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 СВІТОВИХ СТАНДАРТІВ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ ”

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

_____ Назарій ШУЛІПА
(підпис) Ім’я, ПРІЗВИЩЕ здобувача

Виконав: Здобувач вищої освіти гр. УБДМ 61
Назарій ШУЛІПА

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н.,
професор: Галина ГАЙДУР

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 Шуліпі Назарію Сергійовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Етичні норми світових стандартів в управлінні кібербезпекою”

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, 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 норм в управлінні кібербезпекою.
   2. Проаналізувати світовий досвід застосування етичних кодексів у кібербезпеці.
   3. На основі аналізу розробити рекомендації щодо покращення дотримання етичних норм та принципів у сфері управління кібербезпекою.
   4. Здійснити моніторинг та оцінку ефективності розроблених пропозицій.

5. Перелік ілюстративного матеріалу: *презентація*

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

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 основних принципів етичних норм у кібербезпеці	27.10.2023	
4.	Дослідження вимог міжнародних стандартів щодо етичних норм у кібербезпеці	10.11.2023	
5.	Аналіз світового досвіду застосування етичних кодексів у кібербезпеці.	15.11.2023	
6.	Розробка рекомендацій щодо покращення дотримання етичних норм та принципів у сфері управління кібербезпекою	22.11.2023	
7.	Відпрацювання пропозицій та рекомендацій удосконалення застосування корпоративних етичних кодексів в кібербезпеці	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.	16.01.2024	

Здобувачка вищої освіти _____ Назарій ШУЛІПА
(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 Шуліпа Н.С. 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 світових стандартів в управлінні кібербезпекою"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ШУЛІПА Назарій** у кваліфікаційній роботі дослідив сучасний стан застосування сучасних етичних норм в управлінні кібербезпекою, визначив основні етичні виклики та проблеми кібербезпеки, розробив зразок етичного кодексу організації кібербезпеки та визнначив шляхи впровадження запропонованого кодексу у практику діяльності організацій. Розроблені рекомендації разом із мжнародними стандартами забезпечать забезпечать попередження інцидентів та вразливостей систем інформаційної безпеки організацій, дозволять керівниками організацій правильно організувати заходи кібербезпеки при здійсненні управлінської діяльності. **ШУЛІПА Назарій** 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 **ШУЛІПИ Назарія** на оцінку "відмінно" 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 Шуліпа Н.С. 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 Шуліпи Назарія Сергійовича
на тему "ЕТИЧНІ НОРМИ СВІТОВИХ СТАНДАРТІВ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ"

Актуальність

Зроблений в роботі аналіз етичних аспектів кібербезпеки дозволив правильно обгрунтувати вибрану тему дослідження. З аналізу виявлено, що, що дослідження виступає життєво важливими для визначення етичної поведінки, зменшення ризиків, захисту прав користувачів, розбудови довіри, забезпечення дотримання вимог, вирішення проблем і формування культури етичної відповідальності. Вказане дослідження слугує наріжним каменем для прийняття етичних рішень, формування політики та розвитку практик кібербезпеки.

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 кібербезпеки дозволяє імплементувати їх в національну практику управління кібербезпекою вітчизняних організацій та підприємств та національні нормативно-правові акти. Описуються важливість інтеграції етичних норм у національну корпоративну культуру та визначаються основні виклики та переваги їх застосування.

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

Недоліки

Було б також доцільно у роботі зробити аналіз застосування етичних норм у корпоративних кодексах вітчизняних закладів вищої освіти. Однак, зазначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Шуліпа Назарій Сергійович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: професор кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАЙДУР
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 83 стор., 5 рис., 0 табл., 62 джерел.

Метою роботи є дослідження та аналіз етичних норм та стандартів у сфері кібербезпеки та розробка рекомендацій для інтеграції цих стандартів в корпоративні практики.

Об'єктом дослідження є процес етичного управління кібербезпекою.

Предмет дослідження - теоретичні і практичні аспекти етичних норм світових стандартів в управлінні кібербезпекою.

Методи дослідження. Аналіз нормативної бази, синтез існуючих підходів до етичних норм в кібербезпеці, системний аналіз інтеграції етичних стандартів у корпоративні практики.

Короткий зміст роботи. Робота зосереджена на важливості етичних норм в кібербезпеці, аналізує глобальні стандарти, такі як GDPR, ISO/IEC серії стандартів, та їх вплив на етичні аспекти кібербезпеки. Описана важливість інтеграції етичних норм у корпоративну культуру та визначені основні виклики та переваги їх застосування. Зроблений аналіз наукової літератури та публікацій, пов'язаних із застосуванням етичних норм в управлінні кібербезпекою, проаналізований світовий досвід застосування етичних кодексів у кібербезпеці дозволив розробити рекомендації щодо покращення дотримання етичних норм та принципів у сфері управління кібербезпекою.

Галузь застосування. Результати дослідження можуть бути використані для розробки або вдосконалення етичних кодексів у компаніях, особливо в сфері кібербезпеки, а також слугувати навчальним матеріалом у курсах з кібербезпеки.

КЛЮЧОВІ СЛОВА: ЕТИЧНІ НОРМИ, КІБЕРБЕЗПЕКА, КОРПОРАТИВНА КУЛЬТУРА, ЕТИКА КІБЕРБЕЗПЕКИ, УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

ABSTRACT

The text part of the qualification work for the master's degree: 83 pages, 5 figures, 0 tables, 62 sources.

The purpose of the work is research and analysis of ethical norms and standards in the field of cyber security and development of recommendations for the integration of these standards into corporate practices

Object of research is the process of ethical cyber security management.

Subject of research is the theoretical and practical aspects of ethical norms of world standards in cyber security management.

Research methods. Analysis of the regulatory framework, synthesis of existing approaches to ethical norms in cybersecurity, systematic analysis of the integration of ethical standards into corporate practices.

Brief content of research. The work focuses on the importance of ethical norms in cyber security, analyzes global standards such as GDPR, ISO/IEC series of standards, and their impact on ethical aspects of cyber security. The importance of integrating ethical standards into corporate culture is described, and the main challenges and advantages of their application are identified. The analysis of scientific literature and publications related to the application of ethical norms in the management of cyber security, the analyzed world experience in the application of ethical codes in cyber security made it possible to develop recommendations for improving compliance with ethical norms and principles in the field of cyber security management.

Field of research. The results of the study can be used to develop or improve codes of ethics in companies, especially in the field of cybersecurity, and also serve as teaching material in cybersecurity courses.

KEYWORDS: ETHICAL STANDARDS, CYBER SECURITY, CORPORATE CULTURE, CYBER SECURITY ETHICS, CYBER SECURITY MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми. У зв’язку з тим, що нинішні інформаційно-обмінні процеси виступають відносно новим культурним явищем, система моральної регуляції, яка була б ефективною і зрозумілою у сфері інформаційної безпеки ще не сформувалась. І суспільство виявилося ще не готовим до того, що будь-які взаємодії в інформаційному просторі можуть регулюватися моральними нормами і принципами, тому дослідження етичних аспектів у сфері кібербезпеки має першорядне значення в сучасному цифровому ландшафті.

Розуміння і дослідження етичних аспектів кібербезпеки дає фахівцям, політикам і організаціям рекомендації щодо відповідальної та етичної поведінки при роботі з конфіденційними даними, цифровими активами і новими технологіями. Такого роду рекомендації допомагають формувати політику, практики та стандарти, які надають пріоритет етичним міркуванням.

З окресленого випливає, що дослідження етичних аспектів кібербезпеки виступає життєво важливими для визначення етичної поведінки, зменшення ризиків, захисту прав користувачів, розбудови довіри, забезпечення дотримання вимог, вирішення проблем і формування культури етичної відповідальності. Вказане дослідження слугує наріжним каменем для прийняття етичних рішень, формування політики та розвитку практик кібербезпеки у все більш взаємопов’язаному та цифровому світі.

З огляду на зазначене, тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб’єктів підприємницької діяльності в сучасних умовах.

Мета і завдання дослідження. Мета роботи полягає у формулюванні рекомендацій для організацій щодо впровадження етичних норм у сфері кібербезпеки на основі дослідження теоретичних і практичних аспектів управління кібербезпекою.

Для досягнення цієї мети в роботі виконані наступні *завдання*:

- огляд основних принципів етичних норм, визначених світовими стандартами;

- проведений огляд світових стандартів і норм у галузі кібербезпеки та їхнього впливу на етичні питання;

- проаналізовані основні етичні виклики та проблеми, що виникають в управлінні кібербезпекою;

- розглянуті міжнародні стандарти, які включають етичні аспекти в управління кібербезпекою, такі як ISO/IEC 27001, їх зміст та вимоги;

- визначені можливі наслідки недотримання етичних норм;

- проаналізований світовий досвід застосування етичних кодексів у кібербезпеці;

- розглянуті етапи розробки етичного кодексу, який враховує світові стандарти та етичні норми в кібербезпеці;

- окреслені процеси визначення процедур впровадження та моніторингу етичного кодексу;

- сформулювані рекомендації для організацій щодо впровадження етичних норм в управлінні кібербезпекою.

Об'єкт дослідження – процес етичного управління кібербезпекою.

Предмет дослідження – теоретичні і практичні аспекти етичних норм світових стандартів в управлінні кібербезпекою.

Методи дослідження. З метою вирішення вище вказаних наукових завдань у даній роботі застосовані методи системного аналізу для виконання огляду основних принципів етичних норм, визначених світовими стандартами та огляду світових стандартів і норм у галузі кібербезпеки та їхнього впливу на етичні питання; методи індукції і дедукції при вивчити процесів інтеграції етичних норм у протоколи та практики кібербезпеки;

Наукова новизна одержаних результатів полягає в тому, що вперше проведено комплексне дослідження етичних норм світових стандартів в управлінні кібербезпекою та визначені шляхи впровадження етичних кодексів в процеси управління кібербепезкою. Розроблені підходи можуть бути

використані в процесі планування та реалізації системи управління кібербезпекою підприємства.

Практичне значення одержаних результатів. Застосування здобутих результатів дасть змогу 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:

Шуліпа Н., Порохницький О. Застосування етичних норм світових стандартів в корпоративному управління інформаційною безпекою. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 23 лют. 2023 р. Київ, 2023. С. 127–128.

РОЗДІЛ 1
ОСНОВНІ ПРИНЦИПИ ЕТИЧНИХ НОРМ У КІБЕРБЕЗПЕЦІ

1.1 Аналіз основних принципів етичних норм, визначених світовими стандартами

Світове наукове співтовариство у наш час доволі активно займається впровадженням принципів інформаційної етики у практику шляхом інтеграції головних постулатів останньої в навчальний процес обширного кола спеціалістів найбільш різноманітних галузей. В західних країнах створені інститути, які займаються дослідженням проблеми соціального впливу комп'ютерних технологій на суспільство та особистість, до того ж, й розробляють відповідні рекомендації, методи і норми їх впровадження у суспільну свідомість [17].

Завдяки зусиллям ЮНЕСКО та Організації Об'єднаних Націй на міжнародному рівні було створено низку кодексів інформаційного суспільства, котрі, не дивлячись на те, що не охоплюють усього комплексу можливих та існуючих етичних проблем, які мають зв'язок із наслідками застосування інформаційних технологій, проте ставлять проблеми та привертають увагу до них. На пострадянському просторі, й у тому числі в нашій країні, етична проблематика в сфері інформаційних технологій почала вивчатись доволі не давно. Однак, уже сформувалось деяке коло дослідників зазначеної проблематики, зокрема І. А. Авдєєва, І. Ю. Алексєєва, І. Л. Галинська, М. А. Дедюліна, Е. В. Коваль, А. А. Малюк, О. М. Манжуєва, Г. А. Миролюбенко, О. Ю. Полянська, А. І. Панченко, А. С. Сергєєв, Г. П. Отюцький, О. А. Філіна, І. І. Чхеайло, А. А. Чхеайло, О. К. Щіпунов та багато інших. Сьогодні дослідження у галузі інформаційно-комунікаційних технологій провадяться у розрізі наступних напрямків: корпоративна етика Інтернет-спільнот, нетикет, інтернет-етика, цифрова етика, кіберетика, мережева етика, віртуальна етика, інформаційна етика (інфоетика), комп'ютерна етика [2, с. 161]. Частина науковців об'єднують поняття інформаційна і комп'ютерна етика [30], деякі

вчені вважають аналогічною сутність понять мережева етика, кіберетика, інтернет-етика [8]. У деяких роботах ототожнюються інформаційна і цифрова етика [1].

На основі проведеного аналізу, вважаємо, що доцільно розглядати окреслені дефініції окремо, адже кожна з них має свої особливості.

Окреслимо сутність вищенаведених понять.

Г. Миролюбенко вказує на те, що інформаційна етика являє собою «спробу подолання нерегульованості інформаційно-комунікативного простору, привнесення етичної складової частини у відносини, котрі опосередковані технічними засобами» [18, с. 311]. Ще в 1979 році в Сполучених Штатах Америки був прийнятий перший кодекс інформаційної етики, у преамбулі котрого відзначається «життєво вагома потреба додержання усіх норм етики в процесі розробки й експлуатації засобів інформаційних технологій» [27, с. 55–82].

Згідно з В. М. Мартинюк, відмінно від професійної етики інших спеціалістів, інформаційна етика окреслює моральні принципи не тільки комп’ютерних професіоналів, проте і всіх користувачів комп’ютерних систем та фокусує увагу на вагомості вироблення етичних норм для усіх суб'єктів інформаційного суспільства. Не дивлячись на те, що моральні норми підтримуються тільки силою суспільної дії, наявність останніх потрібна ще у зв’язку з тим, що історично на базі норм моралі виробляються нові та покращуються вже існуючі юридичні норми, що забезпечуються силою впливу держави. Міжнародна федерація інформаційних технологій (IFIP) базуючись на етичних стандартах рекомендувала прийняти кодекси комп’ютерної етики держав із урахуванням етичних, культурних, а також й національних традицій [17].

До одного із найбільш вагомих завдань інформаційної етики, направленим на сприяння гуманізації суспільства, виступає домагання того, аби захист свобод та прав людини почав бути ключовим пріоритетом у використанні інформаційних технологій та застосуванні кіберпростору. Вагомість вказаного

завдання підтверджується, у тому числі, й тим, що в положеннях Декларації прав людини ООН принципи інформаційної етики віднайшли власне відображення. Ключовими умовами реалізації даного завдання виступають створення в глобальних інформаційних мережах чим більшого легітимного контенту, до того ж, й забезпечення доступності інформації, відповідних технологій, кіберпростору для якомога широкого загалу [26, с. 51].

До головних ресурсів розвитку інформаційної етики відносяться етичні кодекси. Н. І. Головіна підкреслює, що процеси регламентації основ етики інформаційного суспільства повинні відбуватись як «згори» (до прикладу, зі сторони Організації Об'єднаних Націй і ЮНЕСКО), так й проєкти самоорганізації – створення етичних норм всередині віртуальних спільнот (правила мережевого етикету; до того ж, й внутрішньо мережеві органи саморегуляції) [2, с. 163].

На думку Ж. Андрійченко, цифровий етикет являє собою новий тип етикету, який окреслює правила культури спілкування, що стосуються реальності нової інформації, таким чином цифрова етика представляє стандарти та норми, розроблені для забезпечення незалежності та гідності користувачів [1].

Нетикет або мережевий інтернет за тлумаченням О. М. Кавки, являє собою «правила поведінки, спілкування у мережі, культура і традиції інтернет-спільноти, котрих додержується більшість» [7, с. 167].

Віртуальна етика виступає одним із напрямів прикладної етики, спрямованим на оцінку моральних вимірів, притаманних процесам віртуальної комунікації, філософське осмислення та оцінку етичних підвалин, що керують поведінкою в цій цифровій сфері. Зазначена дисципліна також передбачає розробку теоретичних основ етичних норм і принципів, які регулюють поведінку в онлайн-сфері, а також створення механізмів, що забезпечують їх дотримання [31].

Професійні етичні кодекси слугують ключовими інструментами в етичному регулюванні інтернету, виходячи за межі виключно комп'ютерних фахівців і охоплюючи всіх учасників інформаційного суспільства. До

найвідоміших кодексів відносяться кодекси, які були розроблені Асоціацією розробників комп'ютерних технологій, Асоціацією менеджерів інформаційних технологій, Асоціацією сертифікованих комп'ютерних професіоналів, й Асоціацією користувачів інформаційних технологій в Сполучених Штатах Америки, які підкреслюють універсальні етичні норми, такі як соціальна та особиста відповідальність, рівноправне спілкування та сумлінне виконання професійних обов'язків. Крім того, вказані кодекси визначають основні права, що надаються кожній дорослій людині, яка бере участь у віртуальній комунікації, і ґрунтуються на принципах загальної доступності, конфіденційності та недоторканності приватної власності [5].

Принцип «загальної доступності» забезпечує права громадян на комунікацію і передбачає доступність інформації в публічних сферах. Водночас, принцип «збереження таємниці приватного життя» гарантує автономію, приватність та захист від втручання в особисте життя з боку зовнішніх суб'єктів. Отже, дотримання конфіденційності довіреної інформації виступає фундаментальною моральною нормою, що покладається на творців і користувачів інформаційних систем [8].

Принцип «недоторканності приватної власності» представляє фундамент економічних відносин власності. У сфері віртуальної етики додержання згаданого принципу означає повагу до права власності на інформацію, а також дотримання законів про авторське право. Дотримання цих принципів передбачає дотримання низки більш конкретних правил, зокрема, принципів свободи слова, толерантності (поваги до різних думок), обережності (дотримання мережевого етикету), точності (дотримання протоколів інформаційних систем) та інших [60].

Поява мережевого суспільства характеризує нову соціальну структуру, в якій індивіди є невід'ємними частинами системи, переплетеної мережею зв'язків, включаючи ділових партнерів, друзів та організації, пов'язані за допомогою різних технологічних пристроїв, таких як персональні комп'ютери, мобільні телефони, багатофункціональні портативні пристрої (наприклад, кишенькові комп'ютери), цифрове телебачення та інше. Поширення соціальних

медіа загострює існуючі етичні дилеми і створює нові, що охоплюють питання добровільного обміну даними і конфіденційності, дебати про авторське право і право власності, маніпуляції з боку рекламодавців і політичних інститутів, зростання політичних рухів в Інтернеті і безпеку персональних даних. Етичні характеристики мережі продовжують розвиватися, включаючи її глобальний характер, що сприяє залученню різних культур, проблему анонімності, що спонукає людей ховатися за псевдонімами, швидке поширення даних, що ускладнює розрізнення достовірної та неправдивої інформації, агресивну доступність, що підштовхує до нав'язування інформації, інтерактивні методи комунікації, часто ворожі та принизливі, а також неконтрольоване середовище, яке схильне до вседозволеності [55].

Н. Капустіна висловлює думку, що у зв'язку із вищезазначеним, утворюється нова галузь, яка називається «мережева етика» (чи, як ще її йменують, кіберетика, інтернет-етика), котра досліджує можливості використання кодексів етики і стандартів належної практики у взаємодії із мережею. Згадану етику пов'язують із принципами становлення культури поведінки мережі Інтернет. Відповідно до аналогії із традиційною професійною етикою тут виокремлено головні складові мережевої етики: кодекси мережевої етики (що є регулятором відносин в Мережі) та мережевий етикет (що є регулятором поведінки в Мережі) [8].

Кодексами мережевої етики пропагуються: етика довіри, етика толерантності, етика запобігливості; етика регулювання:

1) «Етика терпимості (її ще йменують етика толерантності) криється в першу чергу в тому, що: неетично придушувати висловлювання інших, навіть в тому разі, коли такі висловлювання ображають власні ваші погляди і віру; неетично за відсутності особливої необхідності тривожити інших; неетично апелювати до судових інстанцій для вирішення спору до того, як використано усі посередницькі і переговорні засоби задля запобігання шкоді.

2) Етика довіри проявляється в такому: неетичним виступає публічно розповсюджувати зображення, думки чи висловлювання інших за відсутності їх

згоди; неетично запитувати або передавати інформацію, яка була створена чи одержана шляхом примусу чи іншими засобами, які зневажають свободу.

3) Етика запобігливості криється у тому, що: неетичним виступає передавати інформацію для осіб, котрі безперечно не є згодними із такого роду інформацією; неетичним є виражати незгоду із ціною застосування комунікаційної мережі. Етика регуляції складається з декількох приписів: представникам корпорацій і держав неетичним є нехтувати чи протидіяти гарантіям законів або нормативів права; етично обговорювати, уточнювати й пропагувати права й етичні норми, подані у цьому документі» [60].

Отже, кіберетика – це розділ етики, який займається етичними питаннями, що виникають у зв'язку з використанням технологій, особливо в контексті інтернету. Вона охоплює широке коло питань, включаючи конфіденційність, безпеку, інтелектуальну власність, кіберзалякування та переслідування в Інтернеті. Кіберетика покликана забезпечити використання технологій з повагою до людських цінностей і гідності, а також сприяти соціальній справедливості та рівності [59]. По суті, кіберетика полягає в тому, щоб збалансувати переваги технологій з потенційними ризиками та негативними наслідками. Вона вимагає враховувати вплив технологій на окремих людей, спільноти і суспільство в цілому, а також приймати рішення, які сприятимуть загальному благу. Кіберетика – це не лише реагування на проблеми в міру їх виникнення, а й передбачення майбутніх етичних викликів та проактивні кроки для їх вирішення. Корпоративна етика, з іншого боку, стосується етичних принципів і цінностей, які керують поведінкою підприємств і організацій. Вона охоплює такі питання, як чесність, прозорість, підзвітність та справедливість, і передбачає забезпечення того, щоб компанії працювали етично обґрунтовано та соціально відповідально. Корпоративна етика важлива, оскільки вона допомагає будувати довіру між бізнесом та його зацікавленими сторонами, зокрема клієнтами, працівниками та акціонерами.

Коли йдеться про інтернет-спільноти, кіберетика та корпоративна етика відіграють вирішальну роль. Інтернет-спільноти створили нові можливості для

людей спілкуватися, співпрацювати та обмінюватися інформацією, але вони також створюють низку етичних проблем. Наприклад, існує занепокоєння щодо приватності та захисту даних, а також поширення дезінформації та мови ворожнечі. Корпоративна етика – це моральні принципи та цінності, які керують поведінкою бізнесу та його стейкхолдерів. У цифрову епоху корпоративна етика набуває особливого значення, оскільки компанії мають доступ до величезних обсягів персональних даних і значний вплив на онлайн-дискурс. Питання щодо конфіденційності даних, прав інтелектуальної власності та підзвітності технологічних гігантів стають все більш актуальними, що підкреслює нагальну потребу в етичних рамках, які можуть вирішити ці проблеми. Крім того, глобальний характер інтернету означає, що підприємствам доводиться мати справу з різними культурними нормами і регуляторними середовищами, що ще більше ускладнює завдання розробки послідовного і відповідального підходу до етики [36].

На основі проведеного дослідження, можемо узагальнити основні принципи етичних стандартів у сфері кібербезпеки наведемо на рис. 1.1.

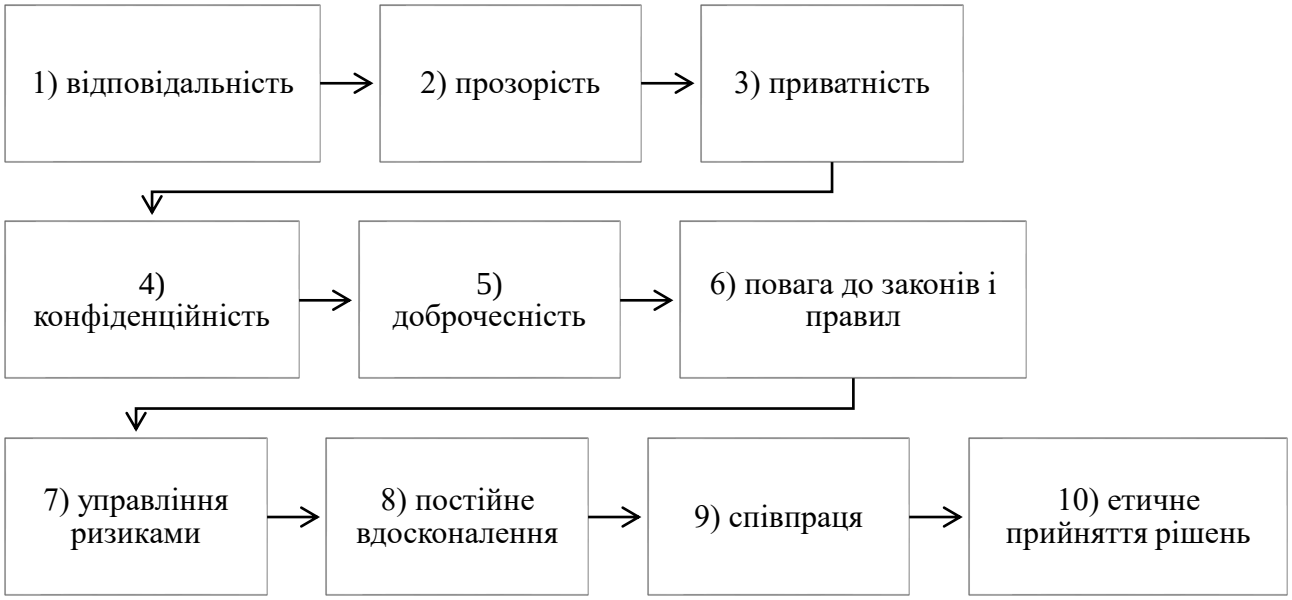

Рис. 1.1. Основні принципи етичних стандартів у сфері кібербезпеки

Джерело: побудовано автором за даними [32]

Розглянемо детальніше сутність кожного вищенаведеного принципу:

1) відповідальність – фахівці з кібербезпеки повинні нести відповідальність за свої дії та рішення, а також відповідати за будь-яку шкоду, заподіяну їхніми діями;

2) прозорість – фахівці з кібербезпеки повинні забезпечувати прозорість своїх дій та процесів прийняття рішень, надаючи чіткі пояснення та обґрунтування свого вибору;

3) приватність – потрібно поважати приватне життя людей та захищати їхню особисту інформацію від несанкціонованого доступу або розголошення;

4) конфіденційність – фахівці з кібербезпеки повинні зберігати конфіденційну інформацію в таємниці та не розголошувати її без належного дозволу;

5) доброчесність – це означає діяти чесно, уникаючи конфлікту інтересів та утримуючись від діяльності, яка може поставити під сумнів їхню неупередженість;

6) повага до законів і правил – фахівці з кібербезпеки повинні дотримуватися відповідних законів і правил, у тому числі тих, що стосуються захисту даних, конфіденційності та безпеки;

7) управління ризиками – потрібно виявляти, оцінювати та зменшувати потенційні ризики для інформаційних систем та даних організації;

8) постійне вдосконалення – фахівці з кібербезпеки повинні бути в курсі нових загроз і технологій, постійно вдосконалювати свої навички та знання, щоб ефективно захищати організацію;

9) співпраця – необхідно співпрацювати з іншими зацікавленими сторонами, включаючи IT-персонал, керівництво та правоохоронні органи, для забезпечення ефективних заходів кібербезпеки;

10) етичне прийняття рішень – фахівці з кібербезпеки повинні застосовувати етичні принципи і системи прийняття рішень для вирішення етичних дилем і прийняття рішень, які відповідають організаційним цінностям і суспільним очікуванням [33].

Перелічені принципи слугують основою етичних стандартів у сфері кібербезпеки, спрямовують фахівців у їхній повсякденній роботі та допомагають забезпечити відповідальний та етичний захист інформаційних систем і даних організацій.

Загалом, узагальнимо, що етичні норми у сфері кібербезпеки мають важливе значення для забезпечення того, щоб фахівці та організації з кібербезпеки діяли відповідально та в інтересах суспільства. Додержуючись зазначених норм, фахівці з кібербезпеки можуть зробити позитивний внесок у розвиток цифрового світу та сприяти формуванню культури довіри, безпеки та конфіденційності. Дотримання ключових етичних стандартів у сфері кібербезпеки слугує основою для встановлення довіри, доброчесності та надійності в цифровій сфері. Додержання таких принципів, як прозорість, підзвітність і повага до приватного життя, не лише захищає конфіденційну інформацію, але й забезпечує відповідальну та етичну поведінку фахівців з кібербезпеки. Надаючи пріоритет цим етичним стандартам, фахівці в цій галузі можуть орієнтуватися в складному ландшафті викликів кібербезпеки, одночасно зменшуючи ризики та захищаючи права і безпеку людей і організацій. Дотримання цих принципів не лише сприяє розвитку культури етичної поведінки, але й робить значний внесок у побудову більш безпечної та надійної цифрової екосистеми на благо суспільства в цілому.

1.2. Аналіз світових стандартів і норм у галузі кібербезпеки та їхнього впливу на етичні питання

В рамках дослідження світових стандартів і норм у галузі кібербезпеці необхідно окреслити сутність поняття кібербезпека.

В літературі наукового спрямування немає єдиного усталеного погляду на зміст поняття «кібербезпека». Згідно до широкого підходу поняття «кібернетична безпека» в статті 1 Закону України «Про основні засади

забезпечення кібернетичної безпеки України» окреслюється у вигляді «захищеності життєво вагомих інтересів людини та громадянина, держави і суспільства в прцоесі використання кіберпростору, за котрої забезпечуються сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, вчасне виявлення, запобігання та нейтралізація потенційних і реальних загроз національній безпеці України в кіберпросторі» [22].

Застосовуючи вужчий підхід, Ю. Г. Даник, тлумачить кібербезпеку (безпеку кіберпростору) як «дії, вжиті у захищеному кіберпросторі з метою запобігання несанкціонованому доступу, пошкодженню чи експлуатації комп'ютерів, електронних систем зв'язку й інших інформаційних технологій, включено із інформаційними технологіями платформи, до того ж інформацію, яка у ній міститься, для забезпечення її цілісності, аутентифікації, доступності, неспростовності та конфіденційності» [4, с. 55].

Відповідно до Б. А. Кормич, відзначається, що кібербезпека являє собою «захищеність встановлених законом правил, за котрими здійснюються інформаційні процеси у державі, які забезпечують гарантовані Конституцією умови існування та розвитку людини, усього суспільства і держави» [14, с. 142].

Низкою науковців на чолі із В. В. Остроуховим, пропонується таке авторське визначення поняття «кібербезпеки»: «стан захищеності держави, особи та суспільства, за котрого досягається інформаційний розвиток (морально-етичний, технічний, соціально-політичний, інтелектуальний), при котрому сторонні інформаційні впливи не завдають їм значної шкоди» [11, с. 10].

А. В. Тарасюк визначає таке важливе поняття у сфері управління етичними нормами кібербезпеки як «соціальні інформаційно-безпекові заходи», відповідно до думки автора – це «ухвалена та підтримувана колективом, особою, державою та суспільством багаторівнева система технологій, яка направлена на створення специфічного механізму регуляції, що окреслює відповідну морально-етичну поведінку індивіда в ході користування інформаційними технологіями і кіберпростором та взаємодії у даному середовищі. Такі заходи стверджують та

зміцнюють усталені правові приписи та морально-етичні настанови що стосуються інформаційної безпеки» [26, с. 50].

Відповідно до М. В. Плескач, будемо вважати механізмом адміністративно- правового забезпечення кібернетичної безпеки людини «узяту у єдності складну систему технічних, юридичних, ідеологічних, організаційних й інших заходів впливу, що здійснюється уповноваженими суб'єктами публічної адміністрації на суспільні відносини, котрі з'являються в процесі застосування кібернетичного простору, задля їх упорядкування, до того ж задля забезпечення охорони та захисту життєво вагомих інтересів, свобод і прав людини у даній сфері» [21, с. 203].

Стандарт кібербезпеки – це набір інструкцій або найкращих практик, які організації можуть використовувати для покращення свого стану кібербезпеки. Стандарти також можуть надавати вказівки щодо реагування на інциденти кібербезпеки та відновлення після них [19].

Глобальні стандарти та норми у сфері кібербезпеки мають важливе значення для забезпечення захисту критичної інфраструктури, запобігання кібератакам та підтримання міжнародного миру і стабільності. Зазначені стандарти і норми є керівними принципами для організацій, які допомагають їм визначати і впроваджувати відповідні заходи для захисту своїх систем і даних від кіберзагроз. Вони також містять вказівки щодо реагування на кіберінциденти та забезпечення відповідальності для тих, хто не дотримується цих норм. Міжнародна організація зі стандартизації (International Organization for Standardization, ISO) розробила основні всесвітньо визнані стандарти з кібербезпеки, зокрема ISO 27001, ISO 27002, ISO 27031, ISO 27032, ISO 27701. Перелічені стандарти забезпечують основу для послідовного та економічно ефективного управління безпекою організацій, а також покликані допомогти організаціям захиститися від кібератак та управляти ризиками, пов'язаними з використанням технологій [16].

Європейський Союз також зробив значні кроки в регулюванні кіберзлочинності, зокрема, за допомогою Директиви про мережеву та

інформаційну безпеку («NIS Directive»), яка окреслює підхід ЄС до кібербезпеки, сприяючи співпраці між країнами ЄС для посилення заходів із кібербезпеки. Оскільки кіберзлочинці націлені на конфіденційні дані, Загальний регламент про захист персональних даних (GDPR) стає важливим правовим орієнтиром для кібербезпеки, який значно посилює захист персональної інформації в цифровій сфері, якщо його дотримуватися. Крім того, Група урядових експертів Організації Об'єднаних Націй (GGE) розробила набір норм для відповідальної поведінки держав у кіберпросторі. Зазначені норми включають принцип невтручання у внутрішні справи інших держав, заборону застосування сили та вимогу належної обачності при захисті критичної інфраструктури. Хоча вказані норми не є юридично обов'язковими, вони забезпечують цінну основу для країн, якої вони повинні дотримуватися у своїй кібердіяльності. Безсумнівно, підхід Сполучених Штатів до кібербезпеки слугує гідним прикладом системної та комплексної стратегії. Впровадження надійних стандартів безпеки, таких як National Institute of Standards and Technology Cybersecurity Framework (NIST CSF Cybersecurity Framework) виступає прикладом ефективного методу виявлення, реагування та попередження кіберінцидентів, який широко застосовується багатьма міжнародними приватними організаціями. «NIST CSF – це добровільна структура, яка надає набір стандартів, рекомендацій і найкращих практик для управління ризиками кібербезпеки». Структура допомагає організаціям виявляти, оцінювати ризики кібербезпеки та керувати ними структурованим і повторюваним способом. Структура не виступає обов'язковою, але вона все частіше приймається організаціями як добровільний захід для покращення стану кібербезпеки [3].

Також в США діє Федеральний закон про управління інформаційною безпекою (Federal Information Security Management Act, FISMA) – це федеральний закон США, прийнятий як Розділ III Закону про електронний уряд 2002 року. Вказаний Закон встановлює комплексні основи забезпечення безпеки інформації та інформаційних систем для всіх органів виконавчої влади. FISMA було запроваджено для посилення інформаційної безпеки у федеральних

агентствах, таких як NIST та Офіс управління та бюджету (Office of Management and Budget, OMB). Він вимагає від федеральних відомств впроваджувати програми інформаційної безпеки, щоб забезпечити конфіденційність, цілісність і доступність своєї інформації та IT-систем, у тому числі тих, що надаються або керуються іншими агенціями чи підрядниками [34]. В лютому 2016 року розробка Плану дій із національної безпеки в сфері кібербезпеки («Cybersecurity National Security Action Plan») підкреслила відданість країни боротьбі з кіберзагрозами. Крім того, окремі штати США демонструють значний прогрес у регулюванні кіберпростору, прикладом чого є Акт про повідомлення про порушення правил безпеки («Notice of Security Breach Act»), що діє в Каліфорнії. Цей закон зобов'язує компанії, які зазнають порушень безпеки, що стосуються особистої інформації жителів Каліфорнії, розкривати деталі інциденту, водночас пропонуючи компаніям гнучкість у виборі заходів безпеки, хоча і з санкціями за витік даних [3].

В Україні кібербезпека врегульовується на законодавчому рівні. Основними нормативними актами є Закон України «Про основні засади забезпечення кібербезпеки України» [22], Стратегія кібербезпеки України [24] та План реалізації Стратегії кібербезпеки України [23].

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», функціонування національної системи кібербезпеки, з-поміж іншого, забезпечується через «досягнення сумісності із відповідними стандартами Північноатлантичного альянсу і Євросоюзу», до того ж із врахуванням «ліпших світових практик та міжнародних стандартів із питань кібербезпеки і кіберзахисту» [22]. В аспекті додержання інформаційної безпеки це, відповідно до Закону (ст. 6,8), в себе включає в першу чергу розроблення на даній основі відповідних нормативно-правових актів, створення єдиної (універсальної) системи індикаторів кіберзагроз та впровадження національної системи аудиту інформаційної безпеки на критично вагомих об'єктах кіберзахисту. Окрім того, у статті 15 Закону зазначається, що головні суб'єкти національної кібербезпеки

теж підлягають аудиту, котрий повинен бути (а) незалежним, (б) щорічним та (в) здійснюватися «відповідно до міжнародних стандартів аудиту» [22].

Однак, незважаючи на існування цих глобальних стандартів і норм, все ще існують значні проблеми в забезпеченні їх дотримання. Багато країн продовжують ігнорувати ці норми, а ті, хто їх не дотримується, не несуть відповідальності. Питання атрибуції також є серйозною проблемою, оскільки буває важко визначити походження кібератаки.

Для подолання цих викликів необхідно посилити співпрацю між країнами і зробити більший акцент на підзвітності. Механізми співпраці та спільне розуміння атрибуції мають важливе значення для зменшення кількості, масштабу та ризику зловмисних кібератак. Крім того, міжнародне співтовариство має спільно працювати над встановленням чіткіших норм і наслідків за їх недотримання.

Глобальні стандарти і норми кібербезпеки здійснили значний вплив на етичні питання, які мають зв’язок з кіберпростором. Зазначені стандарти і норми допомогли створити основу і рамки для розуміння і подолання ризиків кібербезпеки, що сприяло міжнародному співробітництву і координації в питаннях кібербезпеки.

Однією з ключових етичних проблем, яку вирішили глобальні стандарти і норми кібербезпеки, є проблема юрисдикційної фрагментації. До створення глобальних стандартів і норм різні країни мали власні унікальні правові рамки і регуляторні режими, що регулювали кіберпростір. Це призводило до плутанини та неузгодженості при вирішенні транскордонних питань кібербезпеки. Глобальні стандарти і норми допомогли вирішити цю проблему, забезпечивши спільні рамки для розуміння і подолання ризиків кібербезпеки, незалежно від того, де вони виникають [55].

Ще одне етичне питання, яке вирішили глобальні стандарти і норми кібербезпеки, – це питання пропорційності. Пропорційність – це ідея про те, що відповіді на загрози кібербезпеці повинні бути пропорційними самій загрозі, а не вдаватися до надмірних або непотрібних заходів, які потенційно можуть

порушувати права людини або інші етичні принципи. Глобальні стандарти і норми сприяють забезпеченню пропорційності, встановлюючи чіткі керівні принципи і найкращі практики реагування на загрози кібербезпеці таким чином, щоб мінімізувати шкоду невинним сторонам [31].

Глобальні стандарти і норми кібербезпеки також допомогли вирішити етичну проблему недоторканності приватного життя. Недоторканність приватного життя є основоположним правом людини, якому часто загрожують заходи кібербезпеки, що передбачають збір та аналіз персональних даних. Глобальні стандарти і норми допомогли встановити обмеження на збір і використання персональних даних, а також сприяли розвитку технологій і методів, що зберігають конфіденційність.

Нарешті, глобальні стандарти і норми кібербезпеки допомогли підвищити підзвітність і прозорість у розробці та впровадженні заходів з кібербезпеки. Вказане є важливим задля забезпечення ефективності заходів з кібербезпеки, а також їх використання з дотриманням етичних принципів і цінностей. Підзвітність і прозорість можуть допомогти зміцнити довіру до заходів кібербезпеки та забезпечити їх використання відповідно до етичних принципів і цінностей [36].

Незважаючи на численні позитивні впливи глобальних стандартів і норм кібербезпеки на етичні питання, попереду ще багато викликів. Одним з головних викликів є забезпечення широкого прийняття та впровадження глобальних стандартів і норм. Багатьом країнам все ще бракує ресурсів і досвіду, необхідних для ефективного впровадження глобальних стандартів і норм кібербезпеки. Інший виклик полягає в тому, щоб йти в ногу зі швидким розвитком кіберпростору і постійною появою нових загроз кібербезпеці. Глобальні стандарти і норми повинні оновлюватися і переглядатися на регулярній основі, щоб випереджати ці загрози і забезпечувати їхню актуальність та ефективність [60].

Отже, глобальні стандарти і норми кібербезпеки мають значний вплив на етичні питання, пов’язані з кіберпростором. Вони допомогли створити спільну

мову і рамки для розуміння і подолання ризиків кібербезпеки, сприяють пропорційності, захисту приватного життя, а також підвищенню підзвітності та прозорості. Незважаючи на досягнутий прогрес, попереду ще багато викликів, пов'язаних із забезпеченням широкого прийняття і впровадження глобальних стандартів і норм, а також з необхідністю йти в ногу зі швидкою еволюцією кіберпростору. Тим не менш, встановлення глобальних стандартів і норм кібербезпеки є важливим кроком на шляху до створення більш безпечного і захищеного кіберсередовища, яке поважає етичні принципи і цінності. Існують різні міжнародні керівні принципи та рамки, які визначають етичні стандарти кібербезпеки, такі як Рамки кібербезпеки Національного інституту стандартів і технологій (NIST), Загальний регламент захисту даних Європейського Союзу (GDPR) і стандарти Міжнародної організації зі стандартизації (ISO). Ці керівні принципи забезпечують базову основу для етичних практик кібербезпеки і допомагають організаціям орієнтуватися в складному ландшафті загроз і ризиків кібербезпеки. Досягнення балансу між глобальними стандартами кібербезпеки та етичними міркуваннями залишається суттєвим викликом, що вимагає постійної оцінки та адаптації для вирішення етичних проблем, які виникають у цифровому середовищі.

1.3. Інтеграція етичних норм у протоколи та практики кібербезпеки

Етичні норми у сфері кібербезпеки – це керівні принципи та настанови, які визначають поведінку та прийняття рішень фахівцями та організаціями у сфері кібербезпеки з метою захисту суспільства, споживачів та цифрової інфраструктури від шкоди. Ці стандарти допомагають гарантувати, що фахівці з кібербезпеки діють доброчесно, з повагою до приватного життя та відданістю справі захисту вразливих верств населення [36].

Узагальнимо ключові етичні норми в галузі кібербезпеки на рис. 1.2.

1) Відповідальне розкриття інформації	• принцип заохочує науковців і фахівців з кібербезпеки відповідально повідомляти про виявлені вразливості постраждалим сторонам, дозволяючи їм виправити проблему до того, як деталі будуть оприлюднені
2) Конфіденційність	• ця концепція наголошує на інтеграції міркувань конфіденційності в дизайн і розробку програмного, апаратного забезпечення та послуг з самого початку
3) Безпека	• подібно до принципу конфіденційності за замовчуванням, цей принцип зосереджується на впровадженні безпеки на кожному етапі процесу розробки.
4) Прозорість	• робота фахівців з кібербезпеки повинні бути прозорими щодо своїх методів, інструментів та намірів
5) Інформована згода	• користувачі повинні бути повністю поінформовані про те, які дані збираються, як вони будуть використовуватися і хто має до них доступ
6) Анонімність і псевдонімність	• коли це можливо, фахівці з кібербезпеки повинні використовувати анонімні або псевдонімні ідентифікатори для захисту конфіденційності користувачів
7) Мінімізація шкоди	• фахівці з кібербезпеки завжди повинні прагнути мінімізувати шкоду для окремих осіб, організацій та суспільства в цілому
8) Професіоналізм	• фахівці з кібербезпеки повинні діяти професійно, дотримуючись найкращих галузевих практик, бути в курсі нових технологій та загроз, а також постійно розвивати свої навички
9) Дотримання законів та нормативних актів	• організації повинні дотримуватися відповідних законів і правил щодо захисту даних, конфіденційності та кібербезпеки
10) Постійний моніторинг та вдосконалення	• фахівці з кібербезпеки повинні регулярно переглядати та оновлювати свої процеси, інструменти та протоколи, щоб адаптуватися до нових загроз і технологій

Рис. 1.2. Ключові етичні норми в галузі кібербезпеки

Джерело: побудовано автором за даними [33]

Отже, глобальні стандарти і норми у сфері кібербезпеки мають вирішальне значення для забезпечення захисту критичної інфраструктури, запобігання кібератакам і підтримання міжнародного миру і стабільності. Незважаючи на те, що стандарти і норми вже існують, ще багато роботи потрібно зробити для забезпечення їх дотримання та підзвітності. Посилюючи співпрацю і приділяючи

більше уваги підзвітності, можливо створити безпечніше і надійніше кіберсередовище для всіх.

Глобальні стандарти та норми кібербезпеки суттєво впливають на етичні питання в цифровій сфері, формуючи поведінку, практики та суспільні очікування. Ці стандарти слугують керівними принципами, що диктують відповідальну поведінку у захисті цифрових активів, впливаючи на етичні міркування в практиці кібербезпеки в усьому світі. Дотримання етичних стандартів у сфері кібербезпеки є життєво важливим для завоювання та збереження довіри клієнтів, партнерів та зацікавлених сторін. Дотримуючись цих норм, фахівці з кібербезпеки можуть продемонструвати свою відданість захисту конфіденційної інформації та збереженню цілісності цифрової екосистеми.

Інтеграція етичних норм в протоколи та практики кібербезпеки є критично важливим аспектом забезпечення відповідності зусиль організацій з кібербезпеки їхнім цінностям та принципам. Цей процес включає кілька кроків, які організації повинні зробити, щоб забезпечити інтеграцію етичних міркувань у свої політики, процедури та практики кібербезпеки (рис. 1.3).

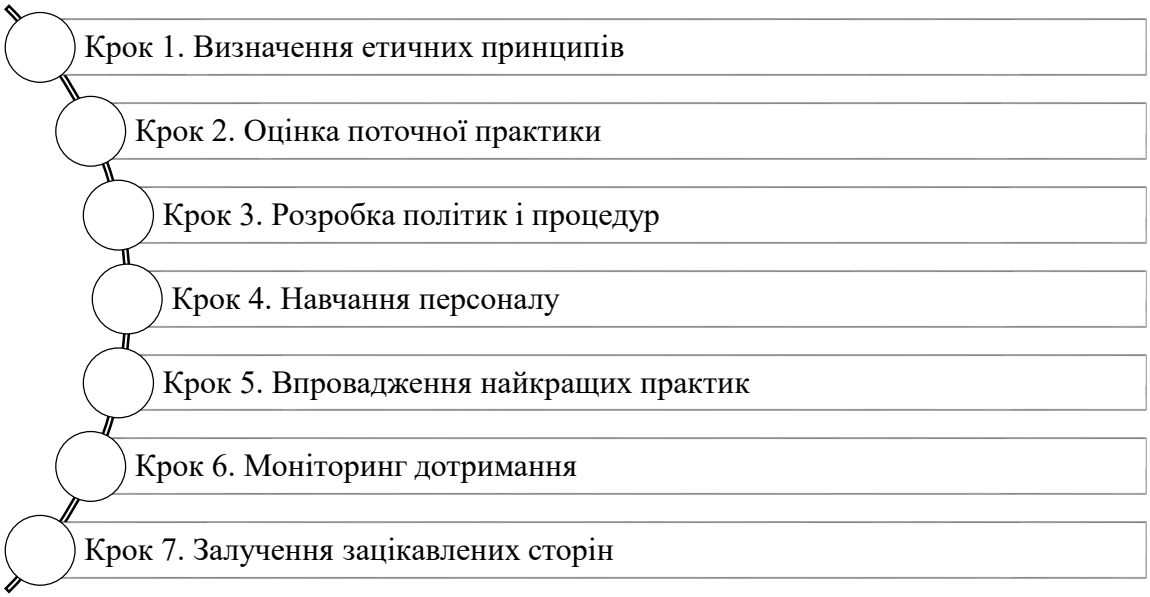

Рис. 1.3. Етапи процесу інтеграції етичних норм у протоколи та практики кібербезпеки

Джерело: побудовано автором за даними [31]

Першим кроком до інтеграції етики в протоколи та практики кібербезпеки є визначення етичних принципів, якими організація має керуватися у своїй діяльності з кібербезпеки. Це включає вироблення чіткого розуміння цінностей і принципів організації, пов’язаних з конфіденційністю, захистом даних, управлінням безпекою та іншими відповідними сферами. Ці принципи повинні бути задокументовані та доведені до відома всіх зацікавлених сторін, які беруть участь у заходах з кібербезпеки.

Після визначення етичних принципів організації повинні провести оцінку своїх поточних практик кібербезпеки, щоб визначити сфери, в яких етичні міркування дотримуються, і сфери, які потребують вдосконалення. Ця оцінка повинна охоплювати політики, процедури, системи та команди, щоб переконатися, що вони відповідають визначеним етичним принципам [9].

На основі оцінки, проведеної на Кроці 2, організації повинні розробити політику та процедури, які включають етичні міркування. Наприклад, політика конфіденційності даних повинна визначати, як збираються, обробляються, зберігаються та поширюються персональні дані, а також забезпечувати дотримання прав осіб на приватне життя. Аналогічно, політика управління безпекою повинна гарантувати, що рішення щодо безпеки приймаються відповідно до етичних принципів, таких як прозорість, підзвітність і справедливість [55].

Навчання персоналу етичним аспектам кібербезпеки має важливе значення для того, щоб кожен, хто бере участь у забезпеченні кібербезпеки, розумів свою роль у дотриманні етичних принципів. Навчання має охоплювати такі теми, як конфіденційність даних, управління безпекою та етичне хакерство, а також підкреслювати важливість дотримання етики в усіх аспектах роботи з кібербезпеки.

Організації повинні впроваджувати найкращі практики кібербезпеки, які відповідають етичним принципам. Наприклад, впровадження технологій шифрування для захисту конфіденційних даних демонструє прихильність до захисту приватного життя людей. Аналогічно, впровадження двофакторної

автентифікації допомагає забезпечити доступ до конфіденційних систем і даних лише уповноваженому персоналу [60].

Моніторинг дотримання етичних принципів має важливе значення для забезпечення того, щоб організації дотримувалися визначених ними етичних принципів протягом тривалого часу. Цей моніторинг повинен охоплювати всі аспекти діяльності з кібербезпеки, включаючи розробку політики, впровадження систем та роботу персоналу. Необхідно проводити регулярні аудити та оцінки для виявлення сфер, які потребують вдосконалення [59].

Залучення зацікавлених сторін до етичних міркувань у сфері кібербезпеки має вирішальне значення для забезпечення інтеграції етичних принципів у протоколи та практики кібербезпеки. Зацікавлені сторони повинні включати працівників, клієнтів, партнерів та постачальників, на яких впливають заходи з кібербезпеки. Організації повинні інформувати зацікавлені сторони про свої етичні принципи і практики та запитувати зворотній зв’язок, щоб покращити свій підхід до етичної кібербезпеки. Інтеграція етики в протоколи і практики кібербезпеки – це безперервний процес, який вимагає постійних зусиль і уваги. Дотримуючись семи кроків, описаних вище, організації можуть гарантувати, що їхні зусилля з кібербезпеки відповідають їхнім цінностям і принципам, і що вони виконують свої етичні зобов’язання перед зацікавленими сторонами. Зрештою, інтеграція етики в протоколи і практики кібербезпеки має важливе значення для побудови довіри і авторитету в сучасну цифрову епоху.

РОЗДІЛ 2
ЕТИЧНІ ВИКЛИКИ ТА ПРОБЛЕМИ В КІБЕРБЕЗПЕЦІ

2.1. Аналіз основних етичних викликів та проблем, що виникають в управлінні кібербезпекою

Управління кібербезпекою стикається з безліччю етичних проблем і питань, які можуть мати значні наслідки для організацій, окремих осіб і суспільства в цілому. Найбільш актуальними етичними проблемами в управлінні кібербезпекою є наступні:

1) баланс між безпекою та конфіденційністю;

2) право власності на дані та контроль над ними;

3) заходи протидії кібератакам;

4) оприлюднення вразливостей;

5) управління ризиками ланцюга постачання;

6) штучний інтелект і машинне навчання;

7) людський фактор.

Однією з основних етичних проблем в управлінні кібербезпекою є досягнення балансу між безпекою та конфіденційністю. Організаціям необхідно збирати і аналізувати величезні обсяги даних для виявлення і запобігання кіберзагрозам, але це може викликати серйозні занепокоєння щодо конфіденційності. Фахівці з кібербезпеки повинні орієнтуватися в складних правових та етичних рамках, щоб гарантувати, що вони захищають особисте життя, одночасно захищаючи національну безпеку та активи організації [31].

Зі збільшенням обсягу даних, що генеруються, питання власності та контролю над ними стають все більш актуальними. Фахівці з кібербезпеки повинні вирішувати такі питання, як суверенітет даних, локалізація даних і угоди про обмін даними, одночасно забезпечуючи дотримання своїх етичних зобов’язань щодо захисту конфіденційної інформації.

Фахівці з кібербезпеки іноді змушені вдаватися до контрзаходів, які можуть бути сприйняті як неетичні, наприклад, здійснювати контрнапади або використовувати тактику обману для введення в оману супротивників. Такі заходи можуть розмити межі між нападом і захистом, що ускладнює визначення того, чи є вони етичними, чи ні [58].

Коли виявляють вразливості, фахівці з кібербезпеки стикаються з етичною дилемою щодо того, чи розголошувати їх публічно, чи тримати в таємниці. Публічне розкриття може чинити тиск на постачальників для швидкого виправлення вразливостей, але це також може наразити організації на потенційні атаки до того, як буде доступне виправлення. Зберігання вразливостей у таємниці може залишити організації відкритими для атак, але також може дати їм час на усунення проблеми до того, як вразливість буде використана.

Управління ризиками ланцюга постачання є ще одним етичним викликом в управлінні кібербезпекою. Фахівці з кібербезпеки повинні переконатися, що сторонні постачальники та підрядники не створюють ризиків для кібербезпеки їхньої організації. Однак це може бути складно зробити, працюючи з постачальниками, які можуть мати обмежені можливості кібербезпеки або не бажати інвестувати в надійні заходи кібербезпеки [28].

Зростаюче використання штучного інтелекту та машинного навчання в кібербезпеці створює етичні проблеми, пов’язані з упередженістю, пояснюваністю та підзвітністю. Алгоритми штучного інтелекту та машинного навчання можуть увічнити упередження, якщо їх навчати на упереджених даних, що призводить до несправедливого ставлення до певних груп. Крім того, складність цих алгоритмів може ускладнити пояснення процесів прийняття ними рішень, що ставить під сумнів підзвітність і прозорість [37].

Нарешті, управління кібербезпекою повинно враховувати людські фактори, такі як втома, стрес і вигорання. Від фахівців з кібербезпеки часто очікують, що вони працюватимуть довгі години в умовах високого рівня стресу, що може призвести до помилок і зниження ефективності. Організації повинні надавати пріоритет благополуччю своїх команд кібербезпеки, щоб гарантувати,

що вони зможуть працювати з максимальною віддачею і приймати обґрунтовані етичні рішення [31].

Розглянемо більш детально таку проблему, що виникає в процесі управління кібербезпекою як протидія кібератакам. Однією з найважливіших етичних проблем в управлінні кібербезпекою є визначення належного балансу між захистом від кіберзагроз і повагою до приватного життя та громадянських свобод. Заходи протидії кібератакам мають важливе значення для запобігання та пом'якшення наслідків витоків даних та інших видів кібератак, які можуть скомпрометувати конфіденційну інформацію та завдати шкоди окремим особам та організаціям. Однак деякі контрзаходи можуть потенційно порушувати право на приватність і громадянські свободи, особливо коли вони пов'язані з моніторингом і спостереженням [33].

Наприклад, розгортання систем виявлення вторгнень, які відстежують мережевий трафік та електронну пошту, може допомогти виявити та запобігти зловмисній діяльності. Однак такий моніторинг може також викликати занепокоєння щодо конфіденційності працівників, оскільки він може перехоплювати особисті повідомлення та дані, не пов'язані з робочими цілями. Аналогічно, впровадження біометричних методів автентифікації, таких як розпізнавання обличчя або сканування відбитків пальців, може посилити безпеку, але також може викликати занепокоєння щодо конфіденційності та потенційного зловживання конфіденційними біометричними даними.

Ще однією етичною проблемою, пов'язаною з протидією кібератакам, є використання штучного інтелекту та алгоритмів машинного навчання для прогнозування та реагування на кіберзагрози. Ці інструменти можуть аналізувати величезні обсяги даних для виявлення закономірностей і аномалій, що вказують на зловмисну діяльність. Однак вони також можуть призводити до упередженості та дискримінації, якщо навчаються на неповних, незбалансованих або упереджених наборах даних. Наприклад, системи зі штучним інтелектом, призначені для виявлення шахрайських транзакцій, можуть ненавмисно

орієнтуватися на певні групи на основі демографічних характеристик, а не фактичної підозрілої поведінки [28].

Крім того, використання наступальних контрзаходів, таких як хакерські атаки на зловмисників або застосування тактики обману, викликає додаткові етичні питання. Хоча ці заходи можуть допомогти стримати або зірвати ворожі атаки, вони також можуть розмити межі між нападом і захистом, потенційно наражаючи організації на ризик порушення законів і моральних принципів. Участь у таких заходах може підірвати довіру та авторитет як всередині організації, так і в ширшій спільноті кібербезпеки.

Щоб вирішити ці етичні проблеми, організації повинні розробити комплексну політику і керівні принципи, які враховують питання конфіденційності та громадянської свободи, але водночас захищають від кіберзагроз. Вони повинні брати участь у прозорих дискусіях із зацікавленими сторонами щодо обґрунтування своїх стратегій протидії та постійно оцінювати ефективність і потенційні негативні наслідки своїх підходів. Крім того, організації повинні інвестувати в постійне навчання та підвищення кваліфікації свого персоналу з кібербезпеки, приділяючи особливу увагу не лише технічним навичкам, але й етичній обізнаності та навичкам прийняття рішень [37].

Заходи протидії кібератакам представляють складну етичну дилему для управління кібербезпекою. Пошук правильного балансу між безпекою і конфіденційністю вимагає ретельного врахування різних факторів, включаючи дотримання законодавства, очікування зацікавлених сторін і етичні принципи. Визнаючи та вирішуючи ці етичні проблеми, організації можуть краще захистити свої активи та зберегти довіру клієнтів і партнерів, дотримуючись при цьому своїх соціальних зобов’язань.

Сьогодні штучний інтелект (Artificial Intelligence, AI) та машинне навчання (Machine Learning, ML) стають все більш популярними інструментами кібербезпеки завдяки їх здатності виявляти і запобігати кібератакам більш ефективно і результативно, ніж традиційні методи. Однак застосування

штучного інтелекту (ШІ) та машинного навчання (МН) в кібербезпеці також викликає етичні проблеми, які необхідно вирішувати [62].

До однієї із головних етичних проблем, які пов’язані із використанням ШІ та МН у кібербезпеці, є потенціал упередженості та дискримінації. Алгоритми ШІ та МН настільки хороші, наскільки хороші дані, на яких вони навчаються, і якщо дані містять упередження або стереотипи, алгоритм, швидше за все, буде давати упереджені або дискримінаційні результати. Наприклад, система штучного інтелекту, призначена для виявлення шахрайських транзакцій, може ненавмисно націлитися на певні групи на основі демографічних характеристик, а не фактичної підозрілої поведінки [49].

Ще однією етичною проблемою є недостатня прозорість алгоритмів штучного інтелекту та машинного навчання. На відміну від людей-аналітиків, алгоритми ШІ та МН не надають чітких пояснень своїм рішенням, що ускладнює розуміння того, чому були зроблені ті чи інші дії. Така непрозорість може призвести до недовіри та складнощів у виявленні та виправленні помилок або упередженості алгоритмів.

Конфіденційність – ще одна сфера, яка викликає занепокоєння, коли йдеться про використання ШІ та МН у кібербезпеці. Для ефективної роботи алгоритми ШІ та МН часто потребують великих обсягів даних, що може викликати занепокоєння щодо конфіденційності та захисту даних. Крім того, використання ШІ та МН у кібербезпеці може вимагати збору та обробки персональних даних, що викликає додаткові етичні занепокоєння щодо захисту даних та конфіденційності [62].

Нарешті, існує також питання підзвітності та відповідальності. Оскільки алгоритми ШІ та МН стають все більш автономними, може бути важко визначити, хто несе відповідальність, коли щось йде не так. Розробник, який створив алгоритм? Користувач, який його розгорнув? Чи сам алгоритм? Встановлення чітких меж підзвітності та відповідальності має важливе значення для забезпечення етичного та відповідального використання ШІ та МН у сфері кібербезпеки [58].

Щоб вирішити ці етичні проблеми, організації повинні розробити комплексну політику і керівні принципи, які враховують питання конфіденційності та громадянської свободи, але водночас захищають від кіберзагроз. Вони повинні брати участь у прозорих дискусіях із зацікавленими сторонами щодо обґрунтування своїх стратегій протидії та постійно оцінювати ефективність і потенційні негативні наслідки своїх підходів. Крім того, організаціям слід інвестувати в постійне навчання та підвищення кваліфікації персоналу з кібербезпеки, приділяючи особливу увагу не лише технічним навичкам, але й етичній обізнаності та навичкам прийняття рішень.

Загалом, використання ШІ та МН в кібербезпеці створює численні етичні проблеми, які необхідно вирішувати. Усвідомлюючи ці проблеми та вживаючи заходів для їх вирішення, організації можуть забезпечити етичність, відповідальність та ефективність використання ШІ та МН у сфері кібербезпеки.

Таким чином, управління кібербезпекою стикається з численними етичними проблемами, які вимагають ретельного розгляду і навігації. Від балансу між конфіденційністю та безпекою до управління ризиками ланцюгів постачання, фахівці з кібербезпеки повинні приймати складні рішення, які можуть мати далекосяжні наслідки. Надаючи пріоритет етичним міркуванням і застосовуючи проактивний підхід до вирішення цих проблем, організації можуть зміцнити довіру, захистити свої активи, а також забезпечити безпеку і благополуччя своїх зацікавлених сторін.

Крім того, фахівці з кібербезпеки повинні визнавати важливість етики у своїй повсякденній роботі та активно шукати ресурси і рекомендації, які допоможуть їм вирішувати етичні дилеми. Це включає в себе постійне ознайомлення з галузевими правилами та стандартами, співпрацю з колегами та наставниками, а також участь у постійному навчанні та освіті. Організації повинні створити культуру, яка цінує етику та підтримує прийняття етичних рішень. Це включає розробку чітких політик і керівних принципів, надання ресурсів і підтримки етичним ініціативам, а також заохочення відкритого спілкування і співпраці між членами команди.

Зрештою, інтеграція етики в протоколи і практики кібербезпеки має важливе значення для зміцнення довіри, захисту активів, а також забезпечення безпеки і добробуту зацікавлених сторін. Надаючи пріоритет етичним міркуванням і застосовуючи проактивний підхід до вирішення етичних проблем, організації можуть створити міцний фундамент для своїх програм кібербезпеки і сприяти створенню більш безпечного і захищеного цифрового середовища.

2.2 Розгляд міжнародних стандартів, які включають етичні аспекти в управління кібербезпекою, їх зміст та вимоги

У постійно мінливому ландшафті управління кібербезпекою міжнародні стандарти відіграють ключову роль у формуванні етичних рамок і керівних принципів захисту цифрових активів. Ці стандарти надають організаціям всеосяжний план для створення надійних практик інформаційної безпеки, неявно інтегруючи етичні міркування в їхні рамки. У цьому контексті ряд міжнародно визнаних стандартів прямо стосуються етичних аспектів, закладаючи основу для відповідального та етичного управління кібербезпекою.

Як уже було згадано, міжнародна організація зі стандартизації (International Organization for Standardization, ISO) розробила основні всесвітньо визнані стандарти з кібербезпеки, зокрема ISO 27001, ISO 27002, ISO 27031, ISO 27032, ISO 27701.

Розглянемо кожен з окреслених стандартів більш детально.

ISO/IEC 27001 – це міжнародний стандарт інформаційної безпеки, який забезпечує основу для управління конфіденційною інформацією компанії. Стандарт містить вимоги до розробки системи управління інформаційною безпекою (СУІБ), впровадження засобів контролю безпеки та проведення оцінки ризиків. Структура стандарту розроблена, щоб допомогти організаціям керувати своїми методами безпеки в одному місці, послідовно та економічно ефективно [34].

Хоча стандарт ISO/IEC 27001 не заглиблюється в етичні аспекти управління кібербезпекою, він забезпечує основу, яка по суті включає етичні міркування як частину його впровадження. Стандарт описує системний підхід до створення, впровадження, підтримки та постійного вдосконалення СУІБ в організації.

Зміст і вимоги ISO/IEC 27001 охоплюють кілька ключових елементів:

- визначення сфери застосування та контексту – стандарт вимагає, щоб організації визначали сферу застосування своєї СУІБ, враховуючи контекст організації, її профіль ризиків, законодавчі та регуляторні вимоги, а також потреби та очікування зацікавлених сторін;

- оцінка та управління ризиками – ISO/IEC 27001 наголошує на ідентифікації ризиків інформаційної безпеки та впровадженні відповідних засобів контролю для управління та зменшення цих ризиків. Це передбачає оцінку загроз, вразливостей та потенційного впливу інцидентів безпеки;

- політика та цілі – організації повинні сформулювати політику інформаційної безпеки, узгоджену з їхніми бізнес-цілями, і визначити вимірювані цілі безпеки. Ця політика повинна відображати етичні міркування, такі як повага до приватності, захист даних і дотримання правових та етичних стандартів;

- впровадження засобів контролю – стандарт надає вичерпний перелік засобів контролю безпеки, розподілених на 14 областей, включаючи такі сфери, як контроль доступу, криптографія, фізична безпека, управління інцидентами тощо. Ці засоби слугують основою для організацій для вирішення етичних аспектів кібербезпеки, таких як захист даних, конфіденційність та цілісність;

- постійне вдосконалення – ISO/IEC 27001 наголошує на необхідності постійного вдосконалення, що передбачає регулярний перегляд, моніторинг та оцінку СУІБ для забезпечення її ефективності, відповідності правовим та етичним вимогам, а також узгодження з цілями організації [41].

Стандарти ISO 27001 та ISO 27001 були опубліковані у 2013 році ISO (Міжнародна організація стандартизації) та IEC (Міжнародна електротехнічна

комісія) і належать до сімейства стандартів ISO 27000. ISO 27001 – це єдиний міжнародно визнаний стандарт інформаційної безпеки, який підлягає сертифікації. ISO 27001 підтримується кодексом правил керування інформаційною безпекою, ISO/IEC 27002:2013, який пояснює, як запроваджувати інформацію засоби контролю безпеки для керування ризиками інформаційної безпеки [45].

ISO/IEC 27001:2022 та ISO/IEC 27002:2022 – найновіші версії ISO 27001 та ISO 27002 – були опубліковані в жовтні 2022 року. Організації, які сертифіковані відповідно до ISO/IEC 27001:2013 та ISO/IEC 27002:2013, мають трирічний перехідний період для внесення необхідних змін до своєї СУІБ (системи управління інформаційною безпекою) [42].

Хоча стандарт ISO/IEC 27001 не містить чітких етичних настанов, він за своєю суттю сприяє етичній поведінці в управлінні кібербезпекою, акцентуючи увагу на захисті конфіденційної інформації, повазі до приватного життя, забезпеченні конфіденційності та дотриманні правових і регуляторних вимог. Дотримання принципів, викладених у цьому стандарті, заохочує етичну поведінку в управлінні кібербезпекою в організаціях, сприяючи зміцненню довіри, доброчесності та відповідальному поводженню з інформацією.

ISO/IEC 27002, раніше відомий як ISO/IEC 17799, є міжнародно визнаним стандартом, який зосереджується на контролі та керівних принципах інформаційної безпеки. Хоча він не містить чітких вказівок на етичні аспекти в управлінні кібербезпекою, він слугує додатковим документом до ISO/IEC 27001 (стандарт для систем управління інформаційною безпекою – СУІБ), надаючи вказівки щодо впровадження засобів контролю, зазначених в ISO/IEC 27001 [41].

Зміст ISO/IEC 27002 охоплює всеосяжний набір керівних принципів і найкращих практик для контролю інформаційної безпеки, структурованих у різних сферах:

- політика інформаційної безпеки – він охоплює настанови щодо розробки та підтримки політики інформаційної безпеки, узгодженої з цілями організації та законодавчими вимогами;

- організація інформаційної безпеки – цей розділ присвячений визначенню обов’язків зацікавлених сторін, створенню структури управління інформаційною безпекою та забезпеченню належних програм навчання та підвищення обізнаності;

- безпека людських ресурсів – настанови щодо відбору, навчання та управління персоналом для забезпечення дотримання ним політики безпеки та етичних стандартів при роботі з інформаційними активами;

- управління активами – зосереджується на інвентаризації та класифікації інформаційних активів, визначенні права власності та впровадженні відповідних заходів захисту з урахуванням їхньої чутливості;

- контроль доступу – детальна інформація про контроль доступу до інформаційних систем і даних, включаючи управління доступом користувачів, автентифікацію, авторизацію та розподіл обов’язків;

- криптографія – інструкції щодо впровадження криптографічного контролю для забезпечення конфіденційності, цілісності та автентичності конфіденційної інформації;

- фізична та екологічна безпека – охоплює заходи для захисту фізичної інфраструктури, обладнання та приміщень, де зберігається або обробляється інформація;

- операційна безпека – охоплює безпечні операційні практики, включаючи управління змінами, управління інцидентами, резервне копіювання та обслуговування системи;

- безпека комунікацій – настанови щодо захисту мережі та каналів зв’язку для захисту інформації під час передачі;

- придбання, розробка та обслуговування систем – надає рекомендації щодо безпечної розробки програмного забезпечення, відносин з постачальниками та процесів придбання систем;

- управління інцидентами – настанови щодо своєчасного та ефективного виявлення інцидентів безпеки, повідомлення про них та реагування на них;

- управління безперервністю бізнесу – розглядає планування та реалізацію стратегій для забезпечення безперервності критично важливих бізнес-операцій під час і після руйнівних інцидентів [39].

Стандарт ISO/IEC 27002, хоча і не фокусується безпосередньо на етичних міркуваннях, опосередковано сприяє етичній поведінці, забезпечуючи структурований підхід до впровадження засобів контролю інформаційної безпеки. Його настанови по суті сприяють розвитку етичних практик в управлінні кібербезпекою, наголошуючи на захисті конфіденційної інформації, повазі до приватного життя та дотриманні законодавчих і регуляторних вимог.

ISO/IEC 27031:2011 – це міжнародний стандарт, спеціально орієнтований на інформаційні технології – методи забезпечення безпеки – настанови щодо готовності інформаційно-комунікаційних технологій (ІКТ) до безперервності бізнесу. Він містить вказівки щодо того, як організації можуть використовувати ІКТ для захисту своїх бізнес-операцій і забезпечення безперервності в разі інциденту або катастрофи. Досягнення відповідності стандарту ISO 27031 допомагає організаціям зрозуміти загрози ІКТ-послугам, забезпечуючи їх безпеку в разі незапланованого інциденту [48]. Хоча в першу чергу він розглядає безперервність бізнесу в контексті ІКТ, він опосередковано включає в себе етичні міркування в рамках своєї структури.

Зміст стандарту ISO/IEC 27031 зосереджений на наданні керівних принципів та найкращих практик для забезпечення готовності інформаційно-комунікаційних технологій до безперервності бізнесу. У ньому викладено різні аспекти та вимоги для підтримки організацій у підготовці та підтримці систем ІКТ для забезпечення їхньої стійкості до збоїв та катастроф.

Ключові компоненти та вимоги ISO/IEC 27031 включають:

- стратегія безперервності бізнесу – розробка комплексної стратегії, що узгоджує системи ІКТ із загальними планами безперервності бізнесу для забезпечення безперервності критично важливих бізнес-функцій;

- розуміння потреб організації – оцінка потреб організації, визначення критично важливих ІКТ-ресурсів, залежностей та визначення пріоритетності послуг для ефективного управління потенційними збоями;

- управління ризиками ІКТ – виявлення та оцінка ризиків, які можуть вплинути на системи ІКТ та бізнес-операції, включно з оцінкою вразливостей та загроз для забезпечення належного зменшення ризиків;

- безперервність та доступність послуг ІКТ – забезпечення безперервної доступності послуг ІКТ під час і після збоїв, включаючи резервне копіювання даних, заходи з резервування та відмовостійкість;

- аналіз впливу на бізнес – проведення оцінок для визначення потенційного впливу збоїв на системи ІКТ та бізнес-операції, що дозволяє планувати ефективне реагування та відновлення;

- реагування на інциденти та відновлення – розробка процедур реагування на інциденти та планів відновлення для мінімізації часу простою, мінімізації збитків та швидкого відновлення послуг ІКТ;

- тестування та обслуговування – регулярне тестування та підтримка планів безперервності ІКТ, проведення навчань та перегляд процедур для забезпечення їх ефективності та актуальності [43].

Хоча стандарт ISO/IEC 27031 прямо не фокусується на етичних аспектах, він опосередковано підкреслює етичні міркування, сприяючи стійкості та цілісності систем ІКТ, забезпечуючи безперервність критично важливих послуг та захищаючи конфіденційну інформацію. Підтримуючи готовність ІКТ до безперервності бізнесу, організації роблять свій внесок в етичні практики кібербезпеки, захищаючи дані, поважаючи конфіденційність користувачів та забезпечуючи цілісність і доступність основних послуг. Етична поведінка є невід’ємною частиною стандарту, спрямованого на підтримання операційної стійкості та здатності відновлюватися після руйнівних інцидентів, що сприяє відповідальному управлінню кібербезпекою.

ISO/IEC 27032:2012 – це міжнародно визнаний стандарт, який безпосередньо стосується кібербезпеки та надає настанови щодо стратегій і

політик кібербезпеки в ширшому контексті управління інформаційною безпекою. Стандарт розроблений, щоб допомогти організаціям захистити себе від кібератак і керувати ризиками, пов’язаними з використанням технологій. Він заснований на підході до управління ризиками та надає вказівки щодо визначення, оцінки та управління кіберризиками. Стандарт також містить вказівки щодо реагування на інциденти та відновлення [10]. Останнє оновлення стандарту ISO/IEC 27032 відбулось у 2023 році.

Зміст ISO/IEC 27032 включає в себе такі напрямки:

- огляд кібербезпеки – стандарт пропонує комплексне розуміння кібербезпеки, підкреслюючи важливість управління ризиками, пов’язаними з кіберзагрозами та атаками в цифровому ландшафті;

- розробка політики кібербезпеки – посібник з розробки політики та стратегій кібербезпеки, узгоджених з цілями організації, законодавчими та нормативними вимогами, а також найкращими галузевими практиками;

- інформування та навчання з кібербезпеки – рекомендації щодо створення інформаційних та навчальних програм для інформування зацікавлених сторін, працівників та користувачів про ризики кібербезпеки, найкращі практики та їхню роль у підтримці безпечного цифрового середовища;

- управління інцидентами кібербезпеки – встановлення процедур і протоколів для виявлення, реагування та відновлення після інцидентів кібербезпеки, підкреслюючи важливість своєчасного та ефективного реагування для мінімізації збитків;

- співпраця і взаємодія – заохочення співпраці та обміну інформацією між зацікавленими сторонами, в тому числі урядами, організаціями та окремими особами, з метою посилення стійкості до кібербезпеки та можливостей реагування;

- етичні міркування – хоча етичні міркування чітко не окреслені, вони пронизують стандарт, зосереджуючи увагу на захисті критично важливих інформаційних активів, повазі до приватного життя користувачів і забезпеченні цілісності цифрової комунікації. Наголос на відповідальній поведінці в

управлінні ризиками кібербезпеки опосередковано сприяє етичній поведінці в практиці кібербезпеки [44].

Вимоги стандарту ISO/IEC 27032 стосуються сприяння комплексному підходу до кібербезпеки, підкреслюючи важливість політик, стратегій, обізнаності, співпраці та управління інцидентами для ефективного подолання ризиків кібербезпеки. Хоча стандарт не містить чіткого визначення етичних аспектів, його спрямованість на захист інформаційних активів, підвищення обізнаності та сприяння співпраці опосередковано сприяє етичним практикам кібербезпеки. Етичні міркування неявно простежуються в акценті стандарту на відповідальній поведінці та розробці стратегій захисту цифрових активів і підтримці довіри зацікавлених сторін у цифровій сфері.

ISO/IEC 27701 визначає вимоги до системи управління конфіденційною інформацією (privacy information management system, PIMS) на основі вимог ISO 27001. Він розширений набором вимог щодо конфіденційності, цілей контролю та засобів контролю. Організації, які запровадили ISO 27001, можуть використовувати ISO 27701, щоб розширити свої зусилля щодо безпеки й охопити керування конфіденційністю [34]. Хоча стандарт не фокусується безпосередньо на етичних аспектах управління кібербезпекою, він розглядає проблеми, пов’язані з конфіденційністю, і за своєю суттю охоплює етичні міркування в рамках цього стандарту.

ISO 27701:2019 (повна назва: ISO/IEC 27701 Методи безпеки – Розширення до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційною інформацією – Вимоги та рекомендації) – це стандарт управління, опублікований у 2019 році у відповідь на зростаючу потребу в глобальна структура конфіденційності даних [25].

Зміст та вимоги стандарту ISO/IEC 27701 включають:

- система управління інформацією про конфіденційність (PIMS) – стандарт розширює вимоги та настанови ISO/IEC 27001 та ISO/IEC 27002, щоб конкретно розглянути управління конфіденційністю в рамках СУІБ організації. Стандарт

інтегрується з цими існуючими системами управління інформаційною безпекою та додає засоби контролю, пов’язані з конфіденційністю;

- захист персональних даних – ISO/IEC 27701 наголошує на захисті персональної інформації шляхом впровадження засобів контролю та заходів для забезпечення її конфіденційності, цілісності, доступності та недоторканності відповідно до чинних законів та нормативних актів;

- ролі та обов’язки – визначає ролі та обов’язки в організації щодо управління процесами, пов’язаними з конфіденційністю, включаючи співробітників із захисту даних, відповідальних за конфіденційність та інших зацікавлених осіб, які беруть участь в обробці персональних даних;

- управління ризиками для конфіденційності – подібно до ISO/IEC 27001, ISO/IEC 27701 вимагає від організацій проводити оцінку ризиків, спеціально зосереджену на ризиках для конфіденційності, забезпечуючи впровадження адекватних засобів контролю та заходів для зменшення цих ризиків;

- права суб’єктів даних – стандарт містить положення щодо управління правами суб’єктів даних, включаючи процедури обробки запитів на доступ, виправлення, видалення та інші запити, пов’язані з персональними даними;

- конфіденційність за задумом і за замовчуванням – заохочує впровадження принципів конфіденційності в проектування та розробку продуктів, послуг і процесів за замовчуванням. Сприяє впровадженню міркувань конфіденційності на кожному етапі життєвого циклу інформації;

- управління третіми сторонами – розглядає наслідки залучення сторонніх постачальників послуг для конфіденційності та встановлює настанови для забезпечення дотримання цими постачальниками вимог щодо конфіденційності [46].

Хоча ISO/IEC 27701 в першу чергу зосереджений на управлінні конфіденційністю, його вимоги та настанови по суті включають етичні міркування, пов’язані з відповідальним поводженням з персональною інформацією. Наголошуючи на захисті прав громадян на недоторканність приватного життя, забезпеченні прозорості та дотриманні законодавчих і

нормативних вимог, стандарт опосередковано сприяє етичній поведінці в рамках практик кібербезпеки. Дотримання ISO/IEC 27701 сприяє створенню культури етичного поводження з даними, поваги до приватності та відповідального управління інформацією в організаціях, узгоджуючись з більш широкими етичними міркуваннями в управлінні кібербезпекою.

Таким чином, набір міжнародних стандартів, що стосуються різних аспектів управління кібербезпекою, хоч і не зосереджені безпосередньо на етичних міркуваннях, за своєю суттю сприяють створенню середовища, сприятливого для етичних практик у цифровій сфері. Такі стандарти, як ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27031, ISO/IEC 27032, ISO/IEC 27701 та інші, закладають основу для надійної інформаційної безпеки, управління конфіденційністю та мережевої безпеки. Ці стандарти наголошують на захисті конфіденційної інформації, створенні безпечних систем та дотриманні законодавчих і нормативних рамок. Опосередковано вони сприяють етичним практикам кібербезпеки, заохочуючи відповідальну поведінку, захищаючи конфіденційність та підтримуючи цілісність і доступність критично важливих інформаційних активів. Хоча етичні міркування не сформульовані явно, вони пронизують ці стандарти, формуючи важливе підґрунтя для створення культури довіри, доброчесності та відповідальної поведінки в постійно мінливому ландшафті управління кібербезпекою.

2.3. Визначення можливих наслідків недотримання етичних норм

Управління кібербезпекою відіграє ключову роль у підтримці етичних норм і принципів у цифровому середовищі. Його функція виходить за рамки технічних гарантій і охоплює етичні міркування, сприяння відповідальній поведінці та забезпечення етичного використання технологій. З розвитком технологій і збільшенням кількості кібератак для організацій як ніколи важливо мати надійну стратегію кібербезпеки, щоб захистити конфіденційну інформацію

та зберегти довіру зацікавлених сторін. Розглянемо основні функції, що підкреслюють його значення в дотриманні етичних норм:

1) захист конфіденційної інформації – однією з найважливіших функцій управління кібербезпекою є захист конфіденційної інформації від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення. Сюди входять персональні дані, фінансова інформація, інтелектуальна власність та інші види конфіденційної інформації, які є критично важливими для діяльності та репутації організації. Впроваджуючи надійні заходи кібербезпеки, такі як шифрування, брандмауери, контроль доступу та плани реагування на інциденти, організації можуть мінімізувати ризик витоку даних та інших кібератак, які можуть скомпрометувати конфіденційну інформацію;

2) конфіденційність – це включає впровадження заходів для захисту персональних даних, таких як збір лише необхідної інформації, отримання згоди від осіб перед збором їхніх даних та надання їм можливості контролювати їхню особисту інформацію. Крім того, управління кібербезпекою має гарантувати, що персональні дані не передаються третім особам без чітко вираженої згоди і що вони видаляються, коли в них більше немає потреби [16];

3) дотримання законів та нормативних актів, що стосуються кібербезпеки та захисту даних. Це включає реалізацію заходів для виконання вимог таких законів, як Загальний регламент про захист даних (GDPR), Закон про переносимість і відповідальність за медичне страхування (HIPAA) та Стандарт безпеки даних індустрії платіжних карток (PCI DSS). Недотримання цих законів і нормативних актів може призвести до серйозних штрафів і шкоди репутації організації;

4) аутентифікація та авторизація – управління кібербезпекою має гарантувати, що доступ до конфіденційної інформації та систем мають лише уповноважені особи. Це передбачає впровадження протоколів автентифікації та авторизації, таких як багатофакторна автентифікація, для перевірки особи користувачів та обмеження доступу до конфіденційної інформації;

5) реагування на інциденти – управління кібербезпекою повинно мати план реагування на інциденти для швидкого та ефективного реагування на кібератаки та інші інциденти безпеки. Це включає в себе процедури стримування та пом'якшення наслідків атаки, повідомлення постраждалих сторін та відновлення систем і даних. Ефективний план реагування на інциденти може допомогти мінімізувати шкоду, завдану кібератакою, і відновити впевненість у здатності організації захистити конфіденційну інформацію [56];

6) навчання та обізнаність – потрібно навчати співробітників і зацікавлених осіб найкращим практикам кібербезпеки та важливості дотримання етичних норм і принципів. Це передбачає проведення тренінгів на такі теми, як управління паролями, фішинг, соціальна інженерія та захист даних. Крім того, менеджмент кібербезпеки повинен сприяти розвитку культури кібербезпеки в усій організації, заохочуючи працівників говорити про це, якщо вони підозрюють, що стався інцидент, пов'язаний з безпекою;

7) сторонні постачальники – управління кібербезпекою повинно гарантувати, що сторонні постачальники та підрядники дотримуються таких же високих стандартів кібербезпеки, як і сама організація. Це включає в себе проведення належної перевірки постачальників перед укладенням з ними партнерських відносин, ведення переговорів щодо укладення контрактів, які включають положення про кібербезпеку, а також моніторинг діяльності постачальників, щоб переконатися, що вони продовжують відповідати стандартам кібербезпеки [32].

Таким чином, управління кібербезпекою відіграє вирішальну роль у забезпеченні дотримання організацією етичних норм і принципів у цифрову епоху. Впроваджуючи ефективні заходи кібербезпеки, захищаючи конфіденційну інформацію, поважаючи приватність, дотримуючись законів і правил, аутентифікуючи та авторизуючи користувачів, реагуючи на інциденти, навчаючи співробітників і керуючи сторонніми постачальниками, управління кібербезпекою може допомогти організаціям зберегти довіру зацікавлених сторін і дотримуватися своїх етичних обов'язків.

Вплив управлінських рішень на етичні аспекти кібербезпеки може бути досить значним. Управлінські рішення можуть впливати на те, як впроваджуються, підтримуються та застосовуються заходи кібербезпеки, а також можуть формувати культуру та цінності організації, що може впливати на поведінку працівників та прийняття ними рішень, пов'язаних з кібербезпекою. Одним із можливих наслідків управлінських рішень на етичні аспекти кібербезпеки є надання пріоритету безпеці над іншими міркуваннями, такими як конфіденційність або зручність використання. Наприклад, управлінське рішення про запровадження суворого контролю доступу може ненавмисно створити бар'єри для законних користувачів, тим самим поставивши під загрозу продуктивність і зручність роботи користувачів. Аналогічно, рішення про розгортання систем виявлення вторгнень без належного налаштування може призвести до хибних спрацьовувань і непотрібних сповіщень, спричиняючи надмірний стрес і марнування ресурсів. Такі рішення можуть мати довгострокові наслідки, підриваючи моральний дух співробітників і довіру громадськості до здатності організації захистити конфіденційну інформацію [46].

Ще один вплив управлінських рішень на етичні аспекти кібербезпеки – створення суперечливих стимулів. Наприклад, системи преміювання або показники ефективності, які винагороджують працівників за досягнення певних показників безпеки, можуть заохочувати поведінку, що шкодить загальному стану безпеки. Працівники можуть зосередитися на тому, щоб поставити галочку замість того, щоб справді покращити безпеку, що призведе до хибного відчуття безпеки та потенційно катастрофічних наслідків [28]. Крім того, управлінські рішення можуть впливати на рівень інвестицій в ініціативи з кібербезпеки, що може мати прямий вплив на ефективність засобів і процесів контролю безпеки. Недофінансованим програмам безпеки може не вистачати ресурсів, необхідних для того, щоб бути в курсі нових загроз, що робить організацію вразливою до атак. І навпаки, надмірні інвестиції в безпеку можуть відволікати кошти від інших важливих напрямків діяльності організації, що призводить до зниження рентабельності інвестицій і зниження конкурентоспроможності [31].

У формуванні культури кібербезпеки в організації життєво важливу роль відіграє передача повідомлень зверху вниз і залучення керівництва. Коли керівники демонструють відданість етичним міркуванням у сфері кібербезпеки, таким як повага до приватного життя співробітників і захист даних клієнтів, це поширюється на нижчі рівні і сприяє формуванню спільного почуття відповідальності серед працівників. З іншого боку, недостатня увага керівництва до етичних питань може заохочувати працівників обирати короткі шляхи або нехтувати політикою безпеки, що в кінцевому підсумку ставить під загрозу все підприємство [46].

Нарешті, управлінські рішення можуть впливати на утримання та найм кваліфікованого персоналу з кібербезпеки. Якщо організація не демонструє відданість етичним міркуванням у сфері кібербезпеки, їй буде складно залучати та утримувати найкращі таланти, які цінують етичну практику. Цей недолік може негативно вплинути на здатність організації ефективно реагувати на нові кіберзагрози та підтримувати належний рівень безпеки.

Щоб зменшити ці ризики, організації повинні інтегрувати етичні міркування у свої стратегії кібербезпеки та забезпечити відповідність управлінських рішень етичним принципам. Така інтеграція повинна включати регулярне навчання та інформаційні кампанії, прозору комунікацію та встановлення чітких політик і процедур, що відображають етичні цінності. Крім того, організації повинні заохочувати культуру, в якій працівники відчувають себе уповноваженими висловлювати занепокоєння та повідомляти про потенційні етичні порушення без страху перед репресіями. Періодичні огляди та оцінки також можуть допомогти виявити сфери, де управлінські рішення можуть суперечити етичним міркуванням, що дозволить вчасно вжити заходів для виправлення ситуації [51].

Кібербезпека є критично важливим аспектом системи безпеки будь-якої організації. Однак простого впровадження заходів кібербезпеки недостатньо; не менш важливо забезпечити, щоб ці заходи були етичними. Недотримання етичних стандартів у сфері кібербезпеки може мати далекосяжні наслідки як для

організації, так і для суспільства в цілому. Узагальнимо провідні можливі наслідки недотримання етичних стандартів у сфері кібербезпеки (рис. 2.1).

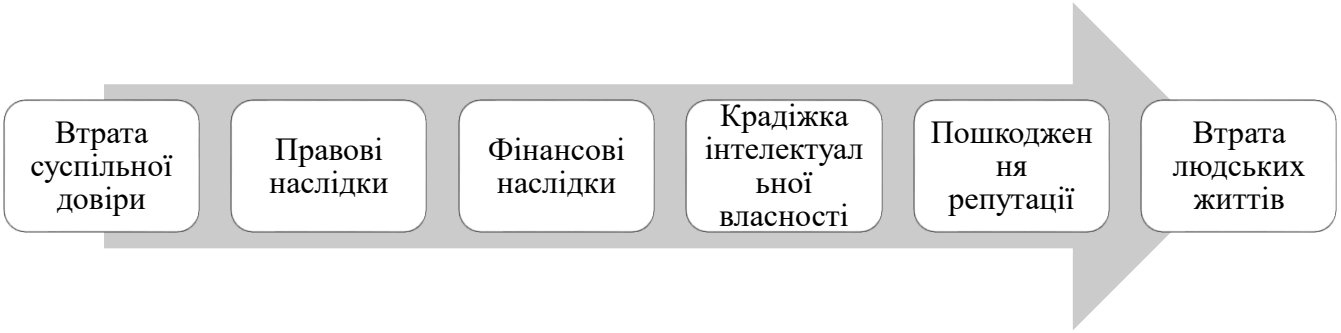

Рис. 2.1. Потенційні наслідки недотримання етичних стандартів у сфері кібербезпеки (Джерело: побудовано автором за даними [54])

Одним з найбільш значущих наслідків недотримання етичних стандартів у сфері кібербезпеки є втрата суспільної довіри. Коли організація не може захистити дані своїх клієнтів, це може підірвати довіру споживачів і зашкодити репутації організації. Люди з меншою ймовірністю будуть співпрацювати з організацією, яка не сприймає їхню приватність і безпеку серйозно. Більше того, втрата суспільної довіри може мати довгострокові наслідки, ускладнюючи відновлення організації після майбутніх порушень безпеки або етичних промахів [57].

Ще одним наслідком недотримання етичних стандартів у сфері кібербезпеки є можливість судового переслідування. Уряди в усьому світі все частіше запроваджують законодавство, спрямоване на захист даних і приватного життя громадян. Недотримання цих норм може призвести до великих штрафів та юридичних санкцій. Наприклад, відповідно до Загального регламенту захисту даних Європейського Союзу (GDPR), організації можуть бути оштрафовані на суму до 20 мільйонів євро або 4% від їхнього річного обороту за недотримання вимог. Аналогічно, Каліфорнійський закон про конфіденційність споживачів (CCPA) надає споживачам право подавати до суду на організації за витік даних, спричинений невжиттям розумних заходів безпеки [50].

Недотримання етичних стандартів у сфері кібербезпеки також може мати значні фінансові наслідки. Порушення безпеки може коштувати організації мільйони доларів у вигляді втраченого доходу, судових витрат та витрат на виправлення ситуації. Згідно зі звітом IBM «Cost of a Data Breach Report 2020», середня загальна вартість витоку даних становить 3,92 мільйона доларів США. Крім того, у звіті зазначено, що вартість витоку зростає на 10% для організацій, які не мають повністю розгорнутого рішення для автоматизації безпеки [56].

Кіберзлочинці часто націлені на інтелектуальну власність, включаючи патенти, торгові марки, авторські права та комерційні таємниці. Якщо організація не дотримується етичних стандартів у сфері кібербезпеки, злочинцям стає легше викрадати інтелектуальну власність, що призводить до фінансових втрат і підриву конкурентних переваг організації. Крадіжка інтелектуальної власності також може підірвати інновації та дослідження, оскільки організації не поспішають інвестувати в дослідження і розробки через страх втратити свою інтелектуальну власність [51].

Порушення безпеки або етичних норм може серйозно зашкодити репутації організації, на відновлення якої можуть піти роки. Згідно з опитуванням, проведеним Ponemon Institute, 71% респондентів заявили, що витік даних негативно вплине на репутацію компанії. Більше того, 57% респондентів вважають, що репутація компанії ніколи не відновиться після витоку даних. Пошкодження репутації може вплинути на фінансові показники організації, ускладнюючи залучення нових клієнтів та утримання існуючих [50].

В екстремальних випадках недотримання етичних стандартів у сфері кібербезпеки може призвести до втрати людських життів. Зі збільшенням кількості пристроїв, підключених до інтернету, зростає ризик кібератак на об’єкти критичної інфраструктури, такі як лікарні, електростанції та транспортні системи. Успішна атака на ці системи може призвести до фізичної шкоди або загибелі людей. Тому дуже важливо, щоб організації надавали пріоритет етичним стандартам у сфері кібербезпеки, щоб запобігти таким катастрофічним подіям.

Отже, управлінські рішення суттєво впливають на етичні аспекти кібербезпеки різними способами, як позитивними, так і негативними. Визнаючи цей вплив і проактивно вирішуючи потенційні конфлікти, організації можуть створити надійне середовище кібербезпеки, яке збалансовує імперативи безпеки з етичними міркуваннями, що в кінцевому підсумку сприятиме безпеці та довірі до їхньої цифрової екосистеми. Дотримання етичних стандартів у сфері кібербезпеки має важливе значення для захисту як організаційних, так і суспільних інтересів. Недотримання етичних стандартів може призвести до втрати суспільної довіри, правових наслідків, фінансових наслідків, крадіжки інтелектуальної власності, шкоди репутації, а в екстремальних випадках – до втрати людських життів. Організації повинні визнати важливість етичних стандартів у сфері кібербезпеки і вжити заходів для їх інтеграції в свої протоколи і практики безпеки. Це не лише принесе користь організації, але й допоможе створити безпечнішу онлайн-спільноту для всіх.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ ЕТИЧНИХ НОРМ У ПРАКТИКУ КІБЕРБЕЗПЕКИ

3.1. Зміст етичних корпоративних кодексів

Одна з головних переваг міцної етичної основи для бізнесу полягає в тому, що він матиме моральний компас, який допоможе приймати етичні рішення в бізнес-середовищі, яке швидко змінюється. Світ переживає масштабні зміни в інформаційних технологіях завдяки прогресу в області штучного інтелекту, алгоритмів машинного навчання, 5G, а також збору та обробки даних.

Ландшафт кіберзагроз також швидко розвивається, і компанії повинні приймати важливі рішення щодо захисту себе та своїх клієнтів. Зі зростанням кіберзлочинності та нових загроз, викликаних новими технологіями, такими як штучний інтелект, компаніям необхідно підвищити рівень кібербезпеки. Щоб це зробити, не жертвуючи клієнтами або клієнтами, яких вони збираються захищати, потрібна міцна етична основа та письмовий кодекс поведінки.

Етичні корпоративні кодекси, також відомі як етичні кодекси або кодекси поведінки, – це документи, в яких викладено етичні принципи та цінності, якими компанія керується у своїй поведінці та прийнятті рішень. Ці кодекси покликані слугувати керівництвом для працівників, керівництва та інших зацікавлених сторін щодо того, як діяти етично та відповідально в усіх аспектах бізнесу.

Кодексом корпоративної етики окреслюються норми і правила корпоративної поведінки, відображаються провідні цінності, стандарти і принципи роботи, які дозволять досягати визначених цілей [13].

Кодексом етики і ділової поведінки окреслюються головні корпоративні цінності, етичні вимоги й відносини між партнерами, співробітниками, акціонерами, державними органами, споживачами, конкурентами, представниками ЗМІ й профспілковими організаціями. Завдяки кодексу дається чітке розуміння принципів ведення бізнесу, вимог і стандартів, котрих повинні додержуватись всі робітники й члени наглядової ради Компанії. Знання й

додержання Кодексу дасть змогу кожному співробітнику приймати правильні рішення, обходячи ситуації, котрі можуть принести шкоду репутації Компанії [12].

В. А. Пігош [20, с. 105] та В. П. Кубко [15, с. 315] висловлюють думку, що кодексом корпоративної етики можуть виконуватися три головні функції: іміджева чи репутаційна, управлінська і розвиток корпоративної культури.

Своєю чергою закордонні науковці вказують, що етичні корпоративні кодекси, можуть виконувати наступні функції: 1) етичні корпоративні кодекси визначають етичні стандарти, яких компанія очікує від своїх працівників. Вони дають чітке розуміння того, що вважається етичною та відповідальною поведінкою в організації; 2) сприяння розвитку позитивної корпоративної культури – окреслюючи цінності та принципи компанії, етичні корпоративні кодекси допомагають створити позитивну корпоративну культуру, яка заохочує етичну поведінку та відповідальне прийняття рішень; 3) етичні корпоративні кодекси пропонують працівникам рекомендації щодо вирішення етичних дилем та складних ситуацій, які можуть виникнути під час їхньої роботи; 4) заохочення дотримання законів і правил – етичні корпоративні кодекси гарантують, що працівники обізнані з відповідними законами та правилами, які застосовуються до їхньої роботи, і заохочують дотримання цих правил; 5) сприяння прозорості та підзвітності – встановлюючи чіткі етичні стандарти, етичні корпоративні кодекси сприяють прозорості та підзвітності в організації. Працівники несуть відповідальність за свої дії, а компанія є прозорою щодо своїх етичних практик; 6) покращення репутації – компанія, яка дотримується етичних корпоративних кодексів, швидше за все, матиме кращу репутацію з-поміж зацікавлених сторін, включно із працівниками, інвесторами й клієнтами; 7) допомагають виявляти та управляти етичними ризиками, які можуть негативно вплинути на репутацію та фінансові показники компанії; 8) сприяння навчанню та освіті – етичні корпоративні кодекси є основою для навчання та освіти працівників з питань етики та відповідальної поведінки; 9) етичні корпоративні кодекси сприяють прийняттю етичних рішень, забезпечуючи основу для оцінки етичних міркувань

і прийняття рішень, які відповідають цінностям і принципам компанії; 10) побудова довіри – демонструючи прихильність до етичної поведінки, етичні корпоративні кодекси допомагають будувати довіру між компанією та її стейкхолдерами. Довіра виступає вагомою складовою усіляких успішних ділових відносин [52].

Зміст корпоративного кодексу компанії окреслюється, насамперед, її особливостями, завданнями розвитку, структурою, установками її керівних органів. Зазвичай, кодекси містять дві частини: ідеологічну (цінності, цілі, місія); нормативну (стандарти робочої поведінки) [20, с. 105].

Зазвичай зміст етичних корпоративних кодексів зазвичай включає наступні питання:

- місія, бачення та цінності – чіткі формулювання, що визначають місію організації, бачення етичної поведінки та основні цінності, якими керуються у прийнятті рішень та діях. Вони задають тон етичній культурі в компанії;

- дотримання законів і правил – наголошує на дотриманні правових вимог і регуляторних стандартів, що стосуються галузі, в якій працює організація. Це слугує основою для етичної поведінки в межах закону;

- цілісність і чесність – заохочує чесність, цілісність і справедливість у всіх ділових відносинах. Включає директиви проти хабарництва, корупції, шахрайства та конфлікту інтересів;

- повага та різноманітність – сприяє повазі до людей, різноманітності та інклюзивності на робочому місці, створюючи середовище, вільне від дискримінації, переслідувань чи несправедливого ставлення на основі раси, статі, релігії чи інших характеристик;

- конфіденційність і приватність – передбачає важливість збереження конфіденційності конфіденційної інформації, захисту даних, що є власністю компанії, та поваги до прав людей на приватне життя;

- професіоналізм та відповідальність – визначає очікування щодо професійної поведінки, підзвітності та відповідальності за дії та рішення працівників як всередині організації, так і під час представлення її назовні;

- відповідальність перед зацікавленими сторонами – цей розділ описує обов'язки компанії перед різними зацікавленими сторонами, включаючи співробітників, клієнтів, постачальників, акціонерів і широку громадськість;

- відносини з клієнтами – охоплює питання, пов'язані з відносинами з клієнтами, такі як конфіденційність, захист даних та розгляд скарг;

- відносини з постачальниками – описує очікування компанії щодо своїх постачальників, включаючи питання, пов'язані з якістю, ціноутворенням, доставкою та етичними джерелами постачання;

- взаємодія з громадськістю – цей розділ описує зобов'язання компанії підтримувати місцеві громади, включаючи ініціативи, пов'язані з освітою, охороною здоров'я та збереженням навколишнього середовища;

- політика інформування про порушення – описує політику компанії щодо інформування про неетичну поведінку, включаючи процес повідомлення та розслідування звинувачень;

- вирішення конфліктів та механізми звітування – надає вказівки щодо процедур вирішення конфліктів та окреслює канали повідомлення про етичні проблеми, забезпечуючи механізм, за допомогою якого працівники можуть повідомляти про порушення або звертатися за порадою, не боячись помсти;

- екологічна та соціальна відповідальність – висвітлює зобов'язання організації щодо екологічної стійкості, соціальної відповідальності та залучення громадськості, узгоджуючи бізнес-практики з етичними принципами, які приносять користь суспільству;

- корпоративне управління та прозорість – підкреслює важливість прозорого ведення бізнесу, ефективного управління та підзвітності в процесах прийняття рішень, забезпечуючи відкритість і справедливість;

- навчання та освіта – заохочує постійне навчання та тренінги з етичної поведінки, підвищення обізнаності та розуміння корпоративного кодексу серед працівників;

- наслідки недотримання – окреслює потенційні дисциплінарні заходи або наслідки за порушення кодексу, підкреслюючи важливість дотримання етичних

стандартів [31; 52].

Охоплюючи ці ключові питання, етичні корпоративні кодекси забезпечують всеосяжну основу для етичного прийняття рішень і поведінки в організації. Вони слугують орієнтиром для працівників, керівництва та інших зацікавлених сторін, до яких можна звертатися, коли вони стикаються з етичними дилемами, а також допомагають зміцнити довіру та авторитет серед зацікавлених сторін, демонструючи прихильність до етичних ділових практик.

В. П. Кубко пропонує традиційний зміст корпоративного кодексу формулювати наступним чином (рис. 2.2).

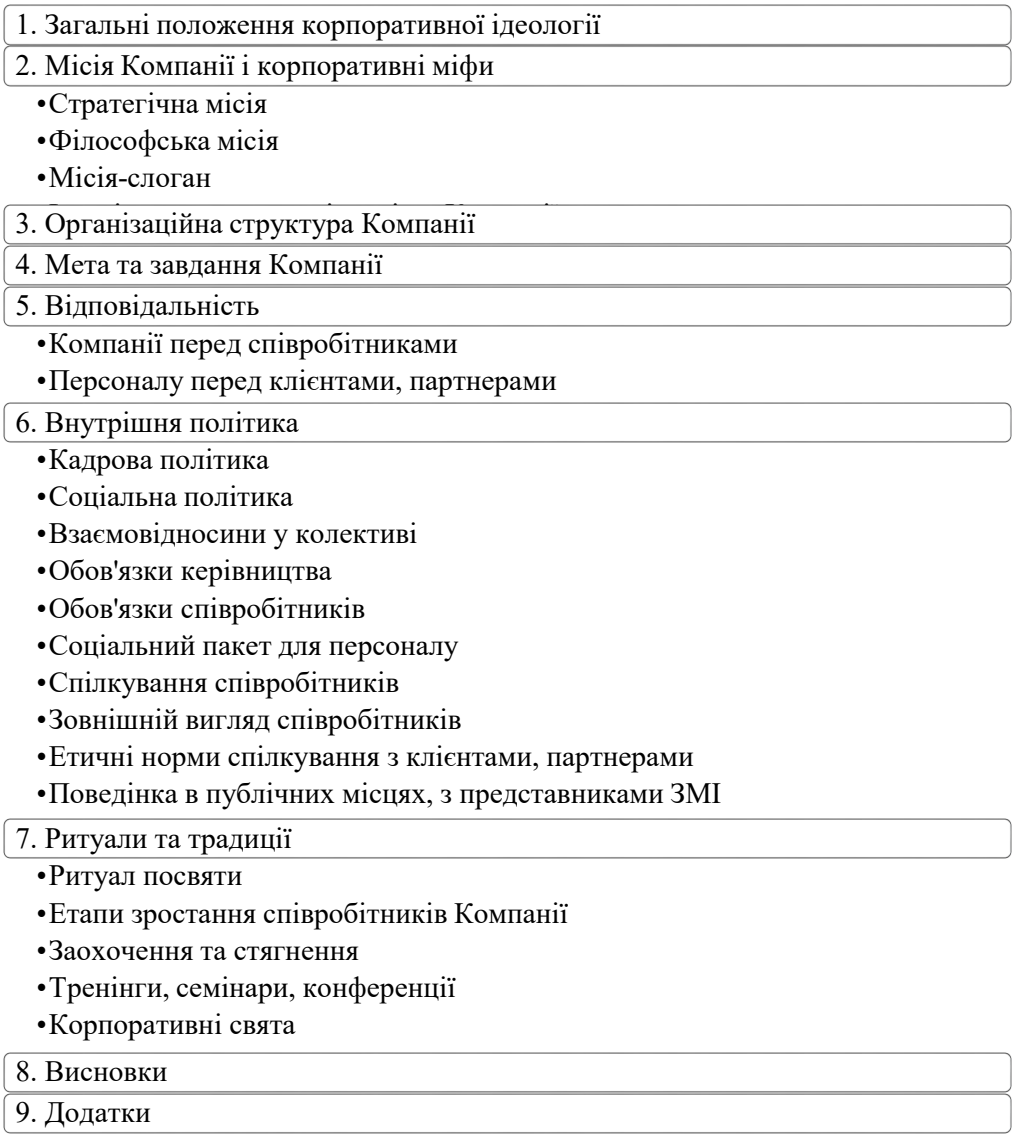

Рис. 2.2. Ключові складові традиційного змісту етичного корпоративного кодексу (Джерело: побудовано автором за даними [15, с. 316])

Етичні корпоративні кодекси відіграють вирішальну роль у формуванні культури та цінностей організації. Встановлюючи чіткі правила етичної поведінки, компанії можуть сприяти формуванню культури доброчесності, поваги та відповідальності серед своїх працівників. Це, в свою чергу, може покращити репутацію компанії, побудувати довіру із зацікавленими сторонами та сприяти довгостроковому успіху.

Ефективне впровадження етичних корпоративних кодексів вимагає поєднання лідерства зверху донизу, залучення працівників та механізмів підзвітності. Керівники вищої ланки повинні демонструвати свою відданість етичній поведінці, задаючи тон зверху і показуючи власний приклад. Співробітники повинні бути ознайомлені з етичним кодексом і розуміти свою роль та обов'язки у дотриманні етичних стандартів компанії. Нарешті, компанія повинна створити надійні механізми підзвітності, такі як канали анонімних повідомлень, аудити та дисциплінарні заходи, щоб забезпечити дотримання кодексу.

Таким чином, етичний корпоративний кодекс – це документ, який визначає цінності, принципи та стандарти поведінки, що очікуються від працівників та зацікавлених сторін в організації. Етичні корпоративні кодекси відіграють життєво важливу роль у заохоченні етичної поведінки, створенні позитивної корпоративної культури, наданні рекомендацій, заохоченні дотримання законів і правил, сприянні прозорості та підзвітності, зміцненні репутації, підтримці управління ризиками, сприянні навчанню та освіті, заохоченні до прийняття етичних рішень і побудові довіри. Впроваджуючи етичні корпоративні кодекси у свою діяльність, компанії можуть гарантувати, що вони ведуть свій бізнес етично та відповідально, що, зрештою, сприяє їхньому довгостроковому успіху та сталому розвитку.

Етичні корпоративні кодекси слугують керівними документами, узгоджуючи організаційну поведінку з етичними принципами, сприяючи формуванню культури доброчесності, довіри та відповідальної поведінки всередині компанії та її взаємодії із зацікавленими сторонами. Регулярний

перегляд, посилення та впровадження цих кодексів є важливими для підтримки етичної корпоративної культури.

3.2. Аналіз світового досвіду застосування етичних кодексів у кібербезпеці

Застосування етичних кодексів у сфері кібербезпеки набуває все більшого значення в сучасну цифрову епоху. З розвитком технологій, а також й збільшенням кількості людей, які покладаються на Інтернет у повсякденній діяльності, потенціал кіберзагроз і атак значно зріс. Етичні кодекси у сфері кібербезпеки створюють рамки, в яких діють окремі особи та організації, гарантуючи, що вони вживають належних заходів для захисту конфіденційної інформації та систем.

Основні переваги застосування етичних кодексів у сфері кібербезпеки є такими:

- захист чутливої інформації – етичні кодекси в кібербезпеці надають пріоритет захисту конфіденційної інформації, такої як персональні дані, фінансова інформація та інтелектуальна власність. Впроваджуючи етичні кодекси, організації можуть гарантувати, що вони вживають необхідних заходів для захисту цієї інформації та запобігання несанкціонованому доступу або порушенням;

- запобігання кібератакам – етичні кодекси у сфері кібербезпеки пропагують найкращі практики та керівні принципи, які можуть допомогти запобігти кібератакам. Наприклад, етичні кодекси можуть вимагати від організацій впровадження надійних паролів, регулярного оновлення програмного забезпечення та брандмауерів для захисту від зловмисних атак;

- зміцнення довіри та авторитету – організації, які дотримуються етичних кодексів у сфері кібербезпеки, демонструють свою відданість захисту конфіденційної інформації та збереженню конфіденційності своїх користувачів.

Вказане зміцнює довіру та авторитет серед клієнтів, партнерів та зацікавлених сторін, що має вирішальне значення в сучасному цифровому ландшафті;

- дотримання регуляторних вимог – у багатьох країнах прийняті нормативні акти і закони, що регулюють кібербезпеку. Етичні кодекси з кібербезпеки допомагають організаціям дотримуватися цих вимог, зменшуючи ризик юридичних санкцій і репутаційних втрат [31].

Провідні проблеми застосування етичних кодексів у сфері кібербезпеки є наступними:

- брак обізнаності та навчання – багато людей і організацій все ще не усвідомлюють важливості етичних кодексів у сфері кібербезпеки. Така необізнаність може призвести до недостатньої підготовки, що може спричинити погане впровадження та дотримання етичних кодексів;

- складність технологій – швидкий розвиток технологій ускладнює розробку та впровадження етичних кодексів, які б відповідали новим загрозам. Нові технології часто створюють нові вразливості, що робить необхідним регулярне оновлення етичних кодексів та навчальних програм;

- баланс між безпекою та зручністю використання – етичні кодекси у сфері кібербезпеки часто вимагають додаткових кроків або заходів для забезпечення безпеки систем і даних. Однак такого роду заходи іноді можуть погіршити досвід користувачів, створюючи напругу між безпекою, а також зручністю використання;

- вартість та ресурсоємність – впровадження та підтримка етичних кодексів у сфері кібербезпеки можуть бути дорогими та ресурсоємними. Малі та середні підприємства (МСП) можуть мати труднощі з виділенням достатніх ресурсів, що потенційно робить їх вразливими до кіберзагроз [31].

Тепер окреслимо майбутні напрямки для етичних кодексів у сфері кібербезпеки:

- підвищення рівня автоматизації – автоматизація може допомогти полегшити деякі проблеми, пов’язані з впровадженням етичних кодексів у сфері кібербезпеки. Технології штучного інтелекту (ШІ) та машинного навчання (МН)

можуть допомогти у виявленні та реагуванні на кіберзагрози, дозволяючи організаціям зосередитися на інших аспектах кібербезпеки;

- інтеграція з новими технологіями – нові технології, такі як блокчейн, Інтернет речей (IoT) та хмарні обчислення, створюють унікальні виклики для кібербезпеки. Етичні кодекси повинні розвиватися, щоб відповідати на ці виклики і гарантувати, що організації, які використовують ці технології, дотримуються суворих протоколів безпеки;

- міжнародна співпраця – загрози кібербезпеці не знають кордонів. Міжнародна співпраця має важливе значення для розробки та впровадження етичних кодексів, які можуть ефективно протистояти глобальним кіберзагрозам. Співпраця між урядами, організаціями та галузями може допомогти встановити узгоджені етичні стандарти в різних регіонах;

- наголос на конфіденційності - у зв’язку зі зростаючим занепокоєнням щодо конфіденційності даних, етичні кодекси з кібербезпеки повинні надавати пріоритет захисту приватності. Організації повинні гарантувати, що вони отримують інформовану згоду від користувачів перед тим, як збирати і обробляти їхні дані, і що вони забезпечують прозорість щодо практик обробки даних [62].

Розглянемо приклади світового досвіду застосування етичних кодексів у сфері кібербезпеки.

Політика конфіденційності Google є яскравим прикладом, що ілюструє застосування етичних кодексів у сфері кібербезпеки в діяльності технологічного гіганта. Політика конфіденційності Google окреслює принципи та керівні положення, що регулюють збір, використання та захист даних користувачів у широкому спектрі послуг і продуктів компанії. Політика конфіденційності Google передбачає, що компанія не продаватиме особисту інформацію третім особам і використовуватиме дані лише з тією метою, яка була вказана під час збору. Крім того, Google надає користувачам інструменти для контролю своїх даних і видалення їх за запитом. Це свідчить про те, що Google дотримується етичних принципів щодо збору, використання та захисту даних. Політика

конфіденційності Google демонструє застосування етичних кодексів у сфері кібербезпеки у напрямках:

1) наголошує на прозорості, надаючи чітку та зрозумілу інформацію про дані, які компанія збирає, чому вона їх збирає та як вона їх використовує. Така прозорість відповідає етичним принципам, забезпечуючи інформування користувачів про обробку їхніх даних;

2) окреслює зобов'язання Google щодо захисту даних користувачів за допомогою надійних заходів безпеки, шифрування та контролю доступу. Вона демонструє етичну відповідальність, надаючи пріоритет захисту даних і впроваджуючи практики безпеки для запобігання несанкціонованому доступу або порушенням;

3) поважає вибір користувачів і забезпечує контроль над їхніми даними. Вона надає користувачам можливість керувати своїми налаштуваннями конфіденційності, контролювати обмін даними та відмовлятися від певних методів збору даних, що відповідає етичним міркуванням щодо автономії та згоди користувачів;

4) відповідає законодавчим вимогам і нормам, забезпечуючи дотримання глобальних законів про конфіденційність, таких як Загальний регламент про захист даних (GDPR) та інших відповідних нормативних актів. Це зобов'язання щодо дотримання вимог відображає етичну поведінку в межах правових норм;

5) підкреслює зобов'язання Google постійно переглядати та вдосконалювати свою політику конфіденційності. Вона відображає етичну відповідальність, адаптуючись до зростаючих проблем конфіденційності, технологічних змін і очікувань користувачів щодо посилення заходів захисту даних;

6) Google надає освітні ресурси та звіти про прозорість, спрямовані на інформування користувачів про питання конфіденційності та безпеки. Ці ініціативи сприяють підвищенню обізнаності та відповідають етичним принципам освіти та прозорості;

7) окреслює механізми вирішення проблем користувачів, надаючи

можливості для запитів, скарг та отримання роз'яснень. Це демонструє підзвітність і реагування на потреби користувачів, зміцнюючи етичні цінності підзвітності та надійності [40].

Таким чином, політика конфіденційності Google слугує прикладом етичних кодексів у сфері кібербезпеки, наголошуючи на прозорості, контролі користувачів, захисті даних, дотриманні законодавства, постійному вдосконаленні, освіті та підзвітності. Вона відображає відданість Google етичним принципам роботи з даними користувачів і сприяє зміцненню довіри та розвитку відповідальних практик кібербезпеки [40].

Facebook впровадив різні заходи для захисту даних користувачів, включаючи шифрування, безпечний вхід та двофакторну автентифікацію. Facebook також надає користувачам можливість керувати тим, хто бачить їхні дані, і має політику, яка гарантує, що сторонні додатки не використовують дані користувачів не за призначенням. Ці зусилля свідчать про те, що компанія Meta зробила кроки для захисту конфіденційності та безпеки користувачів, відображаючи етичні принципи, пов'язані із захистом даних [53].

Корпорація Майкрософт опублікувала політику кібербезпеки, в якій викладено зобов'язання компанії щодо захисту даних і пристроїв клієнтів. Політика передбачає такі заходи, як шифрування, виявлення загроз і реагування на них, а також співпрацю з правоохоронними органами для боротьби з кіберзлочинністю. Політика Microsoft демонструє етичні принципи, пов'язані із захистом конфіденційної інформації та запобіганням кібератакам [53].

Компанія Apple впровадила різні заходи для захисту даних користувачів, включаючи наскрізне шифрування, безпечну автентифікацію та суворий контроль над магазинами додатків. Apple також надає користувачам інструменти для управління своїми даними і публічно зобов'язалася захищати конфіденційність клієнтів. Вказані зусилля ілюструють відданість Apple етичним принципам, пов'язаним із захистом даних і приватності користувачів [46].

Загальний регламент захисту даних (GDPR) – це регламент Європейського

Союзу, який встановлює принципи захисту персональних даних. GDPR вимагає від організацій отримувати явну згоду від користувачів перед тим, як збирати та обробляти їхні дані, а також надає користувачам право на доступ, виправлення та видалення їхніх даних. GDPR є прикладом етичних принципів, пов’язаних із захистом даних і приватності, і слугує моделлю для подібних нормативних актів у всьому світі [62].

Висновок до розділу 3. Наведені приклади демонструють, як організації можуть інтегрувати етичні кодекси у свої практики кібербезпеки. Дотримання етичних принципів, пов’язаних із захистом даних, конфіденційністю та безпекою, допомагає побудувати довіру з клієнтами та захистити конфіденційну інформацію. Організації, які дотримуються етичних кодексів, можуть зменшити кіберзагрози та сприяти створенню безпечнішого та надійнішого цифрового середовища.

Етичні кодекси у сфері кібербезпеки мають важливе значення для захисту конфіденційної інформації, запобігання кібератакам, розбудови довіри та дотримання регуляторних вимог. Хоча впровадження етичних кодексів пов’язане з певними труднощами, їхні переваги значно перевищують витрати. Оскільки технології продовжують розвиватися, а кіберзагрози еволюціонують, етичні кодекси повинні адаптуватися до нових викликів.

РОЗДІЛ 4
РОЗРОБКА ЕТИЧНОГО КОДЕКСУ ДЛЯ ОРГАНІЗАЦІЙ КІБЕРБЕЗПЕКИ

4.1. Розробка етичного кодексу, який враховує світові стандарти та етичні норми в кібербезпеці

Розробка етичного кодексу компанії, який відповідає світовим стандартам та етичним нормам у сфері кібербезпеки, є критично важливим процесом, що вимагає всебічного розуміння найкращих галузевих практик, законодавчих вимог та етичних принципів. Основні етапи створення такого етичного кодексу:

1) почніть з проведення ретельного дослідження світових стандартів, галузевих керівних принципів і поширених етичних норм у сфері кібербезпеки.

Вказане передбачає вивчення міжнародно визнаних стандартів, таких як ISO/IEC 27001, ISO/IEC 27002, GDPR, а також й інших відповідних нормативних актів. Проаналізуйте тематичні дослідження, етичні рамки та найкращі практики у сфері кібербезпеки, щоб отримати уявлення стосовно домінуючих етичних міркувань;

2) залучайте зацікавлені сторони з різних відділів, зокрема експертів з кібербезпеки, юрисконсультів, працівників відділу кадрів та вищого керівництва.

Зберіть інформацію з різних точок зору, щоб зрозуміти конкретні бізнес-потреби, потенційні ризики, а також й етичні виклики, з якими стикається організація;

3) визначте набір основних етичних принципів, на яких базуватиметься етичний кодекс.

Ці принципи повинні відповідати світовим стандартам та загальноприйнятим етичним нормам у сфері кібербезпеки. Приклади включають захист конфіденційності користувачів, забезпечення цілісності даних, прозорості, підзвітності та дотримання відповідних законів і правил;

4) розробіть комплексний етичний кодекс, який включає визначені етичні принципи.

Кодекс має бути чітким, лаконічним і доступним для всіх працівників, визначати очікування, цінності та стандарти поведінки, пов’язані з кібербезпекою. Він має охоплювати такі сфери, як захист даних, інформаційна безпека, конфіденційність користувачів, етичне використання технологій, повідомлення про інциденти та дотримання вимог законодавства;

5) розшліть проєкт серед ключових зацікавлених сторін для отримання відгуків та рецензій.

Переконайтеся, що кодекс відображає цінності організації, резонує з працівниками та узгоджується з глобальними стандартами та етичними нормами. Враховуйте відгуки для доопрацювання та вдосконалення кодексу;

6) після завершення роботи над кодексом впровадьте його через комплексні навчальні програми для всіх співробітників.

Переконайтеся, що всі розуміють принципи, настанови та очікування, викладені в кодексі. Впровадити механізми для постійного навчання та зміцнення етичних практик;

7) створіть основу для регулярного оцінювання та оновлення етичного кодексу.

Загрози кібербезпеці еволюціонують, а етичні міркування змінюються, тому періодичний перегляд гарантує, що кодекс залишається актуальним, відповідає світовим стандартам і відображає нові етичні норми в галузі кібербезпеки;

8) популяризуйте етичний кодекс як невід’ємну частину культури компанії.

Інтегруйте етичні міркування в процеси прийняття рішень, політики та повсякденну діяльність, сприяючи розвитку культури етичної поведінки та підзвітності в організації [31; 47].

Створення етичного кодексу всієї компанії, особливо з урахуванням світових стандартів та етичних норм у сфері кібербезпеки, є складним завданням,

яке, як правило, включає багато аспектів і міркувань, пристосованих до специфіки конкретної організації. Важливо зазначити, що розробка такого документа зазвичай є комплексним процесом, до якого залучаються експерти з юридичних та етичних питань в організації. Нижче наведено скорочену та узагальнену версію, яка демонструє структуру та ключові компоненти, що можуть бути включені до кодексу етики компанії.

Кодекс етики з кібербезпеки компанії Х.

Вступ.

У Компанії ми прагнемо дотримуватися найвищих етичних стандартів у своїй діяльності, особливо щодо кібербезпеки. Ми беремо на себе відповідальність за захист даних наших клієнтів, співробітників та партнерів і визнаємо важливість збереження довіри через відкритість, секретність, чесність та підзвітність. Цей Кодекс етики встановлює керівні принципи та обов’язки, яких ми дотримуємося в нашій повсякденній діяльності.

Основні етичні принципи.

Прозорість. Ми зобов’язуємося бути відкритими та правдивими в наших методах роботи з інформацією. Ми чітко та зрозуміло інформуємо наші зацікавлені сторони про те, як ми збираємо, використовуємо, обмінюємося та зберігаємо персональні дані. Крім того, ми зобов’язуємося бути в курсі відповідних правил, постанов і найкращих галузевих практик щодо прозорості та розкриття інформації.

Анонімність. Оскільки ми розуміємо приватний характер делікатних даних, ми вживаємо заходів для їх захисту від незаконного доступу або розголошення. Виходячи з принципу службової необхідності, доступ до цих матеріалів буде обмежено, а для їхнього безпечного зберігання та передачі будуть вжиті відповідні заходи захисту.

Цілісність. Ми прагнемо вести точний, повний і надійний облік. Обробка даних належним чином і об’єктивно має важливе значення. Ми вживаємо заходів, щоб зупинити зміну, фальсифікацію або корупцію даних.

Підзвітність. Кожен працівник і партнер несе відповідальність за знання та дотримання цих моральних принципів і застосування їх на практиці на своїй посаді. Керівництво створить процедури для повідомлення про правопорушення та їх вирішення, а також забезпечить вжиття коригувальних заходів у разі необхідності. Крім того, ми пропонуємо регулярні інструктажі та програми підвищення обізнаності, щоб допомогти персоналу залишатися поінформованими та готовими до прийняття моральних рішень.

Відповідність. Ми дотримуємося всіх чинних правил, стандартів і галузевих критеріїв, що стосуються кібербезпеки та захисту даних, зокрема ISO/IEC 27002 та ISO/IEC 27701. Щоб протистояти новим загрозам і труднощам, ми постійно працюємо над удосконаленням наших політик, процедур і технологій.

Повага до прав людини. Ми визнаємо, що кожна людина має вроджену цінність і заслуговує на повагу, незалежно від таких характеристик, як раса, стать, вік, релігійна приналежність, сексуальна орієнтація, фізичні здібності або будь-які інші якості, передбачені законом. Ми не будемо займатися діяльністю, яка порушує права людини або заохочує упередження, переслідування, експлуатацію чи насильство.

Соціальна відповідальність. Ми визнаємо свій обов’язок зменшувати несприятливий вплив на суспільство та робити позитивний внесок у створення довготривалих рішень, що сприяють суспільному добробуту та економічному прогресу. Крім того, ми співпрацюємо з регіональними урядами, громадами та групами з метою створення безпечного, доброзичливого середовища, в якому люди можуть процвітати.

Інформаційна безпека. Ми надаємо пріоритет безпеці інформаційних активів, впроваджуючи надійний контроль, заходи шифрування та управління доступом, щоб запобігти несанкціонованому доступу, витоку даних та кіберзагрозам.

Комплаєнс і дотримання законодавства. Ми дотримуємося міжнародних законів, нормативно-правових актів та галузевих стандартів, що стосуються

кібербезпеки. Наші дії та практики не виходять за рамки правових норм, сприяючи розвитку культури комплаєнсу та етичної поведінки.

Етичне використання технологій. Ми відповідально використовуємо технології, утримуючись від зловмисних дій, таких як хакерство, несанкціонований доступ або неетична експлуатація цифрових активів.

Конфіденційність і безпека. Ми впроваджуємо надійні гарантії конфіденційності та безпеки для захисту наданих нам персональних даних. Шифрування, двофакторна автентифікація, обмеження доступу, оцінка вразливостей, часті оновлення та виправлення є одними з таких гарантій.

Повідомлення про проблеми. Якщо ви дізналися про порушення цього Кодексу етики або маєте запитання щодо потенційних етичних конфліктів, повідомте про це свого керівника, представника відділу кадрів або нашого уповноваженого з питань етики. Допускаються анонімні повідомлення, які будуть розглянуті конфіденційно та швидко. Ті, хто добросовісно повідомляють про проблеми, не зазнають жодних покарань.

Сфера застосування.

Цей кодекс поширюється на всіх співробітників, підрядників і сторонніх постачальників, які працюють від імені нашої компанії. Він охоплює нашу професійну поведінку, відносини з клієнтами та взаємодію з ширшою спільнотою кібербезпеки.

Правила поведінки.

Поважайте конфіденційність користувачів, отримуючи згоду на збір даних, надаючи чіткі повідомлення про конфіденційність і дозволяючи користувачам контролювати свої дані.

Поводьтеся з даними обережно, забезпечуючи точність, мінімізуючи збір даних та безпечно видаляючи дані, коли вони більше не потрібні.

Дотримуйтесь суворих протоколів безпеки, зберігайте конфіденційність, регулярно проводьте оцінку ризиків та оперативно реагуйте на інциденти, пов’язані з безпекою.

Проводьте постійні тренінги та навчання для працівників, щоб підвищити їхню обізнаність про ризики кібербезпеки, етичні норми та вимоги до комплаєнсу.

Звітність та комплаєнс.

Ми повідомляємо про неетичну поведінку або порушення цього кодексу нашим керівникам, у відділ кадрів або анонімно на нашу гарячу лінію для викривачів. Ми розслідуємо звинувачення швидко і справедливо, вживаючи відповідних заходів проти тих, хто порушує наші етичні стандарти.

Регулярно переглядайте та оновлюйте етичний кодекс, щоб забезпечити його відповідність світовим стандартам, етичним нормам, що розвиваються, та змінам у регуляторних вимогах.

Впровадження та перегляд.

Ми періодично переглядатимемо та оновлюватимемо цей кодекс, щоб забезпечити його відповідність сучасним тенденціям у сфері кібербезпеки, світовим стандартам та етичним нормам. Усі співробітники, підрядники та сторонні постачальники повинні підписати цей кодекс перед початком роботи з нашою компанією. Порушення можуть призвести до дисциплінарних стягнень, аж до звільнення або розірвання контракту.

Дотримуючись цього етичного кодексу, ми демонструємо нашу прихильність до етичної досконалості в галузі кібербезпеки. Ми завойовуємо довіру наших клієнтів, партнерів і широкої громадськості, послідовно діючи чесно, компетентно та з повагою до приватності. Давайте разом захистимо та захистимо цифровий світ.

Висновок.

Компанія Х зобов’язується дотримуватися цих етичних принципів і стандартів у сфері кібербезпеки. Наша відданість етичній поведінці спрямовує наші дії, зміцнює довіру із зацікавленими сторонами та сприяє створенню безпечного та відповідального цифрового середовища.

Цей Кодекс етики компанії ілюструє нашу відданість дотриманню світових стандартів і моральних принципів у сфері кібербезпеки. Він слугує керівництвом

для прийняття обґрунтованих рішень і сприяє розвитку культури доброчесності, щирості та професіоналізму в нашій організації. Дотримуючись цих моральних принципів, ми прагнемо завоювати довіру наших клієнтів, співробітників, партнерів і широкої громадськості.

Розробка етичного кодексу компанії, який враховує світові стандарти та етичні норми у сфері кібербезпеки, передбачає спільний ітеративний процес, спрямований на узгодження організаційних цінностей із загальноприйнятими етичними принципами. Адже, етичний кодекс слугує керівництвом для прийняття етичних рішень та поведінки, сприяючи розвитку культури доброчесності та відповідальних практик кібербезпеки в компанії.

4.2. Визначення процедур впровадження та моніторингу етичного кодексу

Впровадження та моніторинг етичного кодексу компанії є критично важливим заходом, який відображає прихильність організації до дотримання етичних стандартів та відповідальної поведінки, особливо у сфері кібербезпеки. Створення надійних процедур для впровадження та моніторингу етичного кодексу забезпечує відповідність світовим стандартам, дотримання нормативних вимог та культуру доброчесності в організації.

Наведемо основні процедури впровадження кодексу етики компанії:

- Компанія повинна довести свій Етичний кодекс до відома всіх працівників, підрядників та сторонніх постачальників. Таке інформування повинно включати в себе тренінги, семінари та розповсюдження письмових матеріалів. Метою такого інформування є забезпечення розуміння всіма, хто пов’язаний з компанією, етичних стандартів, які від них очікуються;

- важливо проводити регулярні тренінги для працівників та підрядників з етичних питань та Кодексу етики. Таке навчання має охоплювати такі теми, як конфлікт інтересів, хабарництво, корупція, конфіденційність даних та боротьба

з дискримінацією. Тренінг також має включати ситуаційні вправи, які допоможуть працівникам зрозуміти, як застосовувати Етичний кодекс у реальних життєвих ситуаціях;

- Компанія повинна призначити співробітника з питань комплаєнсу, який відповідає за забезпечення дотримання Кодексу етики. Відповідальний за комплаєнс приймає та розслідує скарги щодо порушень Кодексу етики та звітує безпосередньо генеральному директору або раді директорів;

- необхідно розробити політику щодо викривачів, яка заохочує працівників повідомляти про будь-які підозри у порушенні Кодексу етики. Політика повинна забезпечувати захист працівників, які повідомляють про порушення, включаючи конфіденційність та гарантії непереслідування;

- потрібно проводити періодичні аудити та перевірки для забезпечення дотримання Кодексу етики. Ці перевірки охоплюють такі сфери, як управління фінансами, закупівлі, продажі, маркетинг та людські ресурси. Про результати таких перевірок повідомляється Відповідальному за комплаєнс та Головному виконавчому директору або Раді директорів;

- потрібно застосовувати дисциплінарні заходи до працівників, які порушують Кодекс етики. Дисциплінарне стягнення може варіюватися від попередження до звільнення, залежно від тяжкості порушення;

- Компанія повинна вимагати від сторонніх постачальників згоди на дотримання Кодексу етики. Компанія повинна контролювати дотримання постачальниками Кодексу та вживати відповідних заходів у разі його недотримання;

- регулярний перегляд та оновлення Кодексу етики, забезпечить його актуальність та ефективність. Компанія також повинна отримувати зворотній зв’язок від працівників, клієнтів та зацікавлених сторін для визначення сфер, які потребують вдосконалення;

- необхідно створити кілька механізмів повідомлення про порушення Кодексу етики, щоб працівники могли повідомляти про них. Ці механізми можуть включати анонімні гарячі лінії, електронні адреси або онлайн-портали;

- відповідальний за комплаєнс повинен розслідувати всі повідомлення про порушення Кодексу етики та вирішувати їх у справедливий і прозорий спосіб. Відповідальний за комплаєнс доповідає про свої висновки та рішення Генеральному директору або Раді директорів;

- Компанія заохочує працівників, які демонструють виняткову етичну поведінку та сприяють розвитку культури комплаєнсу. Компанія також відзначає працівників, які повідомляють про порушення Кодексу етики, навіть якщо таке повідомлення не призводить до дисциплінарного стягнення;

- важливо розвивати культуру комплаєнсу в усій організації. Компанія повинна заохочувати працівників говорити про неетичну поведінку, якщо вони стають свідками неетичної поведінки, а також надавати ресурси та підтримку працівникам, які стикаються з етичними дилемами [32; 35].

Кількість витоків даних продовжує зростати, коштуючи компаніям мільярди щороку. На жаль, ця тенденція не зміниться найближчим часом. За прогнозами експертів, до 2025 року кіберзлочинність коштуватиме 10,5 трильйонів доларів щорічно [29].

Оскільки ландшафт загроз стає дедалі складнішим, бізнесу потрібні фахівці з кібербезпеки, щоб забезпечити постійну пильність і випередити хакерів. Оскільки кібербезпека стала серйозною проблемою для організацій по всьому світу, виникає запитання як часто потрібно проводити моніторинг дотримання вимог безпеки. Відповідь очевидна – постійно. Щоб забезпечити захист компанії від кібератак, потрібно впроваджувати послідовну програму моніторингу відповідності вимогам безпеки. Ключовими кроками на цьому шляху можуть бути:

1) Визначення нормативних актів, які застосовуються до нашої компанії.

Загальний регламент захисту даних Європейського Союзу (GDPR), Каліфорнійський закон про конфіденційність споживачів та Закон про переносимість та відповідальність за медичне страхування (HIPAA) – це лише деякі з багатьох нормативно-правових актів, які поширюються на організації в різних секторах.

Наприклад, HIPAA застосовується до постачальників медичних послуг, тоді як GDPR охоплює особисту інформацію, зібрану від громадян ЄС. Це робить важливим розуміння того, який тип регулювання застосовується до вашого бізнесу, незалежно від того, чи працюєте ви на національному або міжнародному рівні.

Окрім визначення того, чи застосовується той чи інший регламент, потрібно також оцінити, як він впливає на нашу компанію. Кожна галузь має унікальні вимоги. Залежно від галузі, певні нормативні акти можуть вимагати додаткового навчання, реєстрації або заходів з дотримання вимог [61].

2) Оцінка ризиків.

Оцінка ризиків кібербезпеки – це процес, який допомагає компанії з'ясувати, як управляти, контролювати та зменшувати ризики кібербезпеки. Він також допомагає приймати рішення та оптимізувати належне реагування. Використання процесу оцінки ризиків може значно зменшити комплаєнс-ризик та покращити процеси управління комплаєнсом. Комапнія може використати шаблон оцінки ризиків для побудови надійного процесу оцінки ризиків незалежно від того, скільки людей працює в організації. Іншим чудовим варіантом є аутсорсинг і залучення команди експертів для проведення оцінки ризиків. Який би варіант не було обрано, дуже важливо ретельно оцінити нашу компанію на предмет слабких місць, щоб уникнути загроз кібербезпеки та керувати вимогами комплаєнсу [38].

3) Комплаєнс-перевірка.

Поширеною помилкою щодо комплаєнсу з кібербезпеки є те, що він передбачає лише технічні рішення. Однак комплаєнс з кібербезпеки також включає юридичні, фінансові, регуляторні, операційні та адміністративні компоненти. Тому компанія повинна мати ефективну програму комплаєнсу з кібербезпеки, яка охоплює ці сфери. І першим кроком до створення ефективної комплаєнс-програми є проведення перевірки на відповідність. Для проведення повної зовнішньої перевірки комплаєнсу організації можуть звернутися до

аутсорсингу, щоб отримати додаткову інформацію та аналіз, які допоможуть їм забезпечити відповідність усім вимогам комплаєнсу [29].

4) Навчання з підвищення обізнаності щодо кібербезпеки.

Ефективний план навчання з підвищення обізнаності щодо кібербезпеки – ще один важливий крок, який компанія може зробити, щоб допомогти задовольнити потреби в дотриманні нормативних вимог і захистити свою організацію від кіберзагроз. Один із способів досягти цього – вимагати від співробітників щорічного проходження навчальних курсів з кібербезпеки та комплаєнсу. Якщо компанія вже проводить певні тренінги з підвищення обізнаності щодо кібербезпеки, можливо, варто оцінити ефективність програми [61]. У рамках цього процесу потрібно оцінити свою поточну базу знань і визначити, де є прогалини. Наприклад, можна виявити, що певні сфери потребують додаткової уваги, наприклад, навчання співробітників інструментам управління мобільними пристроями.

5) Розробка політик та процедур.

Компанія повинна прагнути мати регулярно оновлювані політики та процедури контролю за дотриманням вимог кібербезпеки. Це може включати в себе забезпечення того, щоб співробітники компанії знали політику нашої компанії щодо доступу до конфіденційної інформації, а також те, чи навчені вони розпізнавати фішингові електронні листи. Також можна переконатися, що працівники компанії ознайомлені з найкращими практиками захисту під час доступу до корпоративних систем. Також повинні існувати політики та навчання, коли йдеться про посилення безпеки кінцевих точок. Контроль безпеки є одним з найважливіших методів дотримання вимог безпеки, які може впровадити компанія. Тому команда безпеки компанії повинна забезпечити виконання всіх вимог безпеки за допомогою заходів, політик і процедур безпеки [38].

6) План безперервного моніторингу.

Щоб зменшити ризик, потрібно здійснювати постійний моніторинг для виявлення нових загроз і вразливих місць. Після того, як наша організація

проведе початковий аудит, можна розпочати розробку плану моніторингу відповідності. Почати потрібно з визначення найбільш критичних зон ризику. Крім того, якщо є відомі проблеми, необхідно зосередитися на їх вирішенні в першу чергу. Визначивши потенційні вразливості, необхідно їх негайно усунути. Таким чином, можна запобігти перетворенню потенційних порушень на проблему безпеки [32, 35].

Щоб створити план безперервного моніторингу, команда безпеки компанії повинна спочатку протестувати поточну інфраструктуру безпеки, щоб переконатися, що інструменти працюють належним чином. Потім, на основі цих тестів, необхідно визначити, чи потрібно встановлювати додаткові процедури відповідності вимогам безпеки чи ні. Крім того, команда компанії повинна задокументувати всі політики та процедури безпеки, які вона впроваджує для захисту конфіденційної інформації. Таким чином, документація допоможе систематично узгоджувати потреби в дотриманні нормативних вимог, проводити аудити та переглядати заходи з безпеки вашої організації [40].

У плані має бути зазначено, як часто буде проводитись оцінювання, який тип оцінювання і чи будуть застосовуватись виключно автоматизовані інструменти або на ручна перевірка. Деякі організації використовують комбінацію обох підходів. При виборі підходу важливо враховувати рівень зусиль, який вимагає кожен метод. Наприклад, автоматизовані інструменти зазвичай вимагають менше часу і ресурсів, тоді як ручна перевірка вимагає більше.

На жаль, хакери постійно знаходять нові способи проникнення та викрадення даних, залишаючи вас відкритими для комплаєнс-ризиків. Ось чому моніторинг комплаєнсу з кібербезпеки повинен здійснюватися не тільки регулярно, але й випереджувально. Це означає, що компанії повинні шукати ознаки потенційних порушень до того, як вони відбудуться. Вони також повинні мати план швидкого реагування, якщо порушення відбудеться. Компанії повинні переконатися, що їхні працівники розуміють важливість дотримання вимог кібербезпеки та вживають заходів для захисту від кібератак. Компанія також

повинна визначити, чи буде вона розробляти офіційну політику, яка регулюватиме цей процес, чи вирішить взагалі передати моніторинг комплаєнсу на аутсорсинг.

Отже, узагальнимо основні процедури моніторингу за дотриманням Кодексу етики компанії:

1) компанія повинна створити комплаєнс-групу, відповідальну за моніторинг дотримання етичного кодексу. Ця команда повинна складатися з представників різних відділів, таких як юридичний, кадровий, IT та служба безпеки;

2) відділ комплаєнсу повинен проводити регулярні аудити, щоб переконатися, що всі співробітники дотримуються етичного кодексу. Ці перевірки можуть проводитися як внутрішньо, так і ззовні, залежно від ресурсів та потреб компанії;

3) Компанія повинна проводити регулярні тренінги та навчання для працівників щодо етичного кодексу та його важливості. Це можуть бути тренінги, семінари та онлайн-курси;

4) потрібно розробити політику щодо викривачів, яка заохочує працівників повідомляти про будь-яку неетичну поведінку, свідками якої вони стали або про яку підозрюють. Політика повинна захищати особу викривача та гарантувати, що він не постраждає від помсти;

5) компанія може використовувати технології для контролю за дотриманням етичного кодексу. Наприклад, вона може використовувати програмне забезпечення для моніторингу інтернет-активності, електронної пошти та інших електронних комунікацій. Вона також може використовувати штучний інтелект і алгоритми машинного навчання для виявлення незвичайних моделей поведінки, які можуть свідчити про неетичну поведінку;

6) необхідно проводити ретельну перевірку всіх нових працівників, щоб переконатися, що вони мають хорошу репутацію і не були помічені в неетичній поведінці в минулому;

7) компанія повинна встановити чітку політику та процедури для повідомлення та розслідування звинувачень у неетичній поведінці. Ці політики та процедури повинні бути легко доступними для всіх працівників;

8) потрібно проводити регулярну оцінку ризиків для виявлення сфер потенційних етичних ризиків та розробляти стратегії для їх зменшення;

9) компанія повинна взаємодіяти із зацікавленими сторонами, такими як клієнти, постачальники та регуляторні органи, щоб зрозуміти їхні очікування та занепокоєння щодо етичної ділової практики;

10) важливо порівнювати свої етичні практики з лідерами галузі та колегами, щоб визначити сфери для вдосконалення;

11) компанія повинна гарантувати, що її Кодекс етики узгоджується з відповідними законами та нормативно-правовими актами;

12) керівництво компанії має демонструвати тверду прихильність до етичної поведінки та задавати тон зверху. Вони повинні подавати приклад і заохочувати інших робити те ж саме;

13) можна використовувати сторонніх постачальників для контролю за дотриманням етичного кодексу. Наприклад, вона може найняти зовнішніх аудиторів для проведення незалежного аудиту або використовувати хмарні сервіси, які спеціалізуються на моніторингу комплаєнсу;

14) компанія повинна постійно оцінювати та вдосконалювати свої процедури моніторингу комплаєнсу. Вона повинна бути в курсі останніх етичних стандартів та найкращих практик і відповідно адаптувати свої процедури [29].

Дотримуючись цих процедур, компанія може ефективно контролювати дотримання свого етичного кодексу та гарантувати, що всі працівники дотримуються етичних стандартів.

Впровадження та моніторинг етичного кодексу компанії в сфері кібербезпеки вимагає багатогранної та постійної відданості етичній поведінці та дотриманню нормативних вимог. Описані вище процедури формують надійну основу, яка сприяє розвитку культури доброчесності, прозорості та відповідальної поведінки в організації. Регулярні аудити, відстеження ключових

показників ефективності, моніторинг інцидентів та механізми зворотного зв'язку з питань етики слугують важливими стовпами для забезпечення дотримання етичних норм. Крім того, залучення керівництва, ініціативи з постійного вдосконалення та цілеспрямований нагляд гарантують, що етичні принципи залишатимуться на передньому краї практики кібербезпеки. Старанно впроваджуючи ці процедури, організації можуть зміцнити свій етичний фундамент, підвищити стійкість до кібербезпеки та створити середовище, яке підтримує найвищі стандарти етичної поведінки та досконалості кібербезпеки.

4.3. Формулювання рекомендацій для організацій щодо впровадження етичних норм у сфері кібербезпеки

Впровадження етичних стандартів у сфері кібербезпеки має вирішальне значення для розвитку культури відповідальної поведінки, зміцнення довіри користувачів та зменшення ризиків. Наведемо рекомендації для організацій щодо ефективного впровадження етичних стандартів у сфері кібербезпеки:

1. Встановіть чіткі етичні принципи – створіть чіткий і всеосяжний кодекс етики.

Організації повинні розробити етичний кодекс, який визначає етичні принципи та поведінку, що очікується від їхніх працівників. Кодекс має бути чітким, стислим і зрозумілим для всіх працівників

2. Призначте керівника служби інформаційної безпеки.

Організації повинні призначити керівника з інформаційної безпеки, який відповідає за нагляд за заходами з кібербезпеки та забезпечення їх відповідності етичним принципам. Керівник служби інформаційної безпеки повинен володіти необхідними навичками та досвідом для управління ризиками кібербезпеки та забезпечення дотримання етичних стандартів.

3. Комітети з етики або відповідальні за комплаєнс.

Потрібно призначити спеціальні комітети з етики або відповідальних за комплаєнс, відповідальних за нагляд за впровадженням етичних стандартів у сфері кібербезпеки, забезпечення їх дотримання та постійного вдосконалення.

4. Проводьте навчання та тренінги.

Потрібно заохочувати постійне навчання та підвищення обізнаності працівників щодо найкращих практик кібербезпеки та етичних міркувань. Це повинно включати регулярні тренінги, інформаційні програми, воркшопи та семінари з кібербезпеки та етики зосереджені на етичних аспектах кібербезпеки. Таке навчання має охоплювати такі теми, як конфіденційність, захист даних та найкращі практики кібербезпеки. Потрібно інформувати співробітників про важливість етичної поведінки, конфіденційності даних та дотримання нормативно-правових вимог.

5. Впроваджуйте надійні стратегії оцінки та зменшення ризиків.

Організації повинні впроваджувати надійні стратегії оцінки та зменшення ризиків, які надають пріоритет як безпеці, так і конфіденційності. Це має включати регулярну оцінку вразливостей, тестування на проникнення та планування реагування на інциденти.

6. Сприяйте культурі прозорості та відкритої комунікації.

Організаціям слід розвивати культуру прозорості та відкритої комунікації щодо ризиків та інцидентів кібербезпеки. Це повинно включати регулярне звітування про прогрес у дотриманні етичних стандартів та залучення зацікавлених сторін до процесів прийняття рішень.

7. Залучайте зовнішніх експертів та консультантів.

Організації повинні залучати зовнішніх експертів та консультантів, коли це необхідно для забезпечення дотримання відповідних законів, нормативних актів та найкращих практик, пов’язаних з етичною кібербезпекою.

8. Постійно контролюйте та оцінюйте системи та процеси кібербезпеки.

Організації повинні постійно контролювати та оцінювати свої системи та процеси кібербезпеки на предмет виявлення нових загроз та етичних проблем.

Це повинно включати регулярні аудити та оцінки безпеки для визначення сфер, які потребують вдосконалення.

9. Інтегруйте етичні стандарти в політику та практику.

Потрібно інтегрувати етичні стандарти в існуючі політики, процедури та операційні рамки кібербезпеки, що дасть змогу забезпечити відповідність передовим галузевим практикам і глобальним етичним нормам.

10. Створіть етичні рамки прийняття рішень.

Рамки або моделі прийняття рішень допоможуть працівникам організації приймати етичні рішення, коли вони стикаються з викликами або дилемами у сфері кібербезпеки.

11. Розробляйте плани реагування на інциденти.

Потрібно розробити плани реагування на інциденти, які враховують як технічні, так і етичні міркування. Організації повинні включати процедури реагування на витоки даних та несанкціонований доступ, а також комунікаційні стратегії для зацікавлених сторін.

12. Розгляньте можливість створення внутрішньої або зовнішньої консультативної ради.

Організаціям слід розглянути можливість створення внутрішньої або зовнішньої консультативної ради, що складається з галузевих експертів, фахівців з етики та інших зацікавлених сторін, для забезпечення керівництва та нагляду за етичними питаннями кібербезпеки.

13. Підзвітність та наслідки.

Потрібно встановити відповідальність за недотримання етичних стандартів у сфері кібербезпеки. Визначити наслідки за порушення етичного кодексу та забезпечити послідовність у застосуванні дисциплінарних заходів [31; 33; 40].

Детальніше розглянемо такий важливий для організацій напрям щодо впровадження етичних норм у сфері кібербезпеки, як навчання та тренінги. Впровадження комплексних програм навчання та підвищення обізнаності щодо етичних норм у сфері кібербезпеки має вирішальне значення для того, щоб

співробітники розуміли, приймали та застосовували етичні принципи у своїй повсякденній діяльності. Ефективні ініціативи з навчання та підвищення обізнаності включають наступне:

- розробка спеціалізованих навчальних модулів, присвячених саме етичним аспектам кібербезпеки. Потрібно адаптувати зміст до різних ролей співробітників, забезпечуючи відповідність їхнім обов'язкам;

- важливо висвітлювати такі фундаментальні етичні принципи, як конфіденційність даних, цілісність, підзвітність, дотримання нормативних вимог та відповідальне використання технологій;

- потрібно включити реальні приклади та сценарії, що висвітлюють етичні дилеми та виклики в сфері кібербезпеки. Ці приклади допомагають працівникам зрозуміти, як етичні рішення впливають на практику кібербезпеки;

- необхідно проводити інтерактивні семінари, рольові ігри або симуляції, які моделюють етичні дилеми, з якими можуть зіткнутися працівники. А також заохочувати дискусії та критичне мислення для вирішення етичних проблем;

- важливим є ознайомлення з працівників етичними настановами та політиками, зокрема з етичним кодексом організації та політикою кібербезпеки. Необхідно пояснити значення етичних принципів та їхню роль у підтримці доброчесності організації;

- потрібно запросити експертів з кібербезпеки, фахівців з етики або запрошених спікерів для проведення сесій, присвячених етичним аспектам кібербезпеки. Їхні знання та досвід можуть стати цінним джерелом інформації для співробітників;

- необхідно пропонувати регулярні оновлення та курси підвищення кваліфікації з етичних норм у сфері кібербезпеки. З розвитком технологій та появою нових загроз працівників потрібно інформувати про новітні етичні практики;

- потрібно проводити практичні тренінги з етичного прийняття рішень у сфері кібербезпеки. Надайте рекомендації щодо оцінки етичних наслідків та прийняття обґрунтованих рішень у різних сценаріях кібербезпеки;

- необхідно надати доступ до навчальних онлайн-ресурсів, вебінарів або платформ електронного навчання, присвячених етиці кібербезпеки. Ці ресурси пропонують гнучкість і можливості для самостійного навчання;

- важливим кроком є організація заходів, дискусій чи форумів, які сприяють розвитку етичної культури. Заохочення працівників ділитися етичними дилемами, з якими вони стикаються у своїй роботі, та обговорювати найкращі практики;

- потрібно оцінювати розуміння працівниками етичних норм за допомогою тестів, оцінювання чи сертифікації; пропонувати визнання або сертифікати за проходження навчальних програм з етики;

- необхідно заохочувати зворотній зв’язок від учасників, щоб постійно вдосконалювати навчальні програми. Важливим є врахування пропозицій та адаптація навчального контенту до потреб і викликів, що змінюються [28].

Шляхом реалізації детальних та цілеспрямованих програм навчання та підвищення обізнаності щодо етичних норм у сфері кібербезпеки, організації надають своїм працівникам можливість приймати обґрунтовані етичні рішення, забезпечуючи захист конфіденційних даних та дотримання етичних стандартів у своїй практиці кібербезпеки.

Впроваджуючи окреслені рекомендації, організації можуть створити надійну основу, яка інтегрує етичні стандарти у свої практики кібербезпеки, сприяючи розвитку культури доброчесності, довіри та відповідальної поведінки у захисті цифрових активів та інформації користувачів. Це дасть змогу побудувати довіру з клієнтами, захистити цінні активи та зберегти міцну репутацію, дотримуючись етичних стандартів у швидкозмінному ландшафті кібербезпеки.

ВИСНОВКИ

Вивчивши теоретичні і практичні аспекти етичних норм світових стандартів в управлінні кібербезпекою, можемо сформулювати наступні висновки.

1. Етичні норми у сфері кібербезпеки мають важливе значення для забезпечення того, щоб фахівці та організації з кібербезпеки діяли відповідально та в інтересах суспільства. Дотримуючись цих норм, фахівці з кібербезпеки можуть зробити позитивний внесок у розвиток цифрового світу та сприяти формуванню культури довіри, безпеки та конфіденційності. Дотримання ключових етичних стандартів у сфері кібербезпеки слугує основою для встановлення довіри, доброчесності та надійності в цифровій сфері. Дотримання таких принципів, як прозорість, підзвітність і повага до приватного життя, не лише захищає конфіденційну інформацію, але й забезпечує відповідальну та етичну поведінку фахівців з кібербезпеки. Надаючи пріоритет цим етичним стандартам, фахівці в цій галузі можуть орієнтуватися в складному ландшафті викликів кібербезпеки, одночасно зменшуючи ризики та захищаючи права і безпеку людей і організацій. Дотримання цих принципів не лише сприяє розвитку культури етичної поведінки, але й робить значний внесок у побудову більш безпечної та надійної цифрової екосистеми на благо суспільства в цілому.

2. Глобальні стандарти і норми кібербезпеки мають значний вплив на етичні питання, пов’язані з кіберпростором. Вони допомогли створити спільну мову і рамки для розуміння і подолання ризиків кібербезпеки, сприяють пропорційності, захисту приватного життя, а також підвищенню підзвітності та прозорості. Незважаючи на досягнутий прогрес, попереду ще багато викликів, пов’язаних із забезпеченням широкого прийняття і впровадження глобальних стандартів і норм, а також з необхідністю йти в ногу зі швидкою еволюцією кіберпростору. Тим не менш, встановлення глобальних стандартів і норм кібербезпеки є важливим кроком на шляху до створення більш безпечного і захищеного кіберсередовища, яке поважає етичні принципи і цінності. Існують

різні міжнародні керівні принципи та рамки, які визначають етичні стандарти кібербезпеки, такі як Рамки кібербезпеки Національного інституту стандартів і технологій (NIST), Загальний регламент захисту даних Європейського Союзу (GDPR) і стандарти Міжнародної організації зі стандартизації (ISO). Ці керівні принципи забезпечують базову основу для етичних практик кібербезпеки і допомагають організаціям орієнтуватися в складному ландшафті загроз і ризиків кібербезпеки. Досягнення балансу між глобальними стандартами кібербезпеки та етичними міркуваннями залишається суттєвим викликом, що вимагає постійної оцінки та адаптації для вирішення етичних проблем, які виникають у цифровому середовищі.

3. Залучення зацікавлених сторін до етичних міркувань у сфері кібербезпеки має вирішальне значення для забезпечення інтеграції етичних принципів у протоколи та практики кібербезпеки. Зацікавлені сторони повинні включати працівників, клієнтів, партнерів та постачальників, на яких впливають заходи з кібербезпеки. Організації повинні інформувати зацікавлені сторони про свої етичні принципи і практики та запитувати зворотній зв’язок, щоб покращити свій підхід до етичної кібербезпеки. Інтеграція етики в протоколи і практики кібербезпеки – це безперервний процес, який вимагає постійних зусиль і уваги. Дотримуючись семи кроків, описаних вище, організації можуть гарантувати, що їхні зусилля з кібербезпеки відповідають їхнім цінностям і принципам, і що вони виконують свої етичні зобов’язання перед зацікавленими сторонами. Зрештою, інтеграція етики в протоколи і практики кібербезпеки має важливе значення для побудови довіри і авторитету в сучасну цифрову епоху.

4. Управління кібербезпекою стикається з безліччю етичних проблем і питань, які можуть мати значні наслідки для організацій, окремих осіб і суспільства в цілому. Найбільш актуальними етичними проблемами в управлінні кібербезпекою є наступні: 1) баланс між безпекою та конфіденційністю; 2) право власності на дані та контроль над ними; 3) заходи протидії кібератакам; 4) оприлюднення вразливостей; 5) управління ризиками ланцюга постачання; 6) штучний інтелект і машинне навчання; 7) людський фактор. Фахівці з

кібербезпеки повинні приймати складні рішення, які можуть мати далекосяжні наслідки. Надаючи пріоритет етичним міркуванням і застосовуючи проактивний підхід до вирішення цих проблем, організації можуть зміцнити довіру, захистити свої активи, а також забезпечити безпеку і благополуччя своїх зацікавлених сторін.

5. Набір міжнародних стандартів, що стосуються різних аспектів управління кібербезпекою, хоч і не зосереджені безпосередньо на етичних міркуваннях, за своєю суттю сприяють створенню середовища, сприятливого для етичних практик у цифровій сфері. Такі стандарти, як ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27031, ISO/IEC 27032, ISO/IEC 27701 та інші, закладають основу для надійної інформаційної безпеки, управління конфіденційністю та мережевої безпеки. Ці стандарти наголошують на захисті конфіденційної інформації, створенні безпечних систем та дотриманні законодавчих і нормативних рамок. Опосередковано вони сприяють етичним практикам кібербезпеки, заохочуючи відповідальну поведінку, захищаючи конфіденційність та підтримуючи цілісність і доступність критично важливих інформаційних активів. Хоча етичні міркування не сформульовані явно, вони пронизують ці стандарти, формуючи важливе підґрунтя для створення культури довіри, доброчесності та відповідальної поведінки в постійно мінливому ландшафті управління кібербезпекою.

6. Управлінські рішення суттєво впливають на етичні аспекти кібербезпеки різними способами, як позитивними, так і негативними. Визнаючи цей вплив і проактивно вирішуючи потенційні конфлікти, організації можуть створити надійне середовище кібербезпеки, яке збалансовує імперативи безпеки з етичними міркуваннями, що в кінцевому підсумку сприятиме безпеці та довірі до їхньої цифрової екосистеми. Дотримання етичних стандартів у сфері кібербезпеки має важливе значення для захисту як організаційних, так і суспільних інтересів. Недотримання етичних стандартів може призвести до втрати суспільної довіри, правових наслідків, фінансових наслідків, крадіжки інтелектуальної власності, шкоди репутації, а в екстремальних випадках – до

втрати людських життів. Організації повинні визнати важливість етичних стандартів у сфері кібербезпеки і вжити заходів для їх інтеграції в свої протоколи і практики безпеки. Це не лише принесе користь організації, але й допоможе створити безпечнішу онлайн-спільноту для всіх.

7. Етичний корпоративний кодекс – це документ, який визначає цінності, принципи та стандарти поведінки, що очікуються від працівників та зацікавлених сторін в організації. Етичні корпоративні кодекси відіграють життєво важливу роль у заохоченні етичної поведінки, створенні позитивної корпоративної культури, наданні рекомендацій, заохоченні дотримання законів і правил, сприянні прозорості та підзвітності, зміцненні репутації, підтримці управління ризиками, сприянні навчанню та освіті, заохоченні до прийняття етичних рішень і побудові довіри. Впроваджуючи етичні корпоративні кодекси у свою діяльність, компанії можуть гарантувати, що вони ведуть свій бізнес етично та відповідально, що, зрештою, сприяє їхньому довгостроковому успіху та сталому розвитку. Етичні корпоративні кодекси слугують керівними документами, узгоджуючи організаційну поведінку з етичними принципами, сприяючи формуванню культури доброчесності, довіри та відповідальної поведінки всередині компанії та її взаємодії із зацікавленими сторонами. Регулярний перегляд, посилення та впровадження цих кодексів є важливими для підтримки етичної корпоративної культури.

8. Дотримання етичних принципів, пов’язаних із захистом даних, конфіденційністю та безпекою, допомагає побудувати довіру з клієнтами та захистити конфіденційну інформацію. Організації, які дотримуються етичних кодексів, можуть зменшити кіберзагрози та сприяти створенню безпечнішого та надійнішого цифрового середовища. Етичні кодекси у сфері кібербезпеки мають важливе значення для захисту конфіденційної інформації, запобігання кібератакам, розбудови довіри та дотримання регуляторних вимог. Хоча впровадження етичних кодексів пов’язане з певними труднощами, їхні переваги значно перевищують витрати. Оскільки технології продовжують розвиватися, а

кіберзагрози еволюціонують, етичні кодекси повинні адаптуватися до нових викликів.

9. Розробка етичного кодексу компанії, який враховує світові стандарти та етичні норми у сфері кібербезпеки, передбачає спільний ітеративний процес, спрямований на узгодження організаційних цінностей із загальноприйнятими етичними принципами. Адже, етичний кодекс слугує керівництвом для прийняття етичних рішень та поведінки, сприяючи розвитку культури доброчесності та відповідальних практик кібербезпеки в компанії.

10. Впровадження та моніторинг етичного кодексу компанії в сфері кібербезпеки вимагає багатогранної та постійної відданості етичній поведінці та дотриманню нормативних вимог. Описані вище процедури формують надійну основу, яка сприяє розвитку культури доброчесності, прозорості та відповідальної поведінки в організації. Регулярні аудити, відстеження ключових показників ефективності, моніторинг інцидентів та механізми зворотного зв’язку з питань етики слугують важливими стовпами для забезпечення дотримання етичних норм. Крім того, залучення керівництва, ініціативи з постійного вдосконалення та цілеспрямований нагляд гарантують, що етичні принципи залишатимуться на передньому краї практики кібербезпеки. Старанно впроваджуючи ці процедури, організації можуть зміцнити свій етичний фундамент, підвищити стійкість до кібербезпеки та створити середовище, яке підтримує найвищі стандарти етичної поведінки та досконалості кібербезпеки.

11. Впроваджуючи такі рекомендації як чіткі етичні принципи; призначення керівника служби інформаційної безпеки; комітети з етики або відповідальні за комплаєнс; навчання та тренінги; надійні стратегії оцінки та зменшення ризиків; сприяння культурі прозорості та відкритої комунікації; залучення зовнішніх експертів та консультантів; постійний контроль та оцінка системи та процеси кібербезпеки; інтеграція етичних стандартів в політику та практику; етичні рамки прийняття рішень; плани реагування на інциденти; створення внутрішньої або зовнішньої консультативної ради; відповідальність за недотримання етичних стандартів у сфері кібербезпеки, організації можуть

створити надійну основу, яка інтегрує етичні стандарти у свої практики кібербезпеки, сприяючи розвитку культури доброчесності, довіри та відповідальної поведінки у захисті цифрових активів та інформації користувачів. Це дасть змогу побудувати довіру з клієнтами, захистити цінні активи та зберегти міцну репутацію, дотримуючись етичних стандартів у швидкозмінному ландшафті кібербезпеки.

Наукове використання здобутих результатів можливе в процесі вивчення студентами курсів «Корпоративна та професійна етика в кібербепеці», «Кібербезпека та захист інформації», «Етика кібербезпеки», «Основи кібербезпеки та кібероборони» тощо.

Практичне значення роботи полягає в можливості застосування її результатів в процесі розробки або вдосконалення етичних кодексів компаній, який враховує світові стандарти та етичні норми в кібербезпеці і впровадження запропонованих рекомендацій щодо етичних норм у сфері кібербезпеки компаній.

ПЕРЕЛІК ПОСИЛАНЬ

1. Андрійченко Ж., Близнюк Т., Майстренко О. Digital етикет та комунікації: тенденції та вимоги сьогодення. *Економіка та суспільство.* 2021. №34. URL: https://doi.org/10.32782/2524-0072/2021-34-24 (дата звернення: 03.11.2023)

2. Головіна Н. І. Регулятивний потенціал інформаційної етики. *Філософські обрії*: Наук.-теорет. журн. / Ін-т філософії імені Г. С. Сковороди НАН України, Полтав. нац. пед. ун-т імені В. Г. Короленка. Вип. 42. Київ; Полтава, 2019. С. 160-164. URL: http://dspace.pnpu.edu.ua/bitstream/123456789/16440/1/39.pdf (дата звернення: 07.11.2023)

3. Горбенко О. Нове регулювання кібербезпеки в контексті міжнародного досвіду. Uz.ligazakon. 2018. URL: https://uz.ligazakon.ua/ua/magazine_article/EA011604 (дата звернення: 11.11.2023)

4. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Вид. друге, перероб. та доп. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

5. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань»: монографія. Київ-Одеса: Фенікс, 2021. 176 с.

6. Завадський А. А. Інформаційна та кібербезпека адвокатської діяльності: теоретичні та практичні аспекти (досвід США). *Порівняльно-аналітичне право*. 2020. №1. С. 321-323. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/35837/1/%D0%86%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90%20%D0%A2%D0%90%20%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90.pdf (дата звернення: 12.11.2023)

7. Кавка О. М. Нетикет у соціальних мережах. *Актуальні питання гуманітарних наук*: міжвузівський збірник наукових праць молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка.

2021. Випуск 19. Том 1. С. 166–170. URL: http://zfs-journal.uzhnu.uz.ua/archive/19/part_1/30.pdf (дата звернення: 14.11.2023)

8. Капустіна Н., Токар Л. Цифрова етика: навч.-метод. реком.; Нац.ун-т «Одес. юрид. академія». Одеса: Фенікс, 2023. 50 с.

9. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ, 2023. №7 (липень). 270 с.

10. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. Київ, 2023. №9 (вересень). 351 с.

11. Кібербезпека держави: підручник / В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.; в 2 т. Т. 2. / за заг. ред. В.В. Остроухова. Київ: ДНУ «Книжкова палата України», 2016. 328 с.

12. Кодекс етики та ділової поведінки компанії. *ADU*. 2023. URL: https://adu.com.ua/pro-kompaniiu/kodeks-etyky-ta-dilovoi-povedinky-kom/ (дата звернення: 15.11.2023)

13. Кодекс корпоративної етики. *Mologa osvita*. 2023. URL: https://mologa-osvita.gov.ua/kodeks-korporativnoi-etiki-09-02-15-17-07-2020/ (дата звернення: 17.11.2023)

14. Кормич Б.А. Кібербезпека: організаційно-правові основи: навч. посібн. Київ: Кондор, 2008. 382 с.

15. Кубко В. П. Процес створення корпоративних кодексів. Труды Одесского политехнического университета. 2007. Вип. 2 (28). С. 314-317. URL: https://pratsi.op.edu.ua/app/webroot/articles/1312545882.pdf (дата звернення: 21.11.2023)

16. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.

17. Мартинюк В.М., Ісаєнко Т.К. Інформаційна етика: наповнення поняття. *Людина в інформаційному просторі*: матеріали ІІ Всеукраїнської наук.-практ. Інтернет-конф., м. Кременчук, 14 грудня 2016 р. С. 143– 145. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/1784/3/2_%D0%9C%D0%B0%D1%80%D1%82%D0%B8%D0%BD%D1%8E%D0%BA%2C%20%D0%86%D1%81%D0%B0%D1%94%D0%BD%D0%BA%D0%BE_%D0%A1%D1%82%D0%B0%D1%82%D1%82%D1%8F.pdf (дата звернення: 22.11.2023)

18. Миролюбенко Г. Місце та роль спільнот в інтернет-комунікації. Гілея. *Історичні науки. Філософські науки. Політичні науки*. 2011. Вип. 45 (№ 3). С. 311–318.

19. Пєтков С. В., Журавльов Д. В., Дрозд О. Ю., Дрозд В. Г. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика. Видавнитво ЦУЛ, 2022. 460 с.

20. Пігош В. А. Кодекс корпоративної етики як інструмент розвитку потенціалу підприємств. *Науковий вісник Мукачівського державного університету.* Серія «Економіка»: збірник наукових праць / гол. ред. Т.В. Черничко. Мукачево: МДУ, 2020. Вип. 1(13). С. 104-107. URL: http://dspace-s.msu.edu.ua:8080/bitstream/123456789/7256/1/Code%20_of%20_corporate_%20ethics%20_as_%20a_%20tool_%20for_%20developing_%20the_%20potential%20_of_%20enterprises.pdf (дата звернення: 24.11.2023)

21. Плескач М. В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. *Часопис Київського університету права*. 2020. №4. С. 201-209. https://doi.org/10.36695/2219-5521.4.2020.36. URL: https://chasprava.com.ua/index.php/journal/article/view/568 (дата звернення: 25.11.2023)

22. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 26.11.2023)

23. Про План реалізації Стратегії кібербезпеки України: РНБО; Рішення, План від 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 28.11.2023)

24. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.11.2023)

25. Сертифікат ISO/IEC 27701:2019 як підтвердження захисту персональних даних. Denovo. 23.02.2022. URL: https://denovo.ua/blog/sho-take-iso-27701-2019 (дата звернення: 01.12.2023)

26. Тарасюк А. В. Теоретико-правове підґрунтя інформаційної етики в системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52. URL: http://biblio.umsf.dp.ua/jspui/bitstream/123456789/4264/1/12%20%d0%a2%d0%b0%d1%80%d0%b0%d1%81%d1%8e%d0%ba%20%d0%90.%20%d0%92..pdf (дата звернення: 03.12.2023)

27. Филиппова Л., Зеленецкий В. Компьютерная этика. Морально-этические и правовые нормы для пользователей компьютерных сетей : учебное пособие. Харьков: Кроссроуд, 2006. 266 с.

28. A Holistic Approach to Ethical Issues in Cyber Security. *Swisscyberinstitute*. 15.04.2021. URL: https://swisscyberinstitute.com/blog/a-holistic-approach-to-ethical-issues-in-cyber-security/ (дата звернення: 07.12.2023)

29. Best Practices for Cybersecurity Compliance Monitoring. Marcumllp. 29.08.2023. URL: https://www.marcumllp.com/insights/best-practices-for-cybersecurity-compliance-monitoring (дата звернення: 09.12.2023)

30. Bynum T. Computer and Information Ethics. The Stanford Encyclopedia of Philosophy. Edward N. Zalta (ed.). 2018. URL: https://plato.stanford.edu/archives/sum2018/entries/ethics-computer/ (дата звернення: 11.12.2023)

31. Chin K. Cybersecurity and Social Responsibility: Ethical Considerations. *Upguard.* 21.08.2023. URL: https://www.upguard.com/blog/cybersecurity-ethics (дата звернення: 12.12.2023)

32. Cybersecurity Ethics: Establishing a Code for Your SOC. Securityintelligence. 2023. URL: https://securityintelligence.com/articles/cybersecurity-ethics-establishing-a-code-of-conduct-for-soc/ (дата звернення: 14.12.2023)

33. Cybersecurity Ethics: What Cyber Professionals Need to Know. Augusta. 2023. URL: https://www.augusta.edu/online/blog/cybersecurity-ethics (дата звернення: 03.11.2023)

34. Cybersecurity Standards and Frameworks. Itgovernanceusa. 2023. URL: https://www.itgovernanceusa.com/cybersecurity-standards (дата звернення: 12.11.2023)

35. Ethics of Artificial Intelligence and Robotics. plato.stanford. 30.04.2020. URL: https://plato.stanford.edu/entries/ethics-ai/ (дата звернення: 26.11.2023)

36. Ethics in Cyber Security: Everything You Need to Know. 2023. URL: https://www.elev8me.com/insights/guide-to-ethics-in-cyber-security (дата звернення: 14.11.2023)

37. Ethical Issues in Cybersecurity. Futureoftech. 2023. URL: https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/ (дата звернення: 24.11.2023)

38. Governance, Risk, and Compliance (GRC) Framework. Metricstream. 2023. URL: https://www.metricstream.com/whitepapers/GRC-framework.htm (дата звернення: 26.11.2023)

39. Harvey A. The Ultimate Guide to ISO 27002. ISMS. 14.12.2023. URL: https://www.isms.online/iso-27002/ (дата звернення: 07.11.2023)

40. Impe Van K. Cybersecurity Ethics: Establishing a Code for Your SOC. *Securityintelligence*. 08.01.2021. URL: https://securityintelligence.com/articles/cybersecurity-ethics-establishing-a-code-of-conduct-for-soc/ (дата звернення: 09.11.2023)

41. Irwin L. ISO 27001 vs. ISO 27002: What's the difference? Itgovernance.co. 22.07.2021. URL: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002 (дата звернення: 02.12.2023)

42. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. *ISO*. 2023. URL: https://www.iso.org/standard/75652.html (дата звернення: 03.12.2023)

43. ISO/IEC 27031 2011 Standard. *Itgovernanceusa*. 2023. URL: https://www.itgovernanceusa.com/shop/product/isoiec-27031-2011-standard (дата звернення: 03.12.2023)

44. ISO/IEC 27032:2023 Cybersecurity. Guidelines for Internet security. *ISO*. 2023. URL: https://www.iso.org/standard/76070.html (дата звернення: 03.12.2023)

45. ISO 27001, the International Information Security Standard. *Itgovernanceusa*. 2023. URL: https://www.itgovernance.co.uk/blog/understanding-the-differences-between-iso-27001-and-iso-27002 (дата звернення: 05.12.2023)

46. ISO 27701 The international standard for privacy information management. *Itgovernanceusa*. 2023. URL: https://www.itgovernanceusa.com/iso-27701 (дата звернення: 11.12.2023)

47. Lee W. W., Zankl W., Chang H. An Ethical Approach to Data Privacy Protection. *ISACA*. 24.12.2016. URL: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection (дата звернення: 12.12.2023)

48. Lewis J. A. Creating Accountability for Global Cyber Norms. *CSIS*. 23.02.2022. URL: https://www.csis.org/analysis/creating-accountability-global-cyber-norms (дата звернення: 06.12.2023)

49. Limaj B. Ethical Considerations in AI-Powered Cybersecurity. *Medium*. 15.02.2023. URL: https://medium.com/@besniklimaj/ethical-considerations-in-ai-powered-cybersecurity-45cd83db90e0 (дата звернення: 05.12.2023)

50. Maalem Lahcen R. A., Caulkins B., Mohapatra R. et al. Review and insight on the behavioral aspects of cybersecurity. *Cybersecur* 3. 2020. №10. URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00050-w#citeas (дата звернення: 07.12.2023)

51. Maimon D., Louderback E. R. Cyber-Dependent Crimes: An Interdisciplinary Review. *Ann Rev Criminol*. 2019. №2(1). С. 191–216. URL: https://doi.org/10.1146/annurev-criminol-032317-092057. (дата звернення: 01.12.2023)

52. Morgan G., Gordijn B. A Care-Based Stakeholder Approach to Ethics of Cybersecurity in Business. In: Christen, M., Gordijn, B., Loi, M. (eds) The Ethics of Cybersecurity. *The International Library of Ethics, Law and Technology*. 2020. Vol 21. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-29053-5_6 (дата звернення: 07.12.2023)

53. Morrow S. Five ethical decisions cybersecurity pros face: What would you do? Resources.infosecinstitute. 11.07.2022. URL: https://resources.infosecinstitute.com/topics/industry-insights/five-ethical-decisions-cybersecurity-pros-face-what-would-you-do/ (дата звернення: 09.12.2023)

54. Payne B. K., Hadzhidimova L. Cyber security and criminal justice programs in the United States: Exploring the intersections. *Int J Crim Justice Sci*. 2018. №13(2). P. 385–404.

55. Ronald J. Deibert. Toward a Human-Centric Approach to Cybersecurity. Cambridge University Press. 2018. URL: https://www.cambridge.org/core/journals/ethicsand-international-affairs/article/abs/toward-a-humancentric-approach-to-cybersecurity/4E8819984202A24186BB0F52E51BC1E4#access-block (дата звернення: 07.12.2023)

56. Sadeghi B., Richards D., Formosa P., McEwan M., Bajwa M.H.A., Hitchens M., Ryan M. Modelling the ethical priorities influencing decision-making in cybersecurity contexts. Organizational Cybersecurity Journal: Practice, Process and People. 2023. Vol. 3 No. 2, pp. 127-149. URL: https://doi.org/10.1108/OCJ-09-2022-0015 (дата звернення: 05.12.2023)

57. Search Engines and Ethics. Plato.stanford. 11.08.2020. URL: https://plato.stanford.edu/entries/ethics-search/ (дата звернення: 02.12.2023)

58. The Ethical Dilemmas of Cybersecurity: Balancing Privacy and Security. *Medium.* 11.09.2023. URL: https://medium.com/@skillfloor_29561/the-ethical-

dilemmas-of-cybersecurity-balancing-privacy-and-security-318adcf949a3 (дата звернення: 03.12.2023)

59. The Ethics of Cybersecurity: Debating the Gray Areas. *Sennovate*. 2023. URL: https://sennovate.com/the-ethics-of-cybersecurity-debating-the-gray-areas/ (дата звернення: 04.12.2023)

60. The Importance of Ethics in Information Security. *RiskOptics.* 26.02.2021. URL: https://reciprocity.com/the-importance-of-ethics-in-information-security/ (дата звернення: 07.12.2023)

61. Tunggal A. T. Best Practices for Cybersecurity Compliance Monitoring in 2023. 06.04.2023. URL: https://www.upguard.com/blog/compliance-monitoring (дата звернення: 30.11.2023)

62. Witzsche M. The challenges and ethical considerations of AI and ML in cybersecurity [part 2]. *Linkedin.* 12.07.2023. URL: https://www.linkedin.com/pulse/challenges-ethical-considerations-ai-ml-cybersecurity-witzsche/ (дата звернення: 24.11.2023)