стейкхолдери.
- ділова доброчесність: здійснення ризик-менеджменту відповідно до закону та в межах етичних норм, уникаючи неправомірних дій чи маніпуляцій;
- врахування інтересів стейкхолдерів: врахування та уважне вислуховування інтересів різних стейкхолдерів при виявленні та управлінні ризиками;
- справедливість та рівноправ'я: забезпечення справедливого розподілу ризиків та врахування інтересів усіх сторін без дискримінації;
- збалансованість між ризиком та користю: врахування величини ризику та потенційної користі при прийнятті рішень щодо управління ризиками;
- захист конфіденційності: забезпечення конфіденційності чутливої інформації та уникаючи неправомірного використання цієї інформації при

ризик-менеджменті;

- етика досліджень: здійснення ретельного та об'єктивного дослідження ризиків без намагання на вигоду однієї зі сторін;

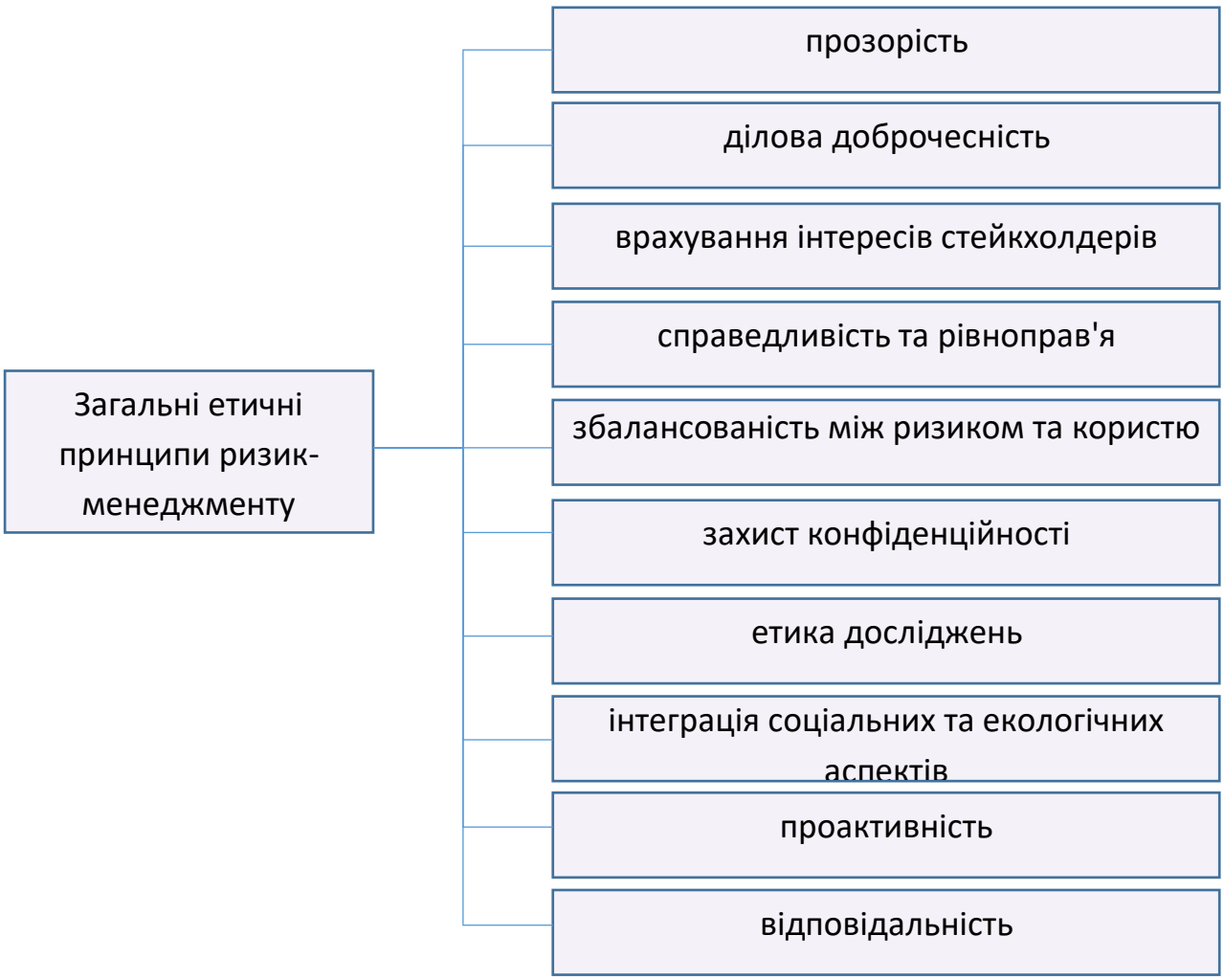

Рис. 2.1. Загальні етичні принципи ризик-менеджменту

- інтеграція соціальних та екологічних аспектів: врахування соціальних та екологічних наслідків ризиків при прийнятті рішень;

- проактивність - проактивне виявлення та управління ризиками перед тим, як вони стануть критичними;

- відповідальність: прийняття відповідальності за управління ризиками та їх вплив на діяльність організації та стейкхолдерів.

Етичні вимоги до управління ризиками інформаційної безпеки мають вирішальне значення для забезпечення захисту інформації організації від

несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення. Згідно зі стандартом ISO/IEC 27001, оцінка ризиків – це те, що встановлює та підтримує вимоги до ризиків інформаційної безпеки, генерує послідовні, точні та позиційні результати, а також визначає, інтерпретує та оцінює ризики у співпраці з власниками ризиків.

У контексті організації ISO/IEC 27001:2013 позиціонує себе як стандарт, який визначає вимоги до встановлення, впровадження, підтримки та постійної розробки стратегії інформаційної безпеки. Крім того, він включає необхідні обставини, які налаштовані відповідно до очікувань компанії щодо оцінки та управління загрозами безпеці даних. Ці передумови мають важливе значення для забезпечення ефективного зниження ризиків інформаційної безпеки. Умови, викладені в стандарті ISO/IEC 27001:2013, є неспецифічними, а це означає, що очікується, що вони застосовуватимуться до всіх організацій, незалежно від типу, розміру чи характеру бізнесу. Це стандарт безпеки, який користується великою повагою і визнається в глобальному масштабі [21-30].

Керівні принципи етичної поведінки, передбачені стандартами ISO 27000, можуть бути використані як частина всеосяжної стратегії інформаційної безпеки.

Окрім стандартів відповідності, управління ризиками розширюється від захисту балансу до сприяння етичного лідерства та прийняття рішень на основі цінностей. Організації повинні встановити прості правила етики для кращого управління ризиками, які віддають пріоритет прийняттю рішень на основі цінностей та етичному лідерству[31].

Науковці [25,27-29] наводять такі переваги впровадження ISO 27001:

- компанія або організація, яка впроваджує ISO 27001, може реалізувати низку важливих і значних переваг.
- компанії можуть захищати свої конфіденційні дані та послідовно керувати ними, впроваджуючи ISO 27001. Це досягається шляхом налаштування прозорого процесу обробки інформації, її контролю, а також обробки. Для досягнення цієї мети процес обробки даних повинен бути чітким

і управлятися безперервно. На додаток до цієї переваги, отримання ISO 27001 може допомогти репутації компанії. Це можна трактувати як збільшення прибутку та частки ринку через те, що клієнти з більшою ймовірністю довіряють свою особисту інформацію бізнесу, сертифікованому за стандартом ISO 27001.

- В результаті компанія отримує впевненість у собі та конкурентну перевагу, необхідну для розширення клієнтської бази. Також важливо переконатися, що ви дотримуєтеся національних і міжнародних норм, таких як Загальний регламент захисту даних (GDPR), а також будь-яких інших застосовних законів. Ризик понести юридичне покарання за розголошення конфіденційної інформації може призвести до затяжних судових баталій, а також до значних фінансових втрат.

Відповідно до пункту 6.1.2 ISO 27001, оцінка ризику – це те, що встановлює та підтримує вимоги до ризиків інформаційної безпеки, генерує послідовні, точні та позиційні результати, а також визначає, інтерпретує та оцінює ризики у співпраці з власниками ризиків.

В рамках оцінки ризику можуть бути виконані наступні процедури: ідентифікація потенційних небезпек, категоризація ймовірності того, що загроза матеріалізується по відношенню до даного суб'єкта господарювання, підтвердження впливу, який зазвичай включає майбутні витрати, структурні збої і витрати на відновлення, а також зниження втрат шляхом об'єднання управління ризиками в уже існуючі бізнес-процеси [32].

Міжнародна організація зі стандартизації (ISO) встановила низку глобальних стандартів для застосування керівних принципів стратегічної практики, одним з яких є стандарт управління ризиками ISO 31000. Ці стандарти управління ризиками є низкою світових стандартів. ISO 31000, як і переважна більшість інших стандартів управління ISO, створює системний підхід з метою задоволення вимог підприємств різного розміру та характеру [33-38]. Крім того, було рекомендовано використовувати стандарт ISO 31000:2018 як належну основу для взаємодії з невизначеністю при

ідентифікації небезпек у промисловій діяльності. Це одна з пропозицій, які були висунуті. Нещодавно було запропоновано структуру управління ризиками ISO 31000:2018 як життєздатну установу для проведення поглибленого дослідження в галузі управління ризиками. Це дослідження призначене для того, щоб краще зрозуміти управління ризиками (рис. 2.2)

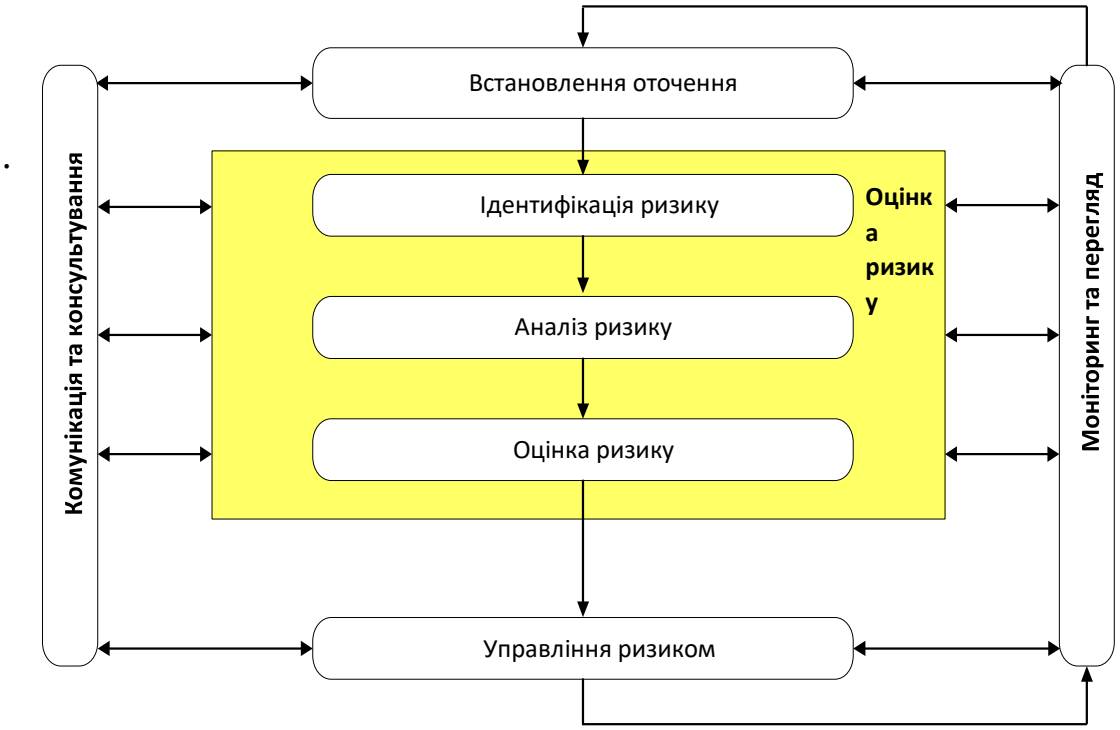

Рис. 2.2. Процес управління ризиками згідно ISO 31000:2009

Незважаючи на те, що респонденти в галузі є основними користувачами бенчмарку, той факт, що він адаптивний і не має бізнес- або галузевої специфіки, робить його привабливим варіантом. У ISO 31000:2018 концепція ризику відрізняється від безлічі несприятливих класифікацій, що використовуються в традиційній оцінці схильності, в тому сенсі, що ризик не просто характеризується у світлі ймовірності несприятливих або несприятливих ефектів. Скоріше, акцент робиться на управлінні ризиками. Це пов'язано з тим, що ризик не просто характеризується у світлі ймовірності негативного або несприятливого впливу. Це суттєва відмінність між визначенням ризику ISO 31000:2018 та іншими визначеннями ризику.

Відповідно до рекомендацій ISO 31000:2018, управління ризиками є прогресивною процедурою, яка включає такі дії:

1) класифікацію компетенції, конотації та вимог;

2) оцінка ризиків, яка включає виявлення, аналіз та оцінку ризиків;

3) поводження з ризиками;

4) збір та звітність даних;

5) перегляд та моніторинг ризиків;

6) комунікація та співпраця [31].

Група стандартів ризик-менеджменту складає (рис. 2.3)

Рис. 2.3. Група стандартів ризик-менеджменту

- ISO 31000:2009 Risk management – Principles and guidelines (принципи та настанови);
- ISO/TR 31004:2013 Risk management – Guidance for the implementation of (настанови до впровадження) ISO 31000.
- IEC 31010:2009 Risk management – Risk assessment techniques (Методи оцінки ризиків).

Еталон ISO 31000 відокремлює програму управління ризиками від принципів управління ризиками та керівних принципів, що використовуються організацією для управління ризиками. Структура системи управління ризиками складається з цих трьох частин. Основи та інституційні механізми для розробки, інтеграції, вимірювання, оцінки та вдосконалення управління ризиками на підприємстві закладаються повним набором елементів

управління ризиками.

ISO 31000 – це структура управління ризиками, яку іноді називають стандартом управління ризиками. ISO 31000 є одним із прикладів такої структури. Терміни «управління ризиками» та «оцінка ризиків» часто використовуються як синоніми, коли обговорюється процес спілкування, консультування, встановлення контексту та виявлення, оцінки, оцінки, лікування, моніторингу та перегляду ризику в організації. Те, що прийнято називати «управлінням ризиками» [39], насправді є процедурою, основною метою якої є боротьба з небезпеками.

Міжнародна організація зі стандартизації (ISO) 31000 викладає фундаментальні принципи, рамки та методи. ЇЇ мета полягає у визначенні процесу управління ризиками в будь-якій конкретній фірмі, включаючи безпеку, а не в забезпеченні однаковості систем управління ризиками. Незалежно від розміру або характеру організації, вона надає підприємствам стандарти управління ризиками, які можуть бути використані в процесі формулювання та досягнення своїх цілей. Концепції, рамки та процедури можуть бути застосовані як до державних, так і до приватних організацій, а також до будь-яких видів груп, асоціацій та підприємств. Вона закладає основу для стандартизованого методу управління ризиками, який не є специфічним ні для галузі, ні для сектора. Підхід, відомий як «управління ризиками», може бути використаний для пом'якшення практично будь-якого типу ризику. Вона застосовна протягом усього існування організації і до будь-якої діяльності, включаючи прийняття рішень на всіх рівнях

Враховуючи положення визначених стандартів необхідно сформувати етичні вимоги до ризик-менеджменту, які спрямовані на те, щоб забезпечити проведення етичних та справедливих практик у сфері управління ризиками:

- забезпечення прозорості у процесі управління ризиками, включаючи чесність у звітності та доступність інформації для всіх зацікавлених сторін;

- забезпечення справедливого та рівноправного доступу до інформації та можливостей управління ризиками для всіх зацікавлених сторін.

- захист конфіденційної інформації та особистих даних під час здійснення процесів ризик-менеджменту;

- врахування етичних засад при прийнятті рішень у контексті управління ризиками, включаючи моральні та соціальні аспекти;

- прийняття відповідальності за наслідки ризикованих рішень та їхній вплив на зацікавлених сторін;

- інтеграція етичних принципів у всі аспекти ризик-менеджменту, включаючи процеси, стратегії та комунікації;

- врахування та відповідність зі суспільними цінностями та очікуваннями щодо етичності в управлінні ризиками;

- урахування соціальних впливів та врахування інтересів груп та спільнот у процесах ризик-менеджменту.

- уникання дискримінації на основі раси, статі, віку, релігії, національності чи інших факторів під час управління ризиками.

Забезпечення етичних стандартів у ризик-менеджменті сприяє підвищенню довіри зацікавлених сторін, зменшенню ризиків щодо негативних наслідків та сприяє сталому розвитку організації.

Врахування цих етичних вимог допомагає забезпечити високий стандарт управління ризиками, підвищує довіру зацікавлених сторін та сприяє сталому розвитку організації.

У зв'язку з тим, що проведення оцінки ризиків є одним з найбільш трудомістких і відповідальних кроків, пов'язаних з розробкою стратегії інформаційної безпеки для компанії, вкрай важливо ідентифікувати кожен потенційний ризик. Ризики унікальні для кожної компанії, але кінцева мета одна: захистити дані та знайти найкраще рішення, яке відповідає всім вимогам бізнесу. Корпорація вже провела значну кількість своїх процедур. Однак переважна більшість з них не була задокументована на регулярній основі або взагалі не була задокументована.

Іншими словами, значна частина небезпек не усвідомлювалася, а отже, не враховувалася

2.2 Аналіз впливу етичних питань на прийняття стратегічних рішень у ризик-менеджменті

Оскільки підприємства продовжують працювати в умовах зростаючої конкуренції та невизначеності, що посилюється загрозами для їхньої діяльності, такими як кібератаки, збої в ланцюжках поставок та кліматичні катастрофи, стратегічне управління ризиками стало ключовим фактором забезпечення успіху організації.

Очевидно, що організації повинні бути готові до різних типів стратегічних ризиків, що виникають на їхньому шляху, і мати надійне стратегічне управління ризиками, щоб не тільки зменшити вплив на свою діяльність, але навіть скористатися перевагами контексту та перетворити його на можливість.

Стратегічний ризик - це ймовірність провалу стратегії організації. Це оцінка майбутнього успіху обраної стратегії. Оскільки стратегія - це сукупність чітких рішень, то стратегічний ризик відображає сукупність ризиків, пов'язаних з цими рішеннями.

Стратегічне управління ризиками – це процес розпізнавання ризиків, виявлення їх причин і наслідків та вжиття відповідних заходів для їх пом'якшення. Ризики виникають через внутрішні та зовнішні фактори, такі як виробничі невдачі, економічні зміни, зміни смаків споживачів тощо.

Організації, які не здійснюють належне управління ризиками, стикаються зі значними загрозами. Іноді вони стикаються з екзистенційними загрозами. Kodak був піонером у сфері фотографії (вони фактично подали патент на одну з перших цифрових камер), але вони програли гонку цифрових камер. На піку свого розвитку Blockbuster отримав 6 мільярдів доларів доходу, але у світі залишився лише один магазин! Колись MySpace була однією з домінуючих соціальних мереж, поки не з'явився Facebook.

Смартфони, електронні книги, сервіси каршерінгу, навіть натуральні засоби для чищення – багато з того, що ми, як споживачі, зараз сприймаємо як

належне, колись було сміливим кроком. Але Apple, Amazon, Zipcar і Method не запустили свої продукти, що визначають категорію, відразу.

Ці організації забезпечили свій успіх за допомогою сильної стратегії управління ризиками. Вони знали, як виглядатиме успіх, які фактори можуть призвести до невдачі, чого їм може коштувати невдача і як вони реагуватимуть на перешкоди на своєму шляху.

Управління стратегічними ризиками є важливим видом діяльності для всіх компаній, незалежно від того, чи виводите ви інноваційне рішення на ринок, чи просто намагаєтеся випередити конкурентів.

Розуміння небезпек (якими б незначними вони не були) та їх потенційного впливу (яким би незначним він не був) дає можливість лідерам різних рівнів приймати розумні, обґрунтовані рішення.

Але це легше сказати, ніж зробити. Управління ризиками є динамічним процесом - воно зміщує фокус при зміні внутрішніх і зовнішніх впливів. Це також вимагає об'єднаного мислення та комунікації в організації.

Стратегічний ризик може порушити здатність бізнесу досягати своїх цілей, вириватися на ринок або навіть виживати. Ефективне, результативне управління передає владу в руки лідерів, щоб уникнути потенційних перешкод на шляху до успіху і максимізувати свою ефективність. Принцип ідентифікації стратегічного ризику показаний на рисунку 2.4.

Рис. 2.4 Ідентифікація стратегічного ризику

Інфографіка стратегічних ризиків на рисунку 2.5:

- Регуляторні ризики;
- Конкурентні ризики;
- Економічні ризики;
- Ризики змін;
- Репутаційні ризики;
- Ризики, пов'язані з управлінням;
- Політичні ризики;
- Фінансові ризики;
- Операційні ризики.

Рис. 2.5. Види стратегічних ризиків

За своєю суттю стратегічні ризики впливають на загальну стратегію організації. Іноді його буває важко помітити та впоратися.

Стратегічні рішення у ризик-менеджменті можуть варіюватися в залежності від конкретного контексту, галузі та особливостей організації.

З етичної точки зору, вирішальною характеристикою сучасного управління ризиками є те, яким чином численні ризики, які зачіпають кожного в суспільстві, перетворюються в область прийняття корпоративних рішень і підпорядковуються умовам прийняття рішень на таких вузько економічних підприємствах. Ризики, пов'язані з бізнесом, хвилюють кожного, і все ж у сучасному управлінні ризиками завдання виявлення цих ризиків, прийняття рішення про їх лікування і, можливо, найважливіше - формування профілю ризику, що відображає власні переваги фірми щодо ризику, делегуються суспільством комерційним корпораціям. Рішення з управління ризиками неминуче пов'язані з вибором ризиків, якими потрібно управляти, вибором одних і ігноруванням інших; І засоби, обрані для управління цими ризиками, пов'язані з витратами і вигодами, які розподіляються, часто нерівномірно, між різними групами, на які впливає корпоративна діяльність. Сучасне управління ризиками виникло, зокрема, для того, щоб задовольнити вимогу суспільства про те, щоб бізнес взяв на себе більшу відповідальність за управління ризиками, але така реакція бізнесу має етичні наслідки, оскільки передбачає розподіл відповідальності за управління ризиками між, перш за все, корпораціями та урядом.

Етичні ризики визначаються як дії, процедури, стандарти, політика, а також рішення, які можуть бути реальними або передбачуваними порушенням цінності чи стандарту. Погляд на етику з точки зору ризику – це привабливо для багатьох дослідників, тому що робить етику досить відчутною і практичною. Це також відкриває двері для використання стандартних методологій ризику в етичному контексті.

Сучасне управління ризиками - це особлива недавня історична подія, в якій певні види ризиків розглядаються певним чином певними суб'єктами для

досягнення певних цілей. Немає сумніву, що ризиком слід управляти, але має величезне значення, якими ризиками управляються, ким, якими засобами і на чию користь. У сучасному управлінні ризиками ризики, про які йде мова, є збитками для фірми та її акціонерів, а управління ризиками здійснюється вищими менеджерами, включаючи, в деяких фірмах, головного ризик-менеджера. Стандартні категорії ринкових, кредитних та операційних ризиків сьогодні зазвичай розглядаються традиційним страхуванням, фінансовими інструментами, операційними модифікаціями та структурою капіталу. Мета сучасного управління ризиками полягає в тому, щоб максимізувати вартість фірми шляхом формування профілю ризику таким чином, щоб уникнути або зменшити одні ризики, передати або хеджувати інші, а також зберегти ті, які складають основний бізнес фірми або які не можуть бути уникненні або перенесені. Профіль ризику фірми відображає її апетит або толерантність до ризику таким чином, щоб максимально використовувати її основні компетенції, наявний капітал і загальну стратегію. Незважаючи на те, що ризик-менеджмент в тій чи іншій формі вже давно практикується, його сучасна форма відрізняється системним способом розширення категорій ризиків і розгляду всіх ризиків разом на вищих рівнях управління, а не розгляду окремо в розрізнених підрозділах персоналом нижчої ланки. Цій трансформації сприяли розвиток комп'ютерів та інформаційних технологій, а також теоретичні досягнення у сфері фінансів, які є основою, зокрема, складних фінансових інструментів.

У дослідженнях [40-42] розглядається роль штучного інтелекту (ШІ) у прийнятті стратегічних рішень та його наслідки для менеджерів у цифрову епоху. Оскільки штучний інтелект продовжує трансформувати бізнес-середовище, з'являються можливості для кращого прийняття рішень на основі даних, інновацій та організаційної гнучкості. Однак проблеми, пов'язані з етичними міркуваннями, безпекою та конфіденційністю даних, а також інтеграцією та впровадженням, залишаються. Менеджери повинні адаптуватися, розвиваючи всебічне розуміння застосувань штучного

інтелекту, сприяючи організаційній культурі, готовій до штучного інтелекту, і забезпечуючи дотримання етичних норм і нормативних вимог. У статті також наголошується на необхідності майбутніх досліджень для вивчення нових застосувань штучного інтелекту, галузевих впливів і найкращих практик інтеграції ШІ в процеси прийняття стратегічних рішень, а також вирішення поточних етичних, нормативних та імплементаційних проблем.

Аналіз впливу етичних питань на прийняття стратегічних рішень у ризик-менеджменті важливий для забезпечення не тільки ефективності, але і етичної легітимності дій організації. Нижче наведені ключові аспекти впливу етичних питань на стратегічні рішення в області ризик-менеджменту (табл. 2.1).

Таблиця 2.1

Перелік ключових аспектів впливу етичних питань на стратегічні рішення

Питання	Вплив	Стратегічне рішення
Справедливість та Зрозуміння Ризиків	Етичний обов'язок розуміти ризики і їхні наслідки для всіх зацікавлених сторін	Врахування принципів справедливості при розподілі ризиків і визначення стратегій для зменшення можливих негативних наслідків для всіх стейкхолдерів
Врахування Соціальних та Екологічних Наслідків	Сприяння етичному управлінню ризиками шляхом врахування соціальних та екологічних аспектів рішень	Прийняття стратегій, які враховують соціальні та екологічні наслідки ризиків, і впровадження політик, спрямованих на сталість
Конфіденційність та	Захист конфіденційної	Розробка політик

Питання	Вплив	Стратегічне рішення
Права Людини	інформації та забезпечення прав людини в процесі управління ризиками	конфіденційності та визначення механізмів захисту прав людини при розгляді ризиків та їхніх можливих наслідків
Інтереси Різних Груп	Уважне врахування інтересів різних стейкхолдерів при виявленні та управлінні ризиками	Співпраця з різними групами, врахування їхніх перспектив та пошук компромісів для досягнення загальної етичної легітимності
Прозорість та Відкритість	Відкритість у процесах прийняття рішень та висвітлення ризиків і їхніх наслідків	Розвиток механізмів звітності та взаємодії зі стейкхолдерами для створення довіри та етичної легітимності
Етичні Кодекси та Стандарти	Дотримання етичних кодексів та стандартів у сфері ризик-менеджменту	Розробка та впровадження етичних стандартів, які допомагають оцінювати та керувати ризиками
Визначення Відповідальності	Прийняття відповідальності за наслідки ризиків та прийнятих стратегій	Визначення чіткої системи відповідальності та визначення осіб, відповідальних за управління ризиками
Інклюзивний Діалог	Залучення всіх	Здійснення

Питання	Вплив	Стратегічне рішення
	зацікавлених сторін до діалогу та уважне врахування різних точок зору	консультацій та діалогу зі стейкхолдерами при прийнятті стратегічних рішень щодо ризиків

:

Подальшим розрізненням є класифікація ризиків і небезпек з точки зору ієрархії стратегічного, програмного та операційного рівнів. Ці три рівні необхідно об’єднати. У моделі Стратегія управління ризиками організація керуватиметься зверху та буде вбудована в звичайні робочі процедури та діяльність організації [43]. Рисунок 2.6 ілюструє цей організаційний погляд на класифікацію ризиків.

Рис. 2.6.Класифікація ризиків

Існує метод Кейс-стаді, що ілюструє впровадження ISO 27001 в інформаційно-технологічній компанії [39, 44-45].

Назва компанії скорочена до XYZ, щоб уникнути будь-яких порушень безпеки. Використовуючи програмне забезпечення та послуги, XYZ може як автоматизувати, так і оптимізувати бізнес-процеси на основі даних. Її консалтингові практики є одними з найвідоміших у всьому світі, і вона утримує позицію лідера світового ринку завдяки відомій платформі.

Галузеві експерти XYZ мають всебічні знання про галузь у широкому спектрі компаній і вертикалей. Компанія усвідомлює, наскільки складно може бути впровадити нові системи в існуючий бізнес, і, як наслідок, вона ретельно співпрацює з бізнес-фахівцями та IT-фахівцями клієнтів, щоб допомогти цим клієнтам розпізнати їхні перспективи та цілі. Після цього XYZ формує з ними партнерські відносини з метою надання послуг, що охоплюють весь життєвий цикл проекту. На цій посаді XYZ ефективно керує всіма аспектами проекту, починаючи з реінжинірингу процесу і закінчуючи етапами проектування, розробки та оптимізації системи. XYZ доступний для оцінки потреб організації в управлінні змінами та розробки методу навчання, який буде найбільш ефективним для забезпечення того, щоб співробітники організації повністю прийняли нові процеси та технології. Врешті-решт, компанія переходить до надання цілеспрямованої та довгострокової підтримки виробництву.

XYZ здатний надавати ефективні програмні рішення для комп'ютеризації та вдосконалення бізнес-процедур вчасно та в межах бюджету завдяки унікальному поєднанню ноу-хау, ґрунтовної науки та вирішення проблем. Технологічні експерти компанії мають численні ступені та сертифікати в суміжних галузях, включаючи науку та інженерію. Його Центр рішень був визнаний Європейським Союзом як Науково-інноваційний центр, який успішно отримав ряд дослідницьких грантів від Європейського Союзу. Вчені та інженери галузі розробили низку передових інструментів для вирішення проблем, спеціально адаптованих до повсякденних проблем, з якими стикається компанія. Важливо, що XYZ протестувала та впровадила ці рішення на величезних обсягах точних даних, наданих деякими з найбільших корпорацій, і в результаті компанія досягла значного та помітного збільшення своїх корпоративних прибутків. Це дуже важлива подія.

Корпорація XYZ – це так званий «проектний» бізнес. Технологічні консультанти компанії делегуються для роботи над кожним проектом для своїх клієнтів. Команди змінюються, а учасники додаються до групи або

видаляються з неї залежно від поточної фази проекту та обсягу роботи, яку потрібно виконати. Кількість людей у команді може коливатися від чотирьох до тридцяти.

Єдина у своєму роді інфраструктура, виготовлена за індивідуальним замовленням, розробляється для кожного окремого замовника. Ядром цього зв'язку є всеосяжна база даних вихідного коду. Цей архів файлів коду дозволяє проектам з кількома розробниками підтримувати різні ітерації, централізовану бібліотеку документів, виділену базу даних у програмному забезпеченні для управління проектами, виділені каталоги, ретельні контейнери як для розробки, так і для тестування, нативний додаток Endeavor і диференційований доступ до методу управління часом. Інструменти та засоби, які були описані, забезпечують команду відповідною структурою, яка підтримує, контролює та реалізує проект, а також базу спільних зусиль, метрики та прогнозний аналіз для забезпечення якості.

Висновок до другого розділу. Застосування проаналізованих стандартів ризик-менеджменту на рівні вітчизняних суб’єктів господарювання дає змогу оцінити заходи щодо управління ризиками, виявити слабкі та сильні аспекти корпоративного ризик-менеджменту, зменшити витрати на підготовку відповідних звітів, внести необхідні зміни в організаційну структуру, підвищити ефективність тощо.

Необхідно наголосити на тому, що міжнародний стандарт ISO 31000:2009 активно використовують і при розробленні національних стандартів управління ризиками. Яскравими прикладами можуть слугувати проекти національних стандартів управління ризиками Російської Федерації та Білорусії. Тому, на нашу думку, вітчизняним фахівцям у сфері ризик-менеджменту потрібно скористатися зарубіжним досвідом та розробити вітчизняний стандарт управління ризиками, що ґрунтуватиметься на новітніх досягненнях у сфері ризик-менеджменту у світі.

За свою недовгу історію сучасний ризик-менеджмент зайняв центральне місце в прийнятті бізнес-рішень, особливо у фінансових установах, і зіграв значну роль в останній фінансовій кризі. Хоча багато було написано про технічні проблеми, пов'язані з цією практикою, порівняно мало уваги було приділено етичним питанням. Цей розділ принаймні розпочинає цей вкрай необхідний аналіз, піднімаючи питання про етичні наслідки прийняття управління ризиками для інших груп, крім акціонерів, а також для питань корпоративної підзвітності, відповідальності та регулювання. Нарешті, певна увага приділяється етичним питанням при застосуванні конкретних методів управління ризиками.

РОЗДІЛ 3
РОЗРОБЛЕННЯ МЕТОДИКИ ЕТИЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ І РИЗИКАМИ

3.1 Визначення параметрів та інструментів для оцінки ризиків із залученням етичного аналізу

Етичні аспекти, як зазначає більшість фахівців, мають вирішальне значення в аналізі ризику, але ними часто нехтують. Однією з причин цього є відсутність операційних інструментів етичного аналізу ризиків [50-54].

ІТ-фахівці покладаються на всілякі контрзаходи, включаючи звичні технічні механізми контролю доступу (такі як брандмауери, криптографічні алгоритми та антивірусне програмне забезпечення), комп'ютерне право та комп'ютерний аудит, але організації все одно страждають від негативних наслідків. Чому це так? Десь щось не так, але що це таке і де виникає несправність? Можливо, наше розуміння ризику потребує оновлення; удосконалення освіти в галузі науки і техніки; Необхідно впроваджувати ефективні моделі прийняття рішень, оскільки ті, що використовуються в даний час, є менш ефективними; Інтернет-спільнота повинна приділяти етичну увагу розробці та використанню продуктів і послуг у сфері інформаційно-комунікаційних технологій (ІКТ).

Проблеми безпеки – як технічного, так і нетехнічного характеру – кореняться в людських помилках, від яких ніхто не застрахований. Де б і коли не була вразливість, існує загроза, готова її використати. Ризик виникає, коли загроза реально здійснюється.

Щоб зменшити ризик (тобто пошкодження, втрату або знищення того, що людина хоче захистити), необхідно мати справу з вразливістю та ідентифікувати загрозу. Можна сказати, що ризик є функцією вразливості та загрози

$$R = f(v, t)\ , \tag{1}$$

де R – величина ризику;

v – величина вразливості;

t – величина загрози

А схильність до ризику є функцією ймовірності (ймовірності виникнення ризику) та збитку (технічного, фінансового та етичного характеру)

$$r = f(p, d), \tag{2}$$

де r – схильність до ризику;

p – ймовірності виникнення ризику;

d – збиток (технічного, фінансового та етичного характеру)

Останнім часом стверджується, що люди вже давно перебувають під впливом неправильного тлумачення ризику [43]. Цей ризик сприймається як технічна проблема і вимірюється в економічних і юридичних термінах, але насправді він також є управлінським інтересом і повинен оцінюватися як в соціально-технічному, так і в юридично-фінансовому плані. Це помилка, і технічні, економічні та соціальні аспекти повинні бути визнані, щоб отримати цілісне уявлення.

Під подвійним впливом неправильного тлумачення ризику та недосконалої освіти в галузі науки та техніки особи, які приймають рішення, незмінно зосереджуються лише на технічних, економічних та правових змінних, залишаючи поза увагою етичні міркування. Результуючий аналіз рішень, що складається з аналізу витрат і вигод і ризиків, є недосконалим. Для

усунення недоліку, або для оцінки соціальної прийнятності та виявлення можливого негативного впливу етичних наслідків, Етичний рух у кіберпросторі (Етичний рух), який відстоює Товариство комп'ютерної етики (iEthics),6 попереджає про новий тип ризику (етичний ризик), нову категорію антиризикового механізму та новий інструмент етичного аналізу (Етична матриця). Він також пропонує додати етичний аналіз до набору інструментів прийняття рішень і використовувати метод етичної матриці для етичного аналізу.

У ризик-менеджменті використовують етичну матрицю [46-47], яка допомагає визначити, які ризики є етично прийнятними, а які - ні. Етична матриця включає в себе такі критерії, як право, справедливість, користь, довіра, повага та інші.

Зразок Етичної матриці показаний з табл. 1.1. (рис. 3.1)

Загальна серйозність ризику				
Втрати	ВИСОКІ	Посередня	Висока	Критична
	ПОСЕРЕДНІ	Низька	Посередня	Висока
	НИЗЬКІ	Відсутня	Низька	Посередня
		НИЗЬКА	ПОСЕРЕДНЯ	ВИСОКА
	Імовірність			

Рис. 3.1. Матриця ризиків

Далі для прикладу наведено застосування матриці для оцінки ризику в аеропорту (рис. 3.2)

Рис. 3.2. Матриця оцінювання ризиків у аеропорту

Оцінка ризиків з використанням етичного аналізу включає в себе врахування етичних аспектів та норм при визначенні потенційних наслідків різних сценаріїв. У таблиці 3.1 подано параметри та інструменти, які можна використовувати для оцінки ризиків з етичним аналізом:

Таблиця 3.1

Параметри для оцінки ризиків

Параметр	Питання для оцінки
Достовірність	Як можливий ризик впливає на достовірність організації та її стосунків із зацікавленими сторонами?
Справедливість	Як можливий ризик впливає на справедливість розподілу витрат чи негараздів між різними групами?
Захист прав людини	Як можливий ризик впливає на захист прав та інтересів людини?
Соціальна відповідальність	Як можливий ризик впливає на відповідальність організації перед

Параметр	Питання для оцінки
	суспільством?
Екологічна стійкість	Як можливий ризик впливає на стійкість навколишнього середовища?

Інструменти для оцінки ризиків з етичним аналізом показані в таблиці 3.2.

Таблиця 3.2

Інструменти для оцінки ризиків

Інструмент	Опис
Ethisphere Framework	Фреймворк Ethisphere надає інструменти для оцінки етичної культури організації та виявлення потенційних етичних ризиків
Етичні картографії ризиків	Розробка картографій ризиків, де окремі області відображають можливі етичні питання та їхні можливі наслідки
Аудит етичного ризику	Проведення аудиту, спрямованого на виявлення етичних ризиків в різних сферах діяльності організації
Етичний імпакт-асесмент (EIA)	Здійснення оцінки впливу прийнятих стратегій та рішень на етичний статус організації
Етичні кейси та сценарії	Розробка та аналіз сценаріїв для ідентифікації можливих етичних

	ризиків та пошуку шляхів їх управління
Аналіз ризиків в контексті етичних кодексів	Застосування аналізу ризиків, орієнтованого на перевірку відповідності дій етичним кодексам та стандартам

Використання цих параметрів та інструментів сприяє створенню комплексного підходу до оцінки ризиків, враховуючи етичні аспекти і визначаючи стратегії управління ризиками, які дозволяють забезпечити етичну легітимність дій організації [48-51].

Для оцінки та пріоритезації ризику можуть використовуватися різні методи. Залежно від того, наскільки добре відомий ризик, і якщо його можна своєчасно оцінити та розставити пріоритети, можна зменшити можливі негативні наслідки або збільшити можливі позитивні ефекти та скористатися можливостями [52] . Кількісний аналіз ризику намагається присвоїти об'єктивні числові або вимірювані значення незалежно від компонентів оцінки ризику та оцінки потенційного збитку. І навпаки, якісний аналіз ризиків ґрунтується на сценаріях [53].

Метою якісного аналізу ризику є виявлення ризику, який потребує детального аналізу та необхідних заходів контролю та дій, заснованих на впливі ризику та впливі на цілі [52]. У якісному аналізі ризику добре відомі і легко застосовуються до ризику два простих методи [54].

Keep It Super Simple (KISS) – цей метод можна використовувати на вузьких або невеликих проектах, де слід уникати непотрібної складності, а оцінка може бути легко зроблена командами, яким не вистачає зрілості в оцінці ризику. Ця одновимірна методика передбачає оцінку ризику за базовою шкалою, наприклад, дуже високий/високий/середній/низький/дуже.

Ймовірність/вплив – цей метод може бути використаний для вирішення більших, складніших питань з багатосторонніми командами, які мають досвід

оцінки ризиків. Цей двовимірний метод використовується для оцінки ймовірності та впливу. Імовірність - це ймовірність того, що ризик виникне. Вплив - це наслідок або наслідок ризику, який зазвичай пов'язаний з впливом на графік, вартість, обсяг і якість. Оцінюйте ймовірність і вплив, використовуючи такі шкали, як від 1 до 10 або від 1 до 5, де показник ризику дорівнює ймовірності, помноженій на вплив (формула 1).

Якісний аналіз ризиків, як правило, може бути проведений по всіх підприємницьких ризиках. Якісний підхід використовується для швидкого виявлення зон ризику, пов'язаних з нормальними функціями бізнесу. Оцінка може оцінити, чи пов'язані занепокоєння людей щодо їхньої роботи з цими зонами ризику. Потім кількісний підхід допомагає за відповідними сценаріями ризику, щоб запропонувати більш детальну інформацію для прийняття рішень [55]. Перед прийняттям критичних рішень або виконанням складних завдань кількісний аналіз ризиків дає більше об'єктивної інформації та точних даних, ніж якісний аналіз. Хоча кількісний аналіз є більш об'єктивним, слід зазначити, що все ж таки існує оцінка або умовивід. Мудрі ризик-менеджери враховують інші фактори в процесі прийняття рішень [56].

Незважаючи на те, що якісний аналіз ризиків є першим вибором з точки зору простоти застосування, кількісний аналіз ризику може бути необхідним. Після якісного аналізу може бути застосований і кількісний аналіз. Однак, якщо якісних результатів аналізу достатньо, немає необхідності проводити кількісний аналіз кожного ризику.

Кількісний аналіз ризику - це ще один аналіз ризику з високим пріоритетом та/або високим впливом, де дається числовий або кількісний рейтинг для розробки ймовірнісної оцінки питань, пов'язаних з бізнесом. Крім того, кількісний аналіз ризиків для всіх проектів або проблем/процесів, що експлуатуються з використанням підходу до управління проектами, має більш обмежене застосування, залежно від типу проекту, ризику проекту та доступності даних, які будуть використовуватися для кількісного аналізу [57].

Мета кількісного аналізу ризику полягає в тому, щоб перевести

ймовірність і вплив ризику в вимірювану величину. Особливості кількісного аналізу полягають у наступному:

- кількісно оцінює можливі результати для бізнес-проблем та оцінює ймовірність досягнення конкретних бізнес-цілей;
- забезпечує кількісний підхід до прийняття рішень в умовах невизначеності;
- створює реалістичні та досяжні цільові показники вартості, графіка або обсягу.

Можливість використання кількісного аналізу ризиків розглядають для

бізнес-ситуації, які потребують планування графіка та бюджетного контролю, великих, складних питань/проектів, які вимагають прийняття рішень «за» / «ні», бізнес-процесів або питань, в яких вище керівництво хоче отримати більш детальну інформацію про ймовірність завершення в межах графіка і в рамках бюджету [58].

До переваг використання кількісного аналізу ризиків можна віднести:

- об'єктивність в оцінці;
- потужний інструмент продажу керівництву;
- пряма проекція витрат і вигод;
- гнучкість для задоволення потреб конкретних ситуацій;
- гнучкість відповідно до потреб конкретних галузей;
- набагато менше схильні викликати розбіжності під час управлінської перевірки;
- аналіз часто виводиться з якихось незаперечних фактів.

Найпоширеніша проблема кількісної оцінки полягає в тому, що недостатньо даних для аналізу.

Для проведення кількісного аналізу ризиків по бізнес-процесу або проекту необхідні якісні дані, чіткий бізнес-план, грамотно розроблена модель проекту і пріоритезований перелік бізнес/проектних ризиків. Кількісна оцінка ризику ґрунтується на реалістичних і вимірюваних даних для розрахунку значень впливу, які ризик створить із ймовірністю виникнення. Ця оцінка

фокусується на математичних і статистичних основах і може «виражати значення ризику в грошовому вираженні, що робить її результати корисними поза контекстом оцінки (втрати грошей зрозумілі для будь-якої бізнес-одиниці) [59]. Найбільш поширеною проблемою кількісної оцінки є те, що недостатньо даних для аналізу. Також можуть виникнути труднощі з розкриттям предмета оцінювання за допомогою числових значень або занадто велика кількість відповідних змінних. Це технічно ускладнює аналіз ризиків.

Існує кілька інструментів і методів, які можуть бути використані в кількісному аналізі ризиків. Ці інструменти та методи включають:

- евристичні методи – засновані на досвіді або експертах методи оцінки непередбачених обставин;
- триточкова оцінка – техніка, яка використовує оптимістичні, найбільш ймовірні та песимістичні значення для визначення найкращої оцінки;
- аналіз дерева рішень – діаграма, яка показує наслідки вибору різних альтернатив;
- очікувана грошова вартість – метод, який використовується для встановлення резервів на випадок непередбачених обставин для бюджету та графіка проекту або бізнес-процесу;
- аналіз монте-карло – метод, який використовує оптимістичні, найбільш ймовірні та песимістичні оцінки для визначення вартості бізнесу та термінів завершення проекту;
- аналіз чутливості – техніка, яка використовується для визначення ризику, який має найбільший вплив на проєкт або бізнес-процес;
- аналіз дерева несправностей та аналіз режимів і наслідків відмов – аналіз структурованої діаграми, яка визначає елементи, які можуть спричинити відмову системи.

Існують також деякі базові (цільові, розрахункові або розрахункові) значення, що використовуються при кількісній оцінці ризику. Очікуваний одноразовий збиток (SLE) являє собою гроші або вартість, які очікуються

втратити, якщо інцидент станеться один раз, а річний коефіцієнт виникнення (ARO) - це те, скільки разів за річний інтервал очікується інцидент. Очікуваний річний збиток (ALE) може бути використаний для обґрунтування витрат на застосування контрзаходів для захисту активу або процесу. Очікується, що ці гроші/вартість будуть втрачені через рік, враховуючи SLE та ARO. Цю величину можна обчислити, помноживши СЧВ на ARO. Для кількісної оцінки ризику це величина ризику.

Використання обох підходів може підвищити ефективність процесу та допомогти досягти бажаного рівня безпеки.

Спираючись на фактичні та вимірювані дані, основними перевагами кількісної оцінки ризику є представлення дуже точних результатів про цінність ризику та максимальні інвестиції, які зроблять лікування ризиків вигідним та прибутковим для організації. Для кількісного аналізу витрат і вигод ALE - це розрахунок, який допомагає організації визначити очікувані грошові втрати активу або інвестиції через пов'язаний з цим ризик протягом одного року.

Наприклад, розрахунок ALE для інвестицій в систему віртуалізації включає наступне:

Вартість апаратного забезпечення системи віртуалізації: 1 мільйон доларів США (SLE для апаратного забезпечення)

Вартість програмного забезпечення для управління системою віртуалізації: 250 000 доларів США (SLE для SW)

Статистика постачальників повідомляє, що катастрофічний збій системи (через програмне або апаратне забезпечення) відбувається один раз на 10 років (ARO = 1/10 = 0,1)

ALE для HW = 1 млн * 1 = 100 000 доларів США

ALE для SW = 250 тисяч * 0,1 = 25 000 доларів США

У цьому випадку організація має щорічний ризик зазнати збитків у розмірі 100 000 доларів США на апаратне забезпечення або 25 000 доларів США на програмне забезпечення окремо у разі втрати системи віртуалізації.

Будь-який реалізований контроль (наприклад, резервне копіювання, аварійне відновлення, система відмовостійкості), який коштує менше цих значень, буде прибутковим.

Деяка оцінка ризику вимагає складних параметрів. Більше прикладів можна навести відповідно до наступного покрокового розподілу кількісного аналізу ризиків:

1) Проведіть оцінку ризиків та дослідження вразливості для визначення факторів ризику.

2) Визначте коефіцієнт експозиції, який є відсотком втрати активів, спричиненої виявленою загрозою.

3) Виходячи з факторів ризику, визначених у вартості матеріальних або нематеріальних активів, що перебувають під ризиком, визначають СЧВ, який дорівнює вартості активу, помноженій на коефіцієнт експозиції.

4) Оцініть історичне підґрунтя та бізнес-культуру закладу з точки зору звітності про інциденти та втрати безпеки (коригувальний коефіцієнт).

5) Оцініть ARO для кожного фактора ризику.

6) Визначте контрзаходи, необхідні для подолання кожного фактора ризику.

7) Додайте рейтингове число від 10 до 10 для кількісної оцінки серйозності (де <> є найсерйознішим) як поправочний коефіцієнт розміру для оцінки ризику, отриманої з профілю ризику компанії.

8) Визначте ALE для кожного фактора ризику. Зауважимо, що ARO для ALE після реалізації контрзаходів не завжди може дорівнювати нулю. ALE (виправлений) дорівнює ALE (таблиця), помноженому на коригувальний коефіцієнт, помножене на корекцію розміру.

9) Розрахуйте відповідний аналіз витрат і вигод, знайшовши відмінності до і після впровадження контрзаходів для ЛЄ.

10) Визначте рентабельність інвестицій (ROI) на основі аналізу витрат і вигод з використанням внутрішньої норми прибутковості (IRR).

11) Представте керівництву для ознайомлення короткий виклад

результатів.

Використання обох підходів може підвищити ефективність процесу та допомогти досягти бажаного рівня безпеки. У процесі оцінки ризиків відносно легко визначити, кількісний чи якісний підхід. Якісна оцінка ризиків швидко реалізується завдяки відсутності математичної залежності та вимірювань і може бути виконана легко. Організації також отримують вигоду від співробітників, які мають досвід роботи з активами/процесами; Однак вони також можуть привнести упередженість у визначення ймовірності та впливу. Загалом, поєднання якісних та кількісних підходів з хорошим плануванням оцінки та відповідним моделюванням може бути найкращою альтернативою для процесу оцінки ризиків

Існує багато сайтів з готовими шаблонами оцінювання ризиків. Один із них показаний на рисунку 3.3.

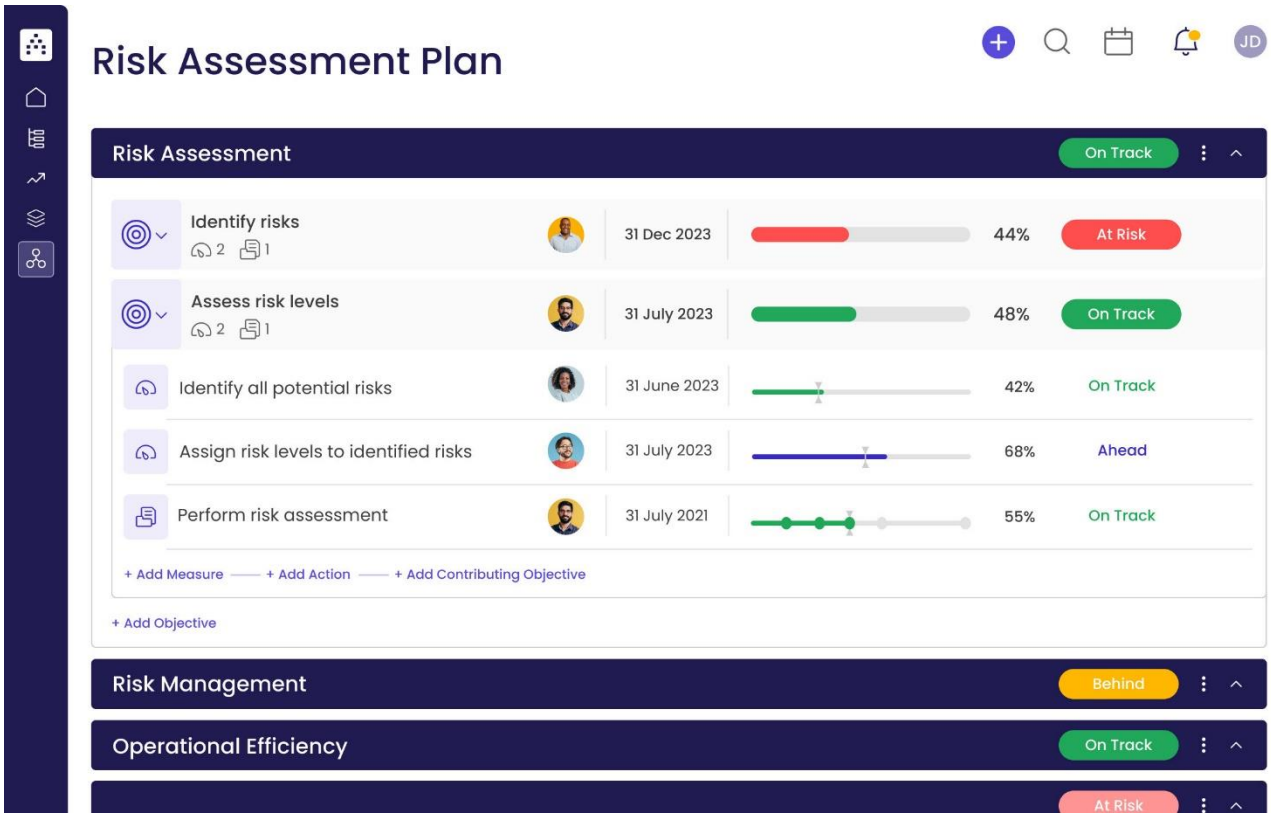

Рис. 3.3. Шаблон плану оцінювання ризиків

План оцінки ризиків окреслює кроки для оцінки та управління ризиками, з якими може зіткнутися організація. Він допомагає організаціям виявляти

потенційні ризики, оцінювати їх ймовірність і серйозність, а також розробляти стратегії для пом'якшення або усунення цих ризиків. План повинен бути адаптований до конкретних цілей, ресурсів і можливостей організації, щоб гарантувати, що він відповідає її потребам.

Шаблон Плану оцінки ризиків розроблений, щоб допомогти організаціям будь-якого розміру та галузі створити план оцінки та управління своїми ризиками. Він забезпечує основу для виявлення потенційних ризиків, оцінки їх рівнів і розробки стратегій їх пом'якшення або усунення. Шаблон простий у використанні та може бути налаштований відповідно до індивідуальних потреб організації.

Для оцінки ризиків можна використовувати Python і його багатофункціональні бібліотеки, які дозволяють створювати власні програми прогнозування та попередження інцидентів і ризиків. Розроблені власні програмні модулі є набагато оперативніші за стандартні, вони дозволяють враховувати сучасні зміни інформаційних технологій, новітні хакерські атаки та своєчасно на них реагувати, планувати превентивні заходи. Існує декілька бібліотек, які можна використовувати для аналізу ризиків та моделювання складних сценаріїв. Ось кілька з них:

- scikit-learn: це потужна бібліотека для машинного навчання, яка містить різноманітні алгоритми для класифікації, регресії, кластеризації та інші. Може бути використана для аналізу даних та оцінки ризиків за допомогою методів машинного навчання (рис. 3.4)

```
from sklearn import preprocessing
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier

# Ваш код для використання scikit-learn
```

Рис. 3.4 Код підключення бібліотеки для оцінки ризиків

- pandas: Це бібліотека для обробки та аналізу даних. З допомогою

pandas можна легко виконувати завдання зі зчитування, обробки та аналізу даних для оцінки ризиків (рис. 3.5).

-

```
import pandas as pd

# Ваш код для використання pandas
```

Рис. 3.5. Код підключення бібліотеки для аналізу ризиків

- numpy: Бібліотека для наукових обчислень, яка надає функції для роботи з числовими даними. Може бути корисною для обчислення статистичних метрик та в інших аспектах аналізу ризиків (рис. 3.6)

-

```
import numpy as np

# Ваш код для використання numpy
```

Рис. 3.6. Код підключення бібліотеки для обчислення статистичних метрик

- matplotlib та seaborn: Ці бібліотеки дозволяють вам візуалізувати дані, що може бути корисним при представленні результатів аналізу ризиків (рис.3.7).

```
import matplotlib.pyplot as plt
import seaborn as sns

# Ваш код для використання matplotlib та seaborn
```

Рис. 3.7 Код підключення бібліотеки для візуалізації аналізу ризиків

Загальний лістинг коду для збору, аналізу та оцінки інцидентів і ризиків на основі машинного навчання на навчальному наборі даних та оцінки якості

на контрольному наборі даних з виводом результатів показний на рисунку 3.8.

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
from sklearn.metrics import classification_report, confusion_matrix
import matplotlib.pyplot as plt
import seaborn as sns

# Зчитування даних
data = pd.read_csv('your_data.csv')

# Перегляд перших декількох рядків даних
print(data.head())

# Розділення даних на навчальний та тестовий набори
X = data.drop('target_column', axis=1)  # Припускається, що 'target_colu
y = data['target_column']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2

# Навчання моделі
model = RandomForestClassifier()
model.fit(X_train, y_train)

# Прогнозування на тестовому наборі
y_pred = model.predict(X_test)

# Виведення звіту про класифікацію та матриці плутанини
print(classification_report(y_test, y_pred))
print(confusion_matrix(y_test, y_pred))

# Візуалізація даних
sns.countplot(x='target_column', data=data)
plt.title('Distribution of Target Variable')
plt.show()

# Візуалізація важливості ознак у моделі
feature_importances = pd.Series(model.feature_importances_, index=X.col
feature_importances.nlargest(10).plot(kind='barh')
plt.title('Top 10 Feature Importances')
plt.show()
```

Рис. 3.8. Лістинг загального коду моделі

Цей код демонструє основні етапи роботи з даними, включаючи зчитування, розділення на навчальний та тестовий набори, навчання моделі (у

цьому випадку RandomForestClassifier) і виведення звітів та візуалізацій. При цьому необхідно пам’ятати, що потрібно адаптувати його до конкретного контексту та завдань проекту конкретної організації.

3.2 Розроблення методики етичного управління інформаційними інцидентами і ризиками

Розробка методики етичного управління інформаційними інцидентами і ризиками передбачає визначення принципів та практик, які сприятимуть ефективному та етичному вирішенню проблем в цій області. Нижче наведена загальна методика, яку можна використовувати для цього. Розроблений алгоритм методики показаний на рисунку 3.9.

Рис. 3.9. Алгоритм методики етичного управління інформаційними інцидентами і ризиками

Крок 1: Визначення етичних засад.

Залучення стейкхолдерів: залучення всіх зацікавлених сторін для визначення основних цінностей та етичних принципів, які повинні бути

враховані при управлінні інформаційними ризиками.

Формулювання етичних правил: розробка конкретних етичних правил та стандартів, які визначають допустимі та недопустимі дії при виявленні та управлінні інформаційними інцидентами.

Крок 2: Створення комплексної системи управління ризиками.

Ідентифікація ризиків: визначення можливих інформаційних ризиків, їхніх джерел та потенційних наслідків.

Оцінка ризиків: визначення ймовірності та впливу інформаційних ризиків на організацію та етичні аспекти цього впливу.

Визначення заходів зменшення ризиків: розробка стратегій та заходів для зменшення інформаційних ризиків та їхніх етичних наслідків.

Крок 3: Розробка системи виявлення та реагування на інциденти.

Створення системи виявлення: розробка механізмів для швидкого та ефективного виявлення інформаційних інцидентів та порушень етичних стандартів.

Розробка етичних процедур реагування: визначення етичних принципів та процедур для реагування на інформаційні інциденти, включаючи взаємодію зі стейкхолдерами та публічною інформацією.

Крок 4: Забезпечення прозорості та комунікації.

Створення культури прозорості: формування культури, де прозорість та відкритість є ключовими принципами в управлінні інформаційними ризиками та інцидентами.

Етична комунікація: розробка стратегій комунікації, спрямованих на забезпечення етичного обговорення інформаційних інцидентів та ризиків як внутрішньо, так і зовнішньо.

Крок 5: Постійне підвищення свідомості та навчання.

Навчання персоналу: організація регулярних тренінгів та навчань щодо етичних аспектів управління інформаційними ризиками.

Аналіз етичних сценаріїв: здійснення аналізу та обговорення етичних сценаріїв, що допомагає співробітникам розуміти та вирішувати етичні

дилеми.

Крок 6: Аудит та постійне вдосконалення.

Етичний аудит: проведення етичних аудитів для оцінки ефективності етичного управління інформаційними ризиками та інцидентами.

Вдосконалення процесів: постійне вдосконалення системи управління інформаційними ризиками на основі результатів аудитів та вивчення етичних досвідів.

Розроблена методика етичного управління інформаційними інцидентами і ризиками має за мету забезпечити кілька ключових результатів, спрямованих на етичний та відповідальний підхід до управління інцидентами та ризиками в інформаційній сфері.

Ця методика спрямована на створення етичної культури в управлінні інформаційними ризиками та інцидентами, що дозволяє забезпечити ефективне та етичне вирішення виникаючих проблем.

3.3 Розроблення пропозицій та рекомендацій застосування методики етичного управління інформаційними інцидентами і ризиками

Пропозиції та рекомендації для застосування методики етичного управління інформаційними інцидентами і ризиками можуть бути спрямовані на створення етичної культури, визначення процесів та засобів для ефективного вирішення етичних дилем, а також на постійне вдосконалення системи управління. Ось деякі пропозиції та рекомендації:

Створення комітету етики: сформуйте спеціальний комітет з представників різних відділів для розгляду етичних аспектів інформаційних інцидентів і ризиків. Цей комітет буде відповідальний за формулювання етичних стандартів та прийняття рішень в етичних ситуаціях.

Тренінг та навчання: організуйте регулярні тренінги для персоналу щодо етичних аспектів управління інформаційними ризиками. Навчання може

включати аналіз етичних сценаріїв та ділитися кращими практиками.

Формулювання етичних правил: розробіть чіткі та конкретні етичні правила, які визначають допустимі та недопустимі дії у випадках інформаційних інцидентів. Поширюйте ці правила серед всього персоналу.

Етична свідомість: створіть свідомість про етичні аспекти в усіх процесах управління інформаційними ризиками. Включіть етичні питання у регулярні обговорення та засідання.

Створення легкодоступної звітності: розробіть простий та доступний механізм для співробітників для звітності про потенційні етичні порушення чи інциденти. Забезпечте конфіденційність для тих, хто надає інформацію.

Етичний аудит: проводьте регулярні етичні аудити для оцінки ефективності системи управління інформаційними ризиками. Визначайте слабкі місця та вживайте заходи для їх вдосконалення.

Взаємодія із стейкхолдерами: залучайте стейкхолдерів до обговорень та прийняття стратегій управління інформаційними ризиками. Враховуйте їхні думки та інтереси при прийнятті рішень.

Забезпечення прозорості: забезпечте прозорість у процесах управління інформаційними ризиками, висвітлюючи не тільки успіхи, а й промахи. Це допомагає збудувати довіру серед співробітників та стейкхолдерів.

Збір та аналіз даних: збирайте та аналізуйте дані щодо етичних аспектів інформаційних інцидентів. Це допоможе вам розуміти та вдосконалювати систему управління на основі реальних випадків.

Постійне вдосконалення: впроваджуйте постійні зміни та вдосконалення в систему етичного управління, враховуючи зміни в інформаційному середовищі та нові етичні виклики.

Нижче відпрацьовані кілька додаткових порад щодо зменшення ризику етики та комплаєнсу:

1) поговоріть про важливість етики.

2) належним чином інформуйте співробітників про проблеми, які на них впливають.

3) виконуйте обіцянки та зобов’язання перед співробітниками та зацікавленими сторонами.

4) визнайте та винагороджуйте етичну поведінку.

5) притягуйте до відповідальності тих, хто порушує стандарти, особливо лідерів.

Ці пропозиції та рекомендації можуть бути адаптовані до конкретних потреб та характеру організації. Важливо постійно вдосконалювати систему, враховуючи нові технології, законодавчі зміни та етичні вимоги.

Втілення визначених пропозицій має бути зроблено в корпоративні етичні кодекси організацій [50-63], що дозволить зменшити або навіть і попередити інформаційні інциденти і ризики. Корпоративним кодексом компанії називають повний перелік корпоративних правил, загальних цілей і цінностей. Створення й впровадження етичного кодексу робить поводження людей усередині організації передбачуваним, знижує рівень конфліктності, забезпечує погодженість роботи всіх підрозділів, дає змогу компанії загалом швидко й злагоджено реагувати на будь-які інциденти і ризики інформаційної безпеки.

Висновок до третього розділу. У процесі дослідження було визначено ключові параметри, які враховують етичні аспекти при оцінці ризиків. Розглянуті інструменти дозволили ретельно врахувати етичні принципи під час аналізу та оцінки інформаційних ризиків. Розглянуті ключові аспекти, пов'язані із визначенням параметрів та інструментів для оцінки ризиків з використанням етичного аналізу дозволили розробити методику етичного управління інформаційними інцидентами і ризиками, а також відпрацювати пропозиції та рекомендації для її застосування.

Методика етичного управління інформаційними інцидентами і ризиками спрямована на забезпечення високого рівня відповідальності та етичності у діяльності з управління ризиками. Вона враховує прозорість, конфіденційність, справедливість та інші етичні принципи для забезпечення

ефективного виявлення, реагування та відновлення після інцидентів.

Пропозиції та рекомендації щодо застосування розробленої методики дозволять впроваджувати етичні принципи в практичну діяльність при управлінні інформаційними ризиками. Це сприятиме збереженню довіри стейкхолдерів, зменшенню можливих збитків від інцидентів та формуванню сталої репутації організації в сфері інформаційної безпеки.

В цілому, методик та пропозиції надають концептуальний та практичний внесок у сфері управління інформаційними ризиками, демонструють значущість етичного підходу у цьому процесі та пропонують конкретні інструменти для ефективного впровадження етичних стандартів.

ВИСНОВКИ

Магістерська робота присвячена істотним аспектам етичного управління інформаційними інцидентами та ризиками в контексті кібербезпеки. Загальною метою роботи є підвищення рівня етичності та відповідальності у сфері управління інформаційними інцидентами і ризиками.

У першому розділі були визначені та досліджені етичні принципи управління інформаційними інцидентами, а також проведено аналіз ризиків і етичних конфліктів в управлінні кібербезпекою. Висвітлення цих аспектів дозволило визначити важливі питання, пов'язані із забезпеченням етичного та відповідального управління інформаційними ризиками.

У другому розділі розглянуто етичні вимоги до ризик-менеджменту та проаналізовано вплив етичних питань на прийняття стратегічних рішень у ризик-менеджменті. Висвітлення цих аспектів вказує на значущість етики у вирішенні ризикованих ситуацій та управлінні ними. Застосування проаналізованих стандартів ризик-менеджменту на рівні вітчизняних суб’єктів господарювання дає змогу оцінити заходи щодо управління ризиками, виявити слабкі та сильні аспекти корпоративного ризик-менеджменту, зменшити витрати на підготовку відповідних звітів, внести необхідні зміни в організаційну структуру, підвищити ефективність тощо

У третьому розділі було проведено визначення параметрів та інструментів для оцінки ризиків з використанням етичного аналізу. Проаналізовані в попередніх розділах основи етичного управління інцидентами і ризиками та теоретичні основи ризик-менеджменту дали можливість розробити методику етичного управління інформаційними інцидентами і ризиками, а також відпрацювати пропозиції та рекомендації для її застосування. Це спрямовано на забезпечення етичних стандартів у виявленні, реагуванні та відновленні після інцидентів, що допомагає зберегти довіру стейкхолдерів та покращити загальну ефективність управління ризиками.

Проведений аналіз та розробка методики внесли вагомий внесок у розуміння та практичне застосування етичних принципів в цій сфері, що є ключовим чинником для забезпечення сталості та успішності організацій в умовах постійно зростаючих інформаційних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Флоріді Л. Про людську гідність як основу права на приватність. *Philos. Technol*. 29(4), с. 307–312. 2016. URL: https://doi.org/10.1007/s13347-016-0220-8 (дата звернення: 03.09.2023).

2. Cekerevac Z.; Dvorak Z.; Prigoda L.; Cekerevac P. Hacking, protection and the consequences of hacking. *Komunikácie*, 2018, Vol 20. Issue 2. p. 83. URL: https://doi.org/10.26552/com.c.2018.2.83-87.

3. Микитюк О.А. Конфлікт в організації. *Сучасні проблеми управління людськими ресурсами.* URL: https://cyberleninka.ru/article/v/ konflikty- v-organizatsii-2 с. 83 (дата звернення: 03.09.2023).

4. Ємільянов С.М. Управління конфліктами в організації: підручник для вищих навчальних закладів URL: http://studentam. net.ua/content/ view/4095/86/ (дата звернення: 22.09.2023).

5. Дойч М. Вирішення конфлікту. Конструктивні та деструктивні процеси. *Соціально-політичний журнал*. 1997. No1. С. 202-212.

6. Вінер С. Роль менеджера в процесі управління конфліктами. URL: http://buklib.net /component/ option,com_ jbook/task,view/Itemid,36/catid,136/id,4195/(дата звернення: 13.09.2023).

7. Скородумова Э. З. Конструктивне управління конфліктами в організації як психологічний феномен. *Науково-методичний електроний журнал «Концепт».* 2015. Т. 10. С. 261–265. URL: http://e-koncept.ru/2015/95096.htm. (дата звернення: 01.09.2023).

8. Ковальчук Г., Подольчак Н. Місце та види управлінських конфліктів в системі менеджменту підприємства. *Менеджмент та підприємництво в Україні: Етапи становлення та проблеми розвитку*. 2012. No748. С. 88-95.

9. Діловий етикет в менеджменті та в бізнесі. URL: http://stud24.ru/management/dlovij-etiket-v-menedzhment-ta/506567-2057609-

page1.html (дата звернення: 17.10.2023).

10. Воронкова В., Беліченко А., Мельник В., Ажажа М. Етика ділового спілкування. Львів: Магнолія, 2006. 2009. 312 с.

11. Гришова І., Шабатура Т. Соціальні інвестиції як інструмент реалізації соціально орієнтованого бізнесу. *Вісник Сумськогонаціонального аграрного університету. Серія «Економіка і менеджмент»*. 2014. 4. С. 183–187.

12. Кульчицька А. Г. *Роль менеджера в процесі управління конфліктами*. Матеріали міжвузівської наук.-практ. конф., присвяченої Дню науки. ЖДТУ, 2012. Т.2. С. 318-319.

13. Лупинос І.В. Особливості управління конфліктами в сучасній організації. *Економічний форум*. №1. 178-182. 2019. URL: https://doi.org/10.36910/6765-2308-8559-2019-4-28.

14. Малік, Дж., Ахунзада А., Бібі І., Імран М., Мусаддік А., Кім С. В. 2020. Гібридне глибоке навчання: ефективний механізм виявлення розвідки та спостереження в SDN. *IEEE Access* 8: 134695–134706. URL: https://doi.org/10.1109/ACCESS.2020.3009849.

15. Фріха К., Хван Дж., Ларс М., Робін М.. Управління витоками даних: інтегрована модель ризиків. Інформація та управління 58 (1): 103392. 2021. URL: https://doi.org/10.1016/j.im.2020.103392.

16. Oliveira N., Praca I., Maia E., Sousa O. Intelligent cyber attack detection and classification for network-based intrusion detection systems. *Applied Sciences—Basel* 11 (4). 2021. URL: https://doi.org/10.3390/app11041674.

17. Banja J, Sumler M. Overriding advance directives: a 20-year legal and ethicaloverview. *J Health Care Risk Manag*. 2019;39(2). pp. 11-18.

18. Swisher K. Developing an ethical model for risk management. *PerspectHealthc Risk Manage*. 1991;11(4). pp. 11-18.

19. Ardichvili A., Mitchell J. A., Jondle D. Characteristics of ethical business cultures. *Journal of business ethics*. 2009. Т. 85. С. 445-451.

20. Freeman R. E., Gilbert D. R., Hartman E. Values and the foundations

of strategic management //Journal of Business Ethics. 1988. Т. 7. С. 821-834.

21. Френсіс, Р.Д. Етичне управління ризиками. Глобальна енциклопедія державного управління, публічної політики та управління. *Шпрінгер, Чам. 2016.* URL: https://doi.org/10.1007/978-3-319-31816-5_2385-1 (дата звернення: 19.09.2023).

22. Ніф, Д. Управління корпоративними ризиками через краще управління знаннями. *The Learning Organization*, том 12 No 2, с. 112-124. 2005. URL: https://doi.org/10.1108/09696470510583502

23. Ferrell O. C., Fraedrich J., Ferrell L. Business ethics: Ethical decision making and cases. Dreamtech Press, 2005. 231 p.

24. Disterer, G. ISO/IEC 27000, 27001 та 27002 для управління інформаційною безпекою. Інф. 2013, 4, pp. 92–100.

25. Velasco J., Ullauri R., Pilicita L., Jácome B., Saa P., Moscoso-Zea O. *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. 2018 International Conference on Information Systems and Computer Science (INCISCOS). Quito, Ecuador, 2018. pp. 294-300, URL: https://doi.org/10.1109/INCISCOS.2018.00049. (дата звернення: 23.19.2023).

26. De-Loecker, J., and A. COLLARD-WEXLER. The productivity impact of new technology: *Evidence from the US Steel industry*. 2016. 214 с.

27. Sanchez L.E., Villafranca D., Fernandez-Medina E., Piattini M. Developing a Maturity Model for Information System Security Management within Small and Medium Size Enterprises. *Wosis*, pp. 256-266, 2016.

28. Nancylia M., Mudjtabar E. K., Sutikno S. Rosmansyah Y. *The measurement design of information security management system*. 2014 8th International Conference on Telecommunication Systems Services and Applications (TSSA), Kuta, Bali, Indonesia, 2014, pp. 1-5, URL: https://doi.org/10.1109/TSSA.2014.7065914.

29. Martelo R., Maderay J., Betin A. *Software para gesti6n documental un componente modular del Sistema de Gesti6n de Seguridad de la Informaci6n*

(SGSI), Informacion Tecnologica, pp. 129-134, 2015. URL: http://dx.doi.org/10.4067/S0718-07642015000200015.

30. K. Pecifia, R. Estremera, A. Bilbao, E. Bilbao. Physical and Logical Security Management Organization Model Based on ISO 31000 and ISO 27000, Carnahan Conference on Security Technology, pp. 1-5, 2011. URL: https://doi.org/10.1109/CCST.2011.6095894.

31. Кіціос, Ф.; Хацідімітріу, Е.; Камаріоту, М. Стандарт управління інформаційною безпекою ISO/IEC 27001: як отримати цінність з даних в IT-секторі. *Сталий розвиток 2023*, 15, 5828. URL: https://doi.org/10.3390/su15075828.

32. Путра Ф. Сетіа, Х. Прадана А. *Розробка управління ризиками інформаційної безпеки з використанням ISO/IEC 27005 та NIST SP 800-31* Редакція 1: Тематичне дослідження додатків комунікаційних даних Інституту XYZ. In Proceedings of the International Conference on Information Technology Systems and Innovation (ICITSI) 2017 року, Бандунг, Індонезія, 23–24 жовтня 2017 р.; P. 251–256.

33. Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, Dewa Made Sri Arsa. *Information Technology Risk Management Using ISO 31000 Based on ISSAF Framework Penetration Testing (Case Study: Election Commission of X City).* International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.4, pp. 30-40, 2020. URL: https://doi.org/10.5815/ijcnis.2020.04.03.

34. Mahtuf R., Hatta P., Wihidiyat E. S., Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan. JOINTECS - *Journal Inf. Technol. Comput. Sci.*. vol. 4. no. 1, p. 17, 2019.

35. Nugraha U. Istambul R., Implementation of ISO 31000 for information technology risk management in the government environment. *Int. J. Innov. Creat. Chang.*, vol. 6, no. 5, pp. 219–231, 2019.

36. Riadi I., Sunardi S., Handoyo E. Security Analysis of Grr Rapid Response Network using COBIT 5 Framework. Lontar Komput. *J. Ilm. Teknol. Inf.* vol. 10, no. 1, p. 29, 2019.

37. Hussain M., Hasan M., Taimoor M., Chughtai A., Penetration Testing In System Administration. *Int. J. Sci. Technol. Res.*, vol. 6, no. 6. 2017, pp. 275–278.

38. Парвіайнен, Т. Герландт, Ф. Гелле, І. Хаапасаарі, П. Куйкка, С. Впровадження байєсівських мереж для управління ризиками розливів нафти на основі ISO 31000: 2018: сучасний стан, переваги та виклики впровадження, а також майбутні напрямки досліджень. *Ж. Навколишнє середовище. Управління.* 2021 р., 278, 111520. URL: https://doi.org/10.1016/j.jenvman.2020.111520.

39. Govender D. The use of the risk management model ISO 31000 by private security companies in South Africa. *Secur J* 32, 218–235. 2019. URL: https://doi.org/10.1057/s41284-018-0158-x.

40. Davenport T. H., Guha A., Grewal D., Bressgott T. How artificial intelligence willchange the future of marketing. *Journal of the Academy of Marketing Science.* 48(1). 2020. pp. 24-42. URL: https://doi.org/10.1007/s11747-019-00672-z.

41. Battilana J., & Casciaro T. Overcoming resistance to organizational change: Strongties and affective cooptation. *Management Science*, 65(2). 2019. pp. 565-583. URL: https://doi.org/10.1287/mnsc.2017.2900.

42. Brynjolfsson E., McAfee A. The business of artificial intelligence. HarvardBusiness Review. 2017. URL: https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence (дата звернення: 13.11.2023).

43. Unisa. 2016. Policy on research ethics, URL: https://my.unisa.ac.za/static/intranet/content/department/college/20of%/20Graduate%20studies/documents/policy/20on%20Research/Ethics/%20rev%/2015.09.2016 pdf (дата звернення: 03.09.2023).

44. Watts L., Medeiros K., McIntosh, T., Mulhearn T. Decision biases in thecontext of ethics: Initial scale development and validation. *Personality & Individual Differences.* 2020. URL: https://doi.org/10.1016/j.paid.2019.109609.

45. Watts, L. L., & Buckley, M. R. A dual-processing model of moral

whistleblowing inorganizations. *Journal of Business Ethics*, 2017. 146, 669-683.

46. Tenbrunsel A. Smith-Crowe K. Ethical decision making: Where we've been andwhere we're going. *Academy of Management Annals*, 2, 2008. Pp. 545-607.

47. Thiel C. E., Bagdasarov Z., Harkrider L., Johnson J. F., Mumford M. D. Leaderethical decision-making in organizations: Strategies for sensemaking. *Journal of BusinessEthics* 107. 2012. Pp. 49-64.

48. Torrence B., Watts L., Mulhearn T., Turner M., Todd E., Mumford M. D., Connelly S. Curricular approaches in ethics education: Reflecting on more andless effective practices in instructional content. *Accountability in Research*, 24, 2017. Pp. 269-296 .

49. Antes A. L., Brown R. P., Murphy S. T., Waples E. P., Mumford M. D., Connelly S., Devenport L. D. Personality and ethical decision-making in research: The role ofperceptions of self and others. *Journal of Empirical Research on Human ResearchEthics*, 2, 2007. 15-34. Available from: URL: https://www.researchgate.net/publication/347781977_Ethical_decision_making [accessed Jan 10 2024].

50. Hermansson H., Hansson, Sven Ove. (). A Three-Party Model Tool for Ethical Risk Analysis. *Risk Management*. 9. 129-144. 2007. URL: https://doi.org/10.1057/palgrave.rm.8250028.

51. Рінгквіст, Е.Дж.. Екологічна справедливість: нормативні та емпіричні Доказів. У Віг, Нью-Джерсі та Крафт, М.Е. (ред.) Екологічна політика: нові напрямки для XT)'-I ст. Вашингтон, округ Колумбія: CQ Press, 2000. с. 232-256.

52. Бансал Е. Диференціація кількісного та якісного аналізу ризиків. iZenBridge 12 лютого 2019 р., URL: https://www.izenbridge.com/blog/differentiating-quantitative-risk-analysis-and-qualitative-risk-analysis/.

53. Тан Д. Кількісний аналіз ризиків крок за кроком, читальний зал інформаційної безпеки Інституту SANS, грудень 2020 р., URL:https://www.sans.org/reading-room/whitepapers/auditing/quantitative-risk-

analysis-step-by-step-849 (дата звернення: 03.12.2023).

54. Холл Х. Оцінка ризиків за допомогою якісного аналізу ризиків, URL: https://projectriskcoach.com/evaluating-risks-using-qualitative-risk-analysis/ (дата звернення: 03.12.2023).

55. Леал Р. Якісна та кількісна оцінка ризиків в інформаційній безпеці: відмінності та подібності. 27001 *Академія*, 6 березня 2017 р. URL: https://advisera.com/27001academy/blog/2017/03/06/qualitative-vs-quantitative-risk-assessments-in-information-security/.(дата звернення: 03.12.2023).

56. Шміттлінг Р., Муннс А.. Проведення оцінки ризиків для безпеки. ISACA Журнал, Том 1. 2010, URL: https://www.isaca.org/resources/isaca-journal/issues. (дата звернення: 08.12.2023).

57. Гудріч Б. Якісний аналіз ризиків vs. кількісний аналіз ризиків. PM Learning Solutions. URL: https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1 (дата звернення: 09.12.2023).

58. Мейєр В. *Кількісна оцінка ризику: вимірювання невидимого*. Глобальний конгрес PMI 2015 – EMEA. Лондон, Англія, 10 жовтня 2015 р., URL: https://www.pmi.org/learning/library/quantitative-risk-assessment-methods-9929 (дата звернення: 14.12.2023).

59. Тірні, М. Кількісний аналіз ризиків: очікувані річні збитки. *Netwrix Blog*, 24 липня 2020 р. URL: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis(дата звернення: 14.12.2023).

60. Siponen M. Vance A. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly: *Management Information Systems.* 34. 2010. pp. 487-502. URL: https://doi.org/10.2307/25750688.

61. Sommestad T., Hallberg J., Lundholm K., Bengtsson J. Variables influencing information security policy compliance. *Information Management & Computer Security* (22:1). 2014. pp 42-75. URL: https://doi.org/10.1108/IMCS-08-2012-0045.

62. Kadenko S., Tsyganok V., Andriichuk O., Karabchuk A. Аналіз інструментарію підтримки прийняття рішень у контексті вирішення задач стратегічного планування. Реєстрація, зберігання і обробка даних. №22(2). 2020. с. 77-91. URL: https://doi.org/10.35681/1560-9189.2020.22.2.211281

63. Kenneally E., Dittrich David. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research (August 3, 2012). URL: http://dx.doi.org/10.2139/ssrn.2445102.

ДОДАТКИ

Додаток А

Проект Кодексу етики та професійної поведінки Форуму груп реагування на інциденти та забезпечення безпеки (FIRST)

Члени груп реагування на інциденти та забезпечення безпеки (Групи) мають доступ до багатьох цифрових систем та джерел інформації. Їхня діяльність може змінити світ. Як представник цієї професійної галузі член Групи повинен усвідомлювати свою відповідальність перед клієнтурою та іншими фахівцями в галузі безпеки, а також перед суспільством в цілому. Приватні особи також мають усвідомлювати відповідальність за забезпечення власного благополуччя.

Завдання цього Кодексу полягає в тому, щоб стимулювати та спрямовувати етичну поведінку всіх членів Групи, включаючи чинних та потенційних фахівців-практиків, інструкторів, студентів, впливових осіб та будь-яких осіб, які ефективно використовують комп'ютерні технології. У Кодексі містяться принципи, сформульовані як заяви про відповідальність та засновані на уявленні про пріоритетну роль суспільного блага у всіх випадках. Кожен принцип доповнюється керівними вказівками, які містять призначені для фахівців у галузі обчислювальної техніки роз'яснення, що забезпечують розуміння і застосування цього принципу.

Обов'язки членів Групи перераховані нижче (не в порядку пріоритетності).

Ці обов'язки слід сприймати не як абсолютні приписи, але як рекомендації, що відповідають за своєю значимістю визначенням "СЛІД" у документі IETF RFC2119: "можуть існувати вагомі умови за певних обставин, в яких цю умову можна ігнорувати, але перед тим як вибрати інший варіант, необхідно повністю усвідомити наслідки та ретельно зважити ситуацію"

Обов'язок підтримувати довіру

Довіра лежить в основі безлічі взаємин між Групами і найчастіше є обов'язковою умовою змістовного обміну інформацією.

Спільнота FIRST ґрунтується на цій довірі і може продовжувати свою діяльність лише за наявності достатнього рівня довіри між Групами.

Відповідно до обов'язку підтримувати довіру членам Груп слід:

1) приймати він лише здійсненні зобов'язання;

2) вести себе передбачуваним чином щодо інших Груп (наприклад, дотримуватися стандарту TLP);

3) підтримувати існуючі відносини з іншими групами на основі взаємної довіри.

Слід спочатку припускати створення перехідних відносин на основі взаємної довіри, тобто тих, хто спирається на принцип довіри при першому

використанні (TOFU) і забезпечує довіру до Груп, яким довіряють інші Групи.

Обов'язок здійснювати скоординоване розкриття інформації про вразливість

Членам Групи, які отримали інформацію про вразливість, слід здійснювати скоординоване розкриття інформації про вразливість, вступивши у співпрацю із зацікавленими сторонами для усунення вразливостей системи безпеки та мінімізації збитків, пов'язаних із розкриттям інформації. До зацікавлених сторін належать, зокрема, особа, яка повідомила про вразливість, порушений постачальник (постачальники), координатори, що захищають сторони, а також споживачі нижче, партнери та користувачі.

Членам Групи слід координувати свої дії з відповідними заінтересованими сторонами для узгодження чітких графіків та порядку розкриття інформації, повідомляючи користувачам подробиці в достатньому обсязі для того, щоб вони могли оцінити ризики та вжити дієвих заходів захисту.

Обов'язок дотримуватися конфіденційності

Члени Групи зобов'язані у відповідних випадках дотримуватися конфіденційності.

Членам Групи може бути направлений прямий запит на збереження конфіденційності певної інформації, наприклад, за допомогою протоколу маркування інформації (TLP) Членам Групи слід, по можливості, виконувати ці запити. У разі неможливості збереження конфіденційності інформації, наприклад, якщо це суперечить вимогам місцевих законів, умовам договорів або обов'язкам надавати інформацію, члену Групи слід негайно повідомити власника інформації про цю суперечність.

Деякі обов'язки щодо збереження конфіденційності ґрунтуються на законах, нормах чи звичаях. Якщо в процесі реагування на інцидент деякі сторони змушені дотримуватись цих вимог або розраховують на збереження конфіденційності на підставі даних міркувань, їм слід докласти всіх зусиль для того, щоб відкрито заявити про свої очікування. В такому випадку всім сторонам слід взяти до уваги дані очікування та виконати прямий запит на збереження конфіденційності інформації там, де це можливо.

Обов'язок підтверджувати отримання інформації

Групи отримують інформацію з багатьох джерел – від дослідників, клієнтів, інших Груп, державних установ тощо. буд. Членам Групи слід своєчасно відповідати на запити, навіть якщо ця відповідь містить лише підтвердження отримання запиту. По можливості членам Групи слід визначити очікувані терміни отримання наступних оновлень.

Обов'язок отримувати дозвіл

Члени Групи мають законні потреби та право вивчати галузі своєї відповідальності, діючи лише в системах, куди їм дозволено доступ. Члени Групи повинні бути поінформовані про те, як їхні дії можуть торкнутися їхніх клієнтів, та вживати заходів до того, щоб не заподіяти додаткової шкоди у процесі виконання своїх обов'язків. Слід роз'яснювати торкнутися зацікавлених сторін суть можливих наслідків цих дій. За наявності можливості

слід проводити консультації з клієнтами, перш ніж вносити зміни до їхньої системи.

Обов'язок надавати інформацію

Членам Групи слід вважати своїм обов'язком надання клієнтам інформації про існуючі загрози безпеці та ризики. Якщо члени Групи мають інформацію, здатну або негативно впливати на безпеку і захист, або підвищити їх ефективність, вони зобов'язані вжити належних заходів щодо надання цієї інформації відповідним сторонам або іншим сторонам, здатним надати допомогу, належним чином дотримуючись при цьому зобов'язань щодо збереження конфіденційності інформації. , закони та нормативні акти про недоторканність приватного життя чи інші зобов'язання.

Обов'язок дотримуватися прав людини

Членам Групи слід мати на увазі, що їхні дії можуть торкатися прав людини інших осіб внаслідок поширення інформації, можливого прояву упередженості у їхніх діях чи зазіхань на майнові права.

У процесі врегулювання інцидентів члени Групи отримують доступ до широкого спектру особистої, закритої та конфіденційної інформації. Цю інформацію слід обробляти так, щоб забезпечити дотримання прав людини.

У процесі врегулювання інциденту особам, які вживають заходів реагування, не слід діяти упереджено. Вони повинні докладати всіх зусиль для того, щоб усунути упередженість з процедур та процесів прийняття рішень як здійснюваних особами, які вживають заходів реагування, так і вбудованих у алгоритми.

Для цілей застосування цього принципу до поняття "майно" (Декларація прав людини ООН, стаття 17) включені також нематеріальні види власності, наприклад об'єкти інтелектуальної власності, а також ідеї та концепції в цілому, незалежно від того, чи вони під захистом закону (наприклад, є запатентованими).

Обов'язок піклуватися про здоров'я членів Групи

Групи повинні бути в змозі постійно надавати своїм клієнтам послуги, які вони обіцяли надати. Цей обов'язок включає турботу про фізичне та емоційне здоров'я членів Групи.

З метою дотримання прав осіб, які є членами Групи, а також з метою забезпечення довгострокової життєздатності Групи та належного рівня обслуговування Групі слід прагнути до створення здорового, безпечного та позитивного робочого середовища, що сприяє збереженню фізичного та емоційного здоров'я (всіх) членів Групи. З метою ефективного реагування на кризу слід вживати заходів щодо захисту емоційного здоров'я та пом'якшення стресів у рамках звичайної діяльності Групи.

Обов'язок зміцнювати потенціал Групи Управління інцидентами є сферою досліджень, що постійно розвивається, і членам Групи слід безперервно вивчати її. Групі слід надавати своїм членам необхідні ресурси для вивчення, застосування та вдосконалення науково-технічних знань у сфері (сферах) їхньої діяльності. У цьому випадку корисними можуть бути навчальні заняття або програми додаткової професійної освіти/підвищення кваліфікації,

однак для належного виконання цього обов'язку недостатньо лише здійснювати відповідні заходи. Групі слід забезпечувати функціонування технічної інфраструктури, достатньої для надання послуг Групи, у тому числі шляхом вживання належних заходів для захисту цієї інфраструктури від втручання зовнішніх сторін.

Обов'язок здійснювати відповідальний збір даних

Збір даних є необхідною умовою реагування на інциденти, однак слід підтримувати баланс між досягненням цілей реагування на інциденти та дотриманням прав зацікавлених сторін, що працюють із даними.

Обсяг інформації, що підлягає збору, може змінюватися в процесі розслідування. У міру розгляду інциденту членам Групи слід наводити обсяг інформації, що збирається, у відповідність до змінних вимог. Слід виключати зі звітності дані, які мають прямого відношення до інциденту та його врегулювання.

Зібрані та вилучені дані слід обробляти відповідно до чинних законів та за умови дотримання недоторканності приватного життя користувача (користувачів). Слід отримати дозвіл власника даних перед тим, як проводити збирання та обробку даних, що знаходяться під його контролем. Слід дотримуватись чинних нормативно-правових актів, що стосуються обробки даних.

Слід надавати іншим групам реагування, що займаються розглядом інших інцидентів, доступ до даних, які можуть бути корисні для них, можливо, у відредагованому вигляді. Доступ до конфіденційної та приватної інформації слід надавати лише за умови забезпечення належного захисту.

Слід оцінити ризики та вигоди, перш ніж ділитися даними з третіми сторонами з метою зменшення обсягу збитків. Ділитись даними слід лише в тому випадку, якщо вигоди помітно переважають ризики. Конфіденційні дані слід зберігати таким чином, щоб їх можна було легко знищити після завершення розгляду інциденту. Слід здійснювати безпечне знищення зібраних даних відповідно до політики збереження даних.

Обов'язок визнавати межі юрисдикцій

Членам Групи слід визнавати та поважати межі юрисдикцій, законні права, правові норми та органи влади сторін, які беруть участь у діях, пов'язаних із реагуванням на інциденти.

У юрисдикціях, що беруть участь у розгляді інциденту, можуть існувати різні закони, норми та інші правові аспекти, у тому числі пов'язані із захистом недоторканності приватного життя або направленням повідомлень про витік даних.

Для визначення меж юрисдикцій можуть використовуватися як фактичне розташування залучених сторін (наприклад, країна або місце юридичної реєстрації), так і інші фактори, що мають відношення до цих сторін. Закони та норми можуть відрізнятися навіть у різних адміністративних регіонах однієї країни (наприклад, в окремих штатах США), а також у різних суб'єктах підприємницької діяльності, галузях чи секторах цієї держави (наприклад, у сфері охорони здоров'я, у сфері фінансових послуг чи державних

установах) . Національні CSIRT можуть мати певні сфери відповідальності та/або повноважень для здійснення діяльності за участю клієнтів у межах своїх юрисдикцій. Крім того, вони можуть співпрацювати з іншими установами, які мають необхідні повноваження для діяльності в інших юрисдикціях, або передавати їм інформацію та право вчиняти певні дії.

Членам Групи слід мати уявлення про ключові фактори, що впливають на залучені юрисдикції, включаючи, зокрема, норми забезпечення недоторканності приватного життя або вимоги до направлення повідомлень про витік даних. Зважаючи на те, що в усьому світі відбувається безперервний розвиток та оновлення законів і норм, що стосуються кібербезпеки та захисту недоторканності приватного життя, рекомендується проводити консультації з обізнаним юристом, щоб визначити, чи ставиться те чи інше питання до кількох юрисдикцій.

Обов'язок будувати логічні міркування на основі фактичних даних.

Групам слід засновувати свою оперативну діяльність на фактах, що піддаються перевірці. При спільному використанні інформації, наприклад, індикаторів компрометації (IOC) або описів інциденту, члени Групи повинні представляти прозорі докази та дані про масштаби інциденту. За відсутності такої можливості слід подати наявну інформацію та повідомити про причини, що перешкоджають спільному використанню доказів та даних про масштаби інциденту.

Членам Групи слід утриматися від поширення чуток чи обміну чутками. Будь-які припущення слід чітко називати такими.

Прозорі процеси збору доказів та побудови логічних міркувань мають велике значення навіть за автоматичного спільного використання даних, тобто за автоматичного спільного використання великих масивів інформації. У такому разі слід розповсюдити докладний опис глибинного аналізу даних.

Додаток

Члени Групи нерідко можуть опинятися в ситуаціях, коли дії, які вони вживають, не відповідають усім етичним принципам. У цій ситуації необхідно вибрати найважливіші принципи. У цій ситуації особам, які займаються розглядом інциденту, слід визначити, чи бажано в ході обговорення з колегами, які зацікавлені сторони можуть бути порушені їхніми діями і яким чином вони будуть порушені. Як правило, слід обирати рішення, яке передбачає мінімальне порушення цього Кодексу. Іноді це може бути неможливим, наприклад, через зовнішній тиск. У такому разі рекомендується продовжувати вживати необхідних заходів, навіть під можливим тиском, відзначивши при цьому існування етичної дилеми.