**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: “МЕТОДИ ВИРІШЕННЯ СКЛАДНИХ ЕТИЧНИХ СИТУАЦІЙ 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*

_____ Леонід НОВИК
*(підпис)* *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Леонід НОВИК

Керівник:
ст. викладач Дмитро РАБЧУН

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

**Київ 2024**

**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 Новику Леоніду Анатолійовичу
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи: " Методи вирішення складних етичних ситуацій в управлінні кібербезпекою"

керівник кваліфікаційної роботи Дмитро РАБЧУН, ст. викладач
*(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: *етика у кібербезпеці, інформаційна безпека підприємств, методи та засоби управління інформаційною безпекою, нормативні документи, міжнародні стандарти, наукова та технічна література*.

4. Перелік питань, які потрібно розробити:
   1. Провести аналіз літератури та наукових джерел щодо етичних аспектів управління кібербезпекою.
   2. Визначити складні етичні ситуації в галузі кібербезпеки, розглядаючи приклади інцидентів та дилем.
   3. Дослідити різні стратегії вирішення етичних викликів у контексті кібербезпеки.
   4. Аналізувати стандарти та рекомендації, що визначають етичну поведінку в галузі кібербезпеки.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання "02" жовтня 2023 р.

## КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

| № з/п | Етапи кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 10.10.2023 | виконано |
| 2. | Збір та аналіз літератури. | 23.10.2023 | виконано |
| 3. | Аналіз основних характеристик інформаційного протиборства. | 27.10.2023 | виконано |
| 4. | Дослідження особливостей етичних ситуацій в управління інформаційною безпекою. | 10.11.2023 | виконано |
| 5. | Визначення напрямів та методів врегулювання складних етичних ситуацій у кібербезпеці. | 15.11.2023 | виконано |
| 6. | Формулювання висновків за результатами проведеного дослідження. | 22.11.2023 | виконано |
| 7. | Оформлення роботи. | 04.12.2023 | виконано |
| 8. | Оформлення презентації. | 14.12.2023 | виконано |
| 9. | Отримання рецензії на роботу. | 18.12.2023 | виконано |
| 10. | Захист в ДЕК. | 17.01.2024 | виконано |

Здобувач вищої освіти _____ Леонід НОВИК
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
*(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 Новик Л.А. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*

за спеціальністю 125 Кібербезпека
*(код, найменування спеціальності)*

Освітньо-професійної програми Управління інформаційною безпекою
*(назва)*

на тему: “ Методи вирішення складних етичних ситуацій в управлінні кібербезпекою ”
Кваліфікаційна робота і рецензія додаються.

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

**Висновок керівника кваліфікаційної роботи**

Здобувач **НОВИК Леонід** у кваліфікаційній роботі дослідив сучасний стан управління та вирішення складних етичних ситуацій, що дало змогу зробити правильний висновок про необхідність застосування сучасних стандартів при відпрацюванні нових підходів до розроблення способів і методів вирішення складних ситуацій в управлінні. Розроблена у роботі методика включає практичні рекомендації керівникам структурних підрозділів кібербезпеки, які орієнтовані на вдосконалення стратегій управління та підвищення рівня захисту в інформаційних системах. Розроблені критерії оцінки ефективності можуть слугувати інструментом практичного оцінювання заходів інформаційної безпеки у організаціях.

**НОВИК Леонід** 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 здобувачки **НОВИКА Леоніда** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2024 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Новик Л.А. 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 Новика Леоніда Анатолійовича
на тему “ МЕТОДИ ВИРІШЕННЯ СКЛАДНИХ ЕТИЧНИХ СИТУАЦІЙ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ ”

**Актуальність**

Актуальність даної теми полягає в тому, що, незважаючи на великі успіхи у сфері кібербезпеки, етичні аспекти не завжди враховуються в стратегіях і прийнятті рішень. Це може мати серйозні наслідки для окремих осіб, організацій і суспільства в цілому.

**Позитивні сторони**

Здійснений аналіз наукової літератури та публікацій, пов'язаних із методами вирішення етичних ситуацій в управлінні, визначив потребу у пошуку та відпрацюванні методики прогнозування з урахуванням досягнень у галузі інформаційної безпеки. На основі аналізу розроблений метод для вирішення складних етичних ситуацій та конкретні рекомендації для практичного впровадження в області безпеки інформаційних систем. Рекомендації орієнтовані на вдосконалення стратегій управління та підвищення рівня захисту в інформаційних системах.

Вказане дослідження слугує наріжним каменем для прийняття рішень керівним складом підрозділів кібербезпеки, формування політики та розвитку практик захисту інформації.

**Недоліки**

Недостатньо приділено уваги застосуванню штучного інтелекту при відпрацюванні методики прогнозування інцидентів. 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 Новик Леонід Анатолійович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач 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: 74 стор., 6 рис., 1 табл., 64 джерела.

***Метою роботи*** є дослідження у вивченні та аналізі методів вирішення складних етичних ситуацій в управлінні кібербезпекою.

***Об'єктом дослідження*** є процеси управління кібербезпекою в сучасному інформаційному середовищі.

***Предметом дослідження*** є етичні аспекти, які впливають на прийняття рішень та ведення управлінських процесів в галузі кібербезпеки.

***Методи дослідження***. Для вирішення завдань у роботі використовуються методи системного аналізу, теорії інформаційної безпеки та теоретичного узагальнення, аналіз і синтез, аналогія, моделювання.

***Короткий зміст роботи.*** У роботі проведено аналіз етичних аспектів інформаційної безпеки, визначено основні поняття, принципи, закони та стандарти. Розглянуто актуальний стан, фактори та виклики для ефективного управління у випадках складних етичних ситуацій. В заключному розділі висвітлені тенденції, проблеми та надані рекомендації для покращення управління кібербезпекою при виявленні складних етичних ситуацій.

***Галузь застосування.*** Результати дослідження можуть бути використані в галузі управління кібербезпекою, а також у дослідженнях, пов'язаних із сучасними тенденціями етики та безпеки в інформаційному середовищі.

**КЛЮЧОВІ СЛОВА :** КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЕТИЧНІ ДИЛЕМИ, СТРАТЕГІЇ ПРИЙНЯТТЯ РІШЕНЬ, ІНФОРМАЦІЙНА ВІЙНА.

## ABSTRACT

The text part of the qualification work for obtaining a master's degree: 74 pages, 6 figures, 1 tables, 64 sources.

The purpose of the work is research in the study and analysis of methods of solving complex ethical situations in cyber security management.

***Object of research*** is cyber security management processes in the modern information environment.

***Subjec***t ***of research*** is ethical aspects that influence decision-making and management processes in the field of cyber security.

***Research methods.*** Methods of system analysis, theory of information security and theoretical generalization, analysis and synthesis, analogy, modeling are used to solve tasks..

***Brief content of research***. As a result, the work analyzes the ethical aspects of information security, defines the main concepts, principles, laws and standards. The current state, factors and challenges for effective management in cases of complex ethical situations are considered. The final section highlights trends, issues, and provides recommendations for improving cybersecurity management when challenging ethical situations are identified.

***Field of research***. The results of the study can be used in the field of cyber security management, as well as in research related to modern trends in ethics and security in the information environment.



**KEYWORDS:** CYBERSECURITY, INFORMATION SECURITY MANAGEMENT, ETHICAL DILEMMA, DECISION-MAKING STRATEGIES, INFORMATION WARFARE.

ЗМІСТ

# ВСТУП

Кібербезпека, як невід'ємна складова сучасного інформаційного суспільства, ставить перед сучасними фахівцями та управлінцями низку складних завдань, зокрема в сфері управління. Зі зростанням комплексності кіберзагроз та швидким розвитком технологій, виникають нові етичні дилеми, які потребують ретельного вивчення та адекватних методів вирішення. Крім технічних аспектів, виникає необхідність розглядати і вирішувати етичні питання, пов'язані з кібербезпекою.

*Актуальність теми* полягає в тому, що, незважаючи на величезні досягнення в області кібербезпеки, етичні аспекти не завжди знаходять належне врахування у стратегіях та рішеннях. Це може призвести до серйозних наслідків для індивідів, організацій та суспільства в цілому.

*Мета роботи* полягає у вивченні та аналізі методів вирішення складних етичних ситуацій в управлінні кібербезпекою. Дослідження спрямоване на визначення основних етичних викликів у галузі кібербезпеки, розгляд та аналіз їхнього впливу на прийняття стратегічних рішень, а також розробку ефективних методів вирішення етичних конфліктів. Для досягнення поставленої мети, дослідження буде зосереджено на таких ключових аспектах, як визначення основних етичних понять у кібербезпеці, аналіз впливу культурних, правових і соціальних чинників, а також розробка та апробація методів вирішення конкретних етичних ситуацій.

*Об'єкт* дослідження – процеси управління кібербезпекою в сучасному інформаційному середовищі.

*Предмет* дослідження – етичні аспекти, які впливають на прийняття рішень та ведення управлінських процесів в галузі кібербезпеки.

*Наукова новизна результатів.* Результати дослідження можуть бути використні для нового підходу до аналізу етичних вимірів управління кібербезпекою та розробки практичних методів вирішення етичних ситуацій у цій галузі. Вперше вивчається етичний вплив на управління кібербезпекою в

українському контексті. Викладення результатів цього дослідження сприятиме підвищенню рівня етичності та відповідальності в управлінні кібербезпекою, забезпечуючи більш ефективний та безпечний цифровий простір для сучасного суспільства.

*Галузь застосування*. Результати дослідження можуть бути використані в галузі управління кібербезпекою, а також у дослідженнях, пов'язаних із сучасними тенденціями етики та безпеки в інформаційному середовищі.

# РОЗДІЛ 1

# ЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

## 1.1. Визначення основних етичних понять

Сучасна галузь кібербезпеки висуває нові вимоги до розуміння та врахування етичних аспектів. У цьому підрозділі буде проведений аналіз та визначення ключових етичних понять та термінів, які використовуються в управлінні кібербезпекою. Зосередимося на розумінні та визначенні понять, таких як конфіденційність, цілісність, доступність, етика хакера, відповідальна вразливість та інші.

Конфіденційність є однією з найважливіших складових етики управління кібербезпекою. Вона визначає рівень захисту конфіденційної інформації, тобто даних, які мають обмежений доступ та не повинні ставати доступними неповноваженим особам чи сторонам від несанкціонованого доступу та розголошення. Це питання стосується захисту особистих даних, комерційних відомостей, технічних розробок та інших конфіденційних матеріалів. Етичні аспекти конфіденційності включають в себе зобов'язання забезпечення захисту конфіденційної інформації від несанкціонованого доступу, використання чи розголошення. Управління конфіденційністю передбачає впровадження ефективних заходів безпеки, політик та процедур, які гарантують надійний захист чутливої інформації. Крім того, це може включати освіту та навчання персоналу щодо відповідального та етичного використання конфіденційної інформації, враховуючи сучасні методи шифрування, аутентифікації та контролю доступу. В сучасному інформаційному середовищі конфіденційність має важливе та широке практичне застосування, особливо в умовах швидкого розвитку цифрових технологій та збільшення обсягів обміну інформацією.

Цілісність визначає недоторканність та невідмінність інформації. У контексті управління кібербезпекою, це означає захист інформації від неправомірної

модифікації чи внесення змін. З етичної точки зору цілісність вимагає від організацій та фахівців у кібербезпеці дотримуватися високих стандартів управління безпекою, включаючи заходи з перевірки цілісності даних, систем та інфраструктури. Етичні аспекти цілісності також охоплюють використання та розвиток технічних засобів для виявлення та запобігання вторгненням або змінами, а також навчання персоналу про актуальні загрози цілісності та етичні методи їх вирішення.

Доступність інформації визначається як забезпечення швидкого та надійного доступу до неї для авторизованих користувачів в рамках встановлених правил та політик безпеки. З етичного погляду, управління доступністю передбачає розробку та впровадження механізмів, що гарантують доступ до систем та даних для користувачів, забезпечуючи при цьому безпеку та виконання правил конфіденційності та цілісності. Етичні аспекти доступності також включають в себе обов'язок уникати несправедливого чи дискримінаційного обмеження доступу, зокрема, врахування потреб користувачів з різними фізичними та іншими обмеженнями, а також забезпечення стійкості систем до намагань заважати їхній роботі.

Етика хакера визначає моральні принципи та стандарти поведінки експертів у галузі кібербезпеки. Етика хакера може включати в себе такі принципи:

- легальність: етичні хакери використовують свої знання та навички в рамках закону, зазвичай з отриманням відповідного дозволу від власників системи або мережі.

- добросовісність: етичний хакер діє добросовісно та чесно, повідомляючи про виявлені вразливості та надаючи рекомендації щодо їх виправлення.

- конфіденційність: етичний хакер поважає конфіденційність інформації, до якої він має доступ у процесі виконання своїх обов'язків.

- справедливість: етичний хакер уникає будь-яких дій, які можуть завдати неправомірного збитку або порушити права користувачів системи.

Ці принципи визначають етичний фундамент для хакерів, які використовують свої навички для покращення безпеки інформаційних технологій.

Відповідальна вразливість передбачає добровільне повідомлення про вразливості в програмному забезпеченні чи системах безпеки. Етичні аспекти відповідальної вразливості включають в себе:

- повага до власності: особа, яка виявила вразливість, поважає власні права власника системи чи розробника програмного забезпечення і не використовує виявлену вразливість для неправомірного доступу чи збитку.

- конфіденційність: повідомлення про вразливість та всі відомості про неї є конфіденційними до того часу, поки не буде розроблено та поширено виправлення для цієї вразливості.

- повага до строків: особа, яка виявила вразливість, дотримується узгоджених строків для повідомлення та публікації інформації про вразливість.

- співпраця з власниками: повідомлюючи про вразливість, відкриваюча особа співпрацює з власниками системи чи розробниками, надаючи достатню інформацію для розробки та впровадження виправлень.

- інформування громадськості: Якщо власники системи чи розробники не вживають заходів для усунення вразливості протягом визначеного строку, особа, яка виявила вразливість, може опублікувати інформацію про неї, щоб попередити громадськість.

Відповідальна вразливість є важливим етичним аспектом управління кібербезпекою, який сприяє покращенню безпеки інформаційних систем та дотриманню принципів етики в IT-сфері.

Етика обробки персональних даних у кібербезпеці включає в себе принципи та стандарти, які повинні дотримуватися при зборі, обробці, зберіганні та використанні особистої інформації. Основні аспекти етики обробки персональних даних включають:

- законність, справедливість і прозорість: обробка персональних даних повинна здійснюватися на законних підставах, справедливо і прозоро для осіб, чиї дані обробляються.

- обмеження цілей: збір та обробка персональних даних повинні здійснюватися лише для визначених, законних і конкретних цілей, які були попередньо визначені.

- мінімізація даних: обробка даних повинна обмежуватися лише тими персональними даними, які є необхідними для досягнення визначених цілей.

- точність: забезпечення точності та актуальності персональних даних. Надання можливості оновлення або виправлення невірних даних.

- обмеження терміну зберігання: зберігання персональних даних лише протягом того періоду, який є необхідним для досягнення цілей обробки.

- цілісність та конфіденційність: захист персональних даних від несанкціонованого доступу та використання, а також гарантування їхньої цілісності.

Всі ці аспекти спрямовані на забезпечення справедливої, етичної та відповідальної обробки персональних даних, з урахуванням прав та інтересів осіб, чиї дані обробляються.

Етичні аспекти глобальної кібербезпеки охоплюють принципи та норми поведінки в цифровому середовищі на міжнародному рівні. Оскільки кібербезпека та інтернет перетинають кордони, етичні питання пов'язані з кібербезпекою стають глобальними і потребують уважного вивчення та регулювання. Декілька ключових аспектів етики глобальної кібербезпеки включають:

- співпраця та міжнародне партнерство: розвиток етичних стандартів для співпраці між країнами, організаціями та приватними суб'єктами для забезпечення безпеки в кіберпросторі.

- захист прав людини в кіберпросторі: визначення та захист основних прав та свобод людини в інтернеті, уникання порушень приватності та цензури.

- боротьба з кіберзлочинністю: розвиток етичних підходів до протидії кіберзлочинності, з обов'язковим дотриманням прав людини та прозорістю в діяльності правоохоронних органів.

- справедливість та включеність: забезпечення справедливого доступу до технологій та інформації, а також врахування інтересів всіх сторін в розвитку кібербезпеки.

- визначення кібервійни та етика військових дій: встановлення етичних норм та правил для кібервійни, визначення етики військових операцій у кіберпросторі.

- забезпечення стабільності та недоторканості інфраструктури: розробка етичних стандартів для захисту критичних інфраструктур та забезпечення стабільності кіберпростору.

Ці аспекти визначають важливі принципи, які повинні гідно враховуватися в управлінні кібербезпекою на глобальному рівні, сприяючи ефективній та етичній взаємодії у цій сфері.

Етичне використання великих даних у кібербезпеці передбачає дотримання принципів та норм, спрямованих на забезпечення прозорості, конфіденційності, справедливості та відповідальності під час збору, обробки та використання великих обсягів інформації в кіберпросторі. Декілька ключових аспектів етичного використання великих даних у кібербезпеці включають:

- прозорість та повага до конфіденційності: забезпечення ясності та відкритості щодо того, як збираються, обробляються та використовуються великі дані в контексті кібербезпеки. Врахування принципів конфіденційності та поваги до особистої інформації.

- справедливість та уникнення дискримінації: забезпечення справедливого та непередбачуваного використання великих даних, уникнення створення або посилення нерівності та дискримінації в кібербезпеці.

- відповідальне використання аналітики: дотримання етичних норм та відповідальне використання аналітичних інструментів для уникнення спотворення результатів аналізу та забезпечення точності та об'єктивності.

- захист прав людини: збереження та захист основних прав та свобод людини в контексті великих даних у кіберпросторі, включаючи право на приватність та безпеку.

- використання даних з урахуванням контексту: етичне використання великих даних передбачає урахування контексту, у якому здійснюється аналіз та використання інформації, з метою уникнення неправильного тлумачення результатів.

Ці аспекти визначають основні принципи етичного взаємодії з великими даними у кібербезпеці та сприяють створенню більш безпечного та справедливого кіберпростору.

Етичні аспекти використання кіберзброї та кібервійськ в управлінні кібербезпекою охоплюють ряд проблем та викликів, які повинні бути враховані для забезпечення відповідального та етичного застосування кіберзасобів. Деякі ключові аспекти цієї теми включають:

- легітимність та міжнародний правопорядок: застосування кіберзброї повинно дотримуватися принципів міжнародного права та легітимних норм, уникати порушення суверенітету країн та інших міжнародних правових стандартів.

- відповідальність та атрибуція: етичний вимір охоплює прозорість та визначення відповідальних за кібератаки, а також можливість атрибуції дій до конкретних суб'єктів.

- захист цивільних об'єктів: важливо дотримуватися принципів захисту цивільних об'єктів та уникати нецільового враження на мирних громадян та інфраструктуру.

- мораторіум на використання кіберзброї: розгляд можливості введення міжнародного мораторію на використання кіберзброї з метою зменшення загрози кібервійни та заохочення мирного вирішення конфліктів.

- співпраця та міжнародні стандарти: розвиток співпраці між країнами для створення міжнародних стандартів щодо етичного використання кіберзасобів та обміну інформацією для запобігання кіберзагроз.

- етика кібервійськ: розробка етичних кодексів для кібервійськ з метою обмеження використання агресивних кіберзасобів та визначення обсягів та умов їхнього застосування.

- захист прав людини: збереження та захист основних прав та свобод людини в контексті кібервійни, включаючи право на приватність та безпеку.

Ці аспекти визначають основні вимоги та норми, які мають дотримуватися при застосуванні кіберзасобів в управлінні кібербезпекою для забезпечення етичності та відповідальності в цьому сфері.

Етичні аспекти кібершпіонажу та кібершантажу. Кібершпіонаж та кібершантаж породжують серйозні питання етики та безпеки в інформаційному просторі, і включають низку важливих питань, пов'язаних із сучасними технологіями та практиками у цих областях. Ключові аспекти:

- прозорість та легітимність: важливо, щоб країни чи організації, які здійснюють кібершпіонаж, робили це з прозорістю та в межах легітимних цілей, таких як забезпечення національної безпеки. Використання кіберзасобів для нелегітимних цілей може порушувати права та свободи осіб із захистом від недоцільних втручань.

- співробітництво та міжнародний діалог: етичний аспект кібершпіонажу включає необхідність співробітництва між країнами та суб'єктами міжнародного співтовариства. Розробка міжнародних стандартів та діалогу може допомогти обмежити негативні наслідки та запобігти міжнародним конфліктам.

- права людини: проведення кібершпіонажу повинно дотримуватися принципів захисту прав людини, зокрема права на приватність. Спостереження та збір інформації повинні враховувати необхідність збереження особистої свободи та непорушності.

- легітимність кібершантажу: кібершантаж як такий є неприпустимим із точки зору етики. Використання кіберзасобів для шантажу чи вимагань є порушенням етичних норм. Організації повинні уникати використання кіберзасобів для вимагань, що можуть завдати шкоди іншим суб'єктам.

- кібербезпека та захист інфраструктури: із врахуванням зростання загроз у кіберпросторі, етичний аспект кібершпіонажу включає необхідність вдосконалення заходів з кібербезпеки та захисту критично важливих систем.

- прозорість та відповідальність: суб'єкти, які використовують кіберзасоби для спостереження чи шпіонажу, повинні мати прозорі цілі та бути відповідальними за свої дії, враховуючи можливі наслідки для інших.

Ці аспекти визначають ключові етичні принципи, які повинні бути враховані при здійсненні кібершпіонажу та управлінні кібербезпекою. Збалансоване та етичне використання кіберзасобів дозволяє підтримувати безпеку та захищати інтереси, уникати неправомірного втручання та дотримуватися міжнародних норм та прав людини.

Етичне використання технологій розпізнавання обличчя в кібербезпеці передбачає врахування ряду принципів та обмежень для забезпечення безпеки та захисту особистої приватності. Декілька аспектів, які варто враховувати:

- законність та дотримання прав людини: використання технологій розпізнавання обличчя повинно відповідати законам та міжнародним стандартам

прав людини. Дотримання прозорих та справедливих правил гарантує відсутність дискримінації та недопущення неправомірного використання.

- оповіщення та згода: користувачі повинні бути чітко проінформовані про використання технологій розпізнавання обличчя, а також мати можливість вираження своєї згоди. Це підкреслює прозорість та повагу до особистої приватності.

- захист даних: забезпечення високого рівня захисту даних є ключовим елементом етичного використання технологій розпізнавання обличчя. Запобігання несанкціонованому доступу та збереження конфіденційності є важливими принципами.

- недопущення зловживань: технології розпізнавання обличчя не повинні використовуватися для зловживань чи порушень основних прав людини. Обмеження використання в специфічних контекстах допомагає уникнути потенційних негативних наслідків.

- тестування та пошук помилок: розробники повинні систематично тестувати та вдосконалювати алгоритми розпізнавання обличчя, враховуючи етичні стандарти. Виявлення та виправлення помилок сприяє покращенню точності та надійності систем.

Загальною метою є забезпечення етичного використання технологій розпізнавання обличчя, зберігаючи баланс між безпекою та захистом особистої приватності.

## 1.2. Аналіз та класифікація етичних ситуацій та дилем в управлінні кібербезпекою.

У сучасному цифровому світі, де кіберзагрози стають все більш складними та виразними, управління кібербезпекою потребує глибокого розуміння етичних аспектів. Аналіз та класифікація етичних ситуацій та дилем в управлінні кібербезпекою стає ключовим завданням для забезпечення високого стандарту

етичності та відповідального ведення діяльності в цій галузі. У рамках управління кібербезпекою існують різноманітні етичні ситуації, які можна класифікувати за різними критеріями. Розглянемо їх:

1. Конфлікт між безпекою та приватністю представляє собою складну проблему, де необхідно балансувати між забезпеченням ефективної безпеки і захистом особистої приватності користувачів. Підвищення рівня безпеки в інформаційних системах часто вимагає збільшення обсягу зібраної та оброблюваної інформації про користувачів. Це може породити конфлікт між потребами забезпечення безпеки та збереженням особистої приватності індивідів. Розглянемо основні аспекти цієї ситуації:

- контроль та обмеження: збільшення обсягу зібраної інформації може вести до можливості її недопустимого використання чи несанкціонованого доступу.

- захист особистої приватності: підвищення безпеки може потребувати збереження великої кількості особистої інформації, що порушує право на приватність.

- пошкодження репутації: несанкціонований доступ чи витік інформації може завдати шкоди репутації користувачів та підірвати довіру до систем безпеки.

- прозорість та інформованість: збільшення обсягу зібраної інформації може бути неприйнятним для користувачів, які можуть не бути повністю інформованими про цей процес.

Ця етична ситуація вимагає ретельного балансу між потребами забезпечення безпеки та захистом приватності користувачів, враховуючи права та очікування двох сторін.

2. Підзвітність та прозорість управління. У контексті управління може виникнути ситуація, коли компанії чи організації володіють значущою кількістю конфіденційної інформації та владною позицією у кіберпросторі. Однак, виникає питання про те, наскільки вони підзвітні та прозорі у своїй діяльності. Розглянемо основні деталі цієї ситуації:

- публічна довіра: багато користувачів та зацікавлених сторін мають обґрунтовану побоюваність щодо недостатньої прозорості компаній у сфері інформаційної безпеки.

- конфіденційність інформації: забезпечення підзвітності повинно враховувати також конфіденційність низки даних.

- відповідальність перед зацікавленими сторонами: недостатня підзвітність може викликати невпевненість серед клієнтів, партнерів та інших зацікавлених сторін.

- надмірна захопленість: компанії можуть надто активно збирати та аналізувати дані для вдосконалення своєї кібербезпеки, що породжує питання про обґрунтованість таких заходів.

- ефективність заходів управління: зацікавлені сторони мають право знати, наскільки ефективним є управління кібербезпекою в організації.

Ця етична ситуація визначає необхідність поєднання заходів безпеки з підзвітністю та прозорістю, щоб забезпечити ефективність управління та збереження довіри соціуму.

3. Експлуатація вразливостей для атак. Хакери можуть використовувати вразливості в програмному забезпеченні чи системах з метою несанкціонованого доступу, крадіжки конфіденційної інформації та завдання шкоди. Зловмисники можуть використовувати знання про вразливості, щоб здійснювати цілеспрямовані атаки на системи та мережі. А експлуатація вразливостей може призводити до витоку конфіденційної інформації, що порушує приватність користувачів та може мати серйозні наслідки для компаній. Розробка ефективних механізмів виявлення та усунення вразливостей є ключовою для запобігання таким атакам.

4. Співпраця із зловмисниками. Ситуація, коли фахівці з кібербезпеки чи організації стикаються з можливістю співпраці чи взаємодії із зловмисниками, може виникнути у випадках потреби в розслідуванні або виявленні загроз для

кібербезпеки. Та може викликати багато питань і дилем. Розглянемо основні обставини цієї ситуації:

- взаємодія з експертами: деякі сценарії передбачають співпрацю з технічними експертами, які можуть мати злочинний статус, для отримання або обміну інформацією про нові загрози та вразливості. Це підводить під сумнів етичність співпраці з тими, хто може використовувати отримані дані для злочинних цілей.

- співпраця під час інцидентів: в інцидентному реагуванні може виникнути необхідність співпраці з експертами, які мають знання про атаки або мають інформацію про зловмисників. Проте, це може викликати питання етики, оскільки це може означати обмін інформацією з особами, які порушують закон. Співпраця із зловмисниками повинна відбуватися в межах закону та за належного дозволу компетентних органів. При співпраці із зловмисниками необхідно враховувати конфіденційність інформації. Розробка стандартів для визначення легітимних обставин для такої співпраці є важливою.

- участь у закритих спільнотах: деякі експерти з кібербезпеки можуть вступати в закриті спільноти або форуми, де обмінюються інформацією про нові загрози. Проте, участь у таких спільнотах може підтвердити етичні питання, оскільки це може створювати середовище для обговорення та розвитку нових методів атак.

### 1.3. Роль етики в управлінні кібербезпекою

В сучасному цифровому світі, де технології невпинно розвиваються, етика в управлінні кібербезпекою виявляється визначальною для забезпечення стійкої та ефективної захисту інформації. Кількість та складність кіберзагроз росте та вимагає уважного розгляду етичних аспектів усіх аспектів управління безпекою інформації. Вивчення етичних аспектів управління інформаційною безпекою відкриває можливість розуміти не лише технічні виклики, але й вплив рішень на

суспільство, конфіденційність, приватність та права людини. Це важлива частина будівництва сталого та етичного цифрового середовища.

Етика в сфері кібербезпеки відіграє ключову роль у формуванні та прийнятті стратегічних рішень, орієнтованих на забезпечення безпеки та захист цифрового простору. Цей вплив проявляється в різноманітних аспектах, визначаючи характер та напрямок управлінських вирішень в контексті кібернетичних загроз. А саме:

1. Визначення цілей та пріоритетів. Етика визначає стратегічні цілі в області кібербезпеки, забезпечуючи баланс між технічними можливостями та важливими етичними принципами. Під час прийняття стратегічних рішень важливо враховувати етичні аспекти, такі як приватність, конфіденційність та свобода.

- вплив на основні цілі безпеки: етика визначає основні цілі управління кібербезпекою, враховуючи важливі етичні принципи. Наприклад, збалансованість між захистом конфіденційності та доступністю інформації стає етичним викликом, який формує стратегічні цілі.

- етичне визначення пріоритетів: етика в управлінні кібербезпекою визначає порядок пріоритетів у забезпеченні безпеки. Наприклад, пріоритет захисту особистої інформації користувачів може визначати стратегії з обмеженням обсягу збирання та використання даних.

- урахування соціокультурних аспектів: етичне визначення цілей управління кібербезпекою пов'язане з урахуванням різноманітних соціокультурних контекстів. Врахування цих аспектів дозволяє визначати цілі, які відповідають потребам і цінностям різних груп користувачів.

- збалансованість технічних та етичних аспектів: етичний підхід визначає необхідність збалансованості між технічними можливостями та етичними вимогами. Забезпечення безпеки повинно враховувати не лише технічні аспекти, але й високі етичні стандарти.

- врахування економічних вимог: етика управління кібербезпекою також визначає врахування економічних аспектів у визначенні цілей. Оптимальне

використання ресурсів та фінансів при забезпеченні безпеки стає об'єктивом етичної стратегії.

Врахування етичних аспектів визначення цілей та пріоритетів в управлінні кібербезпекою сприяє створенню стратегій, які враховують потреби користувачів, соціокультурний контекст та економічні реалії.

2. Забезпечення прозорості. Етичний підхід в управлінні кібербезпекою сприяє створенню прозорих механізмів прийняття рішень. Прозорість сприяє відкритості та відповідальності перед зацікавленими сторонами, збільшуючи рівень довіри до стратегічних рішень.

- відкритість щодо збору та використання інформації: етичний підхід вимагає, щоб організації були прозорими щодо збору та використання інформації. Користувачі повинні мати змогу зрозуміти, як їхні дані використовуються для забезпечення кібербезпеки.

- оголошення етичних принципів та стандартів: прозорість включає оголошення етичних принципів та стандартів, які визначають дії організації в сфері кібербезпеки. Це допомагає створити довіру серед користувачів та інших зацікавлених сторін.

- інформування про потенційні ризики: етична прозорість передбачає інформування користувачів про потенційні ризики, пов'язані з зберіганням та обробкою їхніх даних в контексті кібербезпеки. Це дозволяє користувачам приймати обізнані рішення щодо власної безпеки.

- системи відповідальності та звітності: забезпечення прозорості також включає встановлення систем відповідальності та звітності за етичне використання інформації та засобів кібербезпеки. Це допомагає уникнути недобросовісної поведінки та надає користувачам можливість виражати свої зауваження.

- взаємодія з зацікавленими сторонами: прозорість також означає взаємодію з зацікавленими сторонами, такими як органи регулювання, громадські організації та

інші організації. Відкритий діалог сприяє створенню ефективних етичних підходів управління кібербезпекою.

Забезпечення прозорості в управлінні кібербезпекою допомагає створити довіру користувачів та інших стейкхолдерів, підвищує ефективність заходів з кібербезпеки та відповідає основним етичним принципам.

3. Регулювання використання технологій. Етика в кібербезпеці регулює використання технологій та інструментів, забезпечуючи, що стратегічні рішення відповідають вимогам етичних стандартів. Це включає в себе етичне використання штучного інтелекту, аналітичних інструментів та інших технологій.

- етичне використання штучного інтелекту: забезпечення етичного використання технологій, зокрема штучного інтелекту, передбачає розробку етичних стандартів, які обмежують або регулюють можливість застосування ШІ в контексті кібербезпеки. Це включає в себе визначення меж використання автоматизованих систем при прийнятті стратегічних рішень.

- контроль за розвитком кіберзброї та кібервійськ: етичні аспекти управління кібербезпекою передбачають регулювання розвитку та використання кіберзброї та кібервійськ. Це включає в себе створення міжнародних стандартів та договорів, що обмежують застосування кіберзброї в агресивних цілях та визначають етичні рамки для ведення кібервійниць.

- етичне використання кіберзасобів у кібербезпеці: регулювання використання кіберзасобів передбачає визначення етичних норм щодо їхнього застосування. Це включає в себе обмеження використання кіберзасобів у ворожих цілях та встановлення етичних стандартів для проведення експлойтів та тестування безпеки.

- регулювання використання технологій розпізнавання обличчя: етичні аспекти використання технологій розпізнавання обличчя передбачають контроль та регулювання їхнього застосування. Це включає в себе розробку етичних директив для уникнення порушень приватності та недобросовісного використання таких технологій.

- етичне використання великих даних в кібербезпеці: регулювання використання великих даних передбачає розробку етичних стандартів, що визначають обсяг та межі збору, обробки та зберігання інформації. Етичні норми повинні забезпечити права та приватність користувачів, а також уникнення зловживань зі зібраними даними.

Забезпечення етичного використання технологій у кібербезпеці включає в себе розробку стандартів, що визначають допустимі межі та обмеження для їхнього застосування. Такі заходи регулювання допомагають уникнути етичних порушень та захистити права та свободи користувачів.

4. Захист прав та свобод особи. При прийнятті стратегічних рішень важливо враховувати етичні аспекти, що стосуються захисту прав та свобод особи в цифровому просторі. Етика управління кібербезпекою допомагає визначати межі використання технологій для забезпечення прав та свобод кожного користувача.

- конфіденційність та приватність: визначення етичних принципів захисту конфіденційності та приватності в управлінні кібербезпекою має на меті забезпечення поваги до особистої інформації. Це включає в себе розробку політик та процедур, які гарантують безпечне зберігання та обробку даних, а також забезпечення дотримання прав особи на конфіденційність.

- транспарентність та інформованість: етичне використання кібербезпекових заходів передбачає обов'язок забезпечення транспарентності та інформованості осіб, які підлягають впливу цих заходів. Це включає в себе розробку чітких комунікаційних стратегій та інформаційних кампаній, які пояснюють сутність заходів з кібербезпеки та їхні можливі наслідки для особистої свободи.

- заборона дискримінації та недопущення надмірного контролю: етичні аспекти управління кібербезпекою передбачають заборону будь-якої форми дискримінації та надмірного контролю над особистою інформацією. Це включає в себе визначення чітких норм та стандартів, що обмежують можливість

використання кібербезпекових засобів для недопустимого втручання у приватний та особистий простір особи.

- відповідальне використання великих даних: захист прав та свобод особи включає в себе впровадження відповідального використання великих даних. Це передбачає розробку етичних стандартів, які регулюють обробку та використання великих обсягів інформації, з урахуванням важливості захисту прав та свобод кінцевого користувача.

- захист від недобросовісного використання технологій: етичні аспекти управління кібербезпекою передбачають заходи захисту від можливого недобросовісного використання технологій. Це включає в себе розробку механізмів виявлення та попередження можливих порушень етичних норм та негайне реагування на такі ситуації.

5. Створення етичної корпоративної культури. Етичні принципи визначають корпоративну культуру в галузі кібербезпеки, що впливає на прийняття стратегічних рішень. Створення етичної корпоративної культури сприяє впровадженню етичних стандартів на всіх рівнях управління.

- розробка та впровадження етичних кодексів: практична реалізація етичних принципів включає в себе активну участь у розробці та впровадженні етичних кодексів для фахівців у галузі кібербезпеки. Створення чітких та обов'язкових норм поведінки сприяє викоріненню неправомірних дій та встановленню етичних стандартів у сфері.

- постійне професійне навчання: забезпечення постійного професійного навчання фахівців у галузі кібербезпеки є необхідною умовою для ефективної реалізації етичних принципів. Оновлення знань та навичок у відповідності до швидких змін у технологічному середовищі дозволяє забезпечити високий рівень етичності у вирішенні кібербезпекових завдань.

- етичні аудити та оцінка ризиків: систематичне проведення етичних аудитів та оцінка ризиків дозволяють виявляти та усувати можливі етичні порушення в

управлінні кібербезпекою. Аналіз можливих наслідків дій сприяє зменшенню ризиків та вдосконаленню системи етичного управління.

- співпраця з громадськістю та зацікавленими сторонами: активна участь у взаємодії з громадськістю та зацікавленими сторонами є важливим аспектом практичної реалізації етичних принципів. Відкритість до взаємодії та залучення різних стейкхолдерів сприяє побудові етичного обличчя управління кібербезпекою.

- ефективна реакція на етичні порушення: розробка ефективних механізмів реагування на етичні порушення та їх швидке виправлення є ключовим елементом практичної реалізації етичних принципів. Запровадження механізмів звітності та контролю дозволяє вчасно реагувати на можливі негативні наслідки та забезпечує високий рівень етичності в управлінні кібербезпекою.

В цілому, врахування етичних аспектів в управлінні кібербезпекою сприяє формуванню стратегій, які ефективно забезпечують безпеку інформації, враховуючи соціальні, правові та моральні вимоги сучасного суспільства.

А також забезпечується відповідність цих стратегій суспільним та моральним цінностям, а саме:

1. Суспільна відповідальність:

Адаптація до соціальних вимог: управління кібербезпекою повинно адаптуватися до соціальних вимог та очікувань суспільства. Визнання та врахування цінностей, які важливі для суспільства, дозволяє побудовувати стратегії, що відповідають громадським потребам.

Відповідність цінностям громадян: врахування та визначення загальних цінностей суспільства є ключовим для побудови етичних стратегій управління кібербезпекою.

Принципи справедливості: справедливий розподіл ризиків та відповідальності між різними групами суспільства враховує принципи справедливості та моральної відповідальності. Та стеження за тим, щоб інтереси

всіх зацікавлених сторін були враховані є обов’язковим, адже сприяє зміцненню суспільної відповідальності.

Такий підхід до суспільної відповідальності в управлінні кібербезпекою впливає на побудову стратегій, що враховують реальні потреби та цінності громадян, забезпечуючи високий ступінь етичності та суспільної відповідальності.

2. Етичні кодекси:

Відповідність моральним цінностям: розробка та впровадження етичних кодексів ґрунтується на моральних цінностях, що є прийнятними для суспільства. Ці кодекси враховують загальноприйняті етичні норми та стандарти.

Впровадження етичних норм у практику: етичні кодекси повинні бути інтегровані в практичну діяльність управління кібербезпекою для забезпечення їх ефективності.

Моніторинг та оновлення: впровадження систем моніторингу за дотриманням етичних кодексів дозволяє вчасно виявляти та усувати порушення. Етичні кодекси повинні регулярно оновлюватися, враховуючи зміни в технологічному та етичному середовищі.

Створення етичних комітетів: формування етичних комітетів допомагає вирішувати складні етичні ситуації та надавати рекомендації. В етичних комітетах можуть брати участь експерти з різних галузей для об'єктивного розгляду питань.

3. Забезпечення прозорості:

Громадський контроль: Прозорість у діяльності забезпечує громадський контроль та відкритість перед суспільством. Важливо, щоб усі рішення та дії в управлінні кібербезпекою відповідали загальним суспільним цінностям.

Опублікування стратегій: Забезпечення прозорості включає опублікування ключових стратегій управління кібербезпекою для загального доступу.

Відкритість щодо заходів безпеки: організації повинні надавати відкритий доступ до інформації про заходи безпеки, які вони впроваджують.

Взаємодія зі зацікавленими сторонами: забезпечення прозорості включає активний діалог з громадськістю та іншими зацікавленими сторонами.

Аудит та перевірка: проведення регулярних незалежних аудитів забезпечує об'єктивну перевірку рівня прозорості та відповідність стандартам.

Відкриті звіти: забезпечення прозорості передбачає публікацію звітів про інциденти та їхні наслідки для громадськості. Створення ефективних систем звітності дозволяє підтримувати сталу взаємодію зі зацікавленими сторонами.

Забезпечення прозорості в управлінні кібербезпекою визначається не лише доступністю інформації, але й активною взаємодією з різними стейкхолдерами. Прозорі стратегії та діалог сприяють підвищенню рівня довіри та ефективності управління.

4. Етичні аудити та оцінка ризиків:

Проведення етичних аудитів: етичні аудити спрямовані на оцінку дотримання етичних стандартів та процедур в управлінні кібербезпекою.

Моральні аспекти ризиків: Проведення етичних аудитів та оцінка ризиків враховують моральні аспекти можливих наслідків. Визначення, наскільки дії можуть впливати на суспільство, дозволяє управлінцям уникати негативних етичних наслідків.

Визначення стратегій ризик-менеджменту: на основі аналізу етичних ризиків формується стратегія ризик-менеджменту для зменшення негативних впливів.

Відкритий доступ до результатів: отримані під час аудитів та оцінки ризиків результати публікуються для громадськості та стейкхолдерів.

Залучення незалежних експертів: забезпечення об'єктивності включає залучення незалежних фахівців до оцінки етичних аспектів.

Етичне врахування при управлінні ризиками: прийняття етичних принципів в управлінні ризиками сприяє підтримці високих стандартів ділової етики.

Оцінка ефективності заходів: постійна оцінка етичних аспектів в управлінні ризиками дозволяє забезпечити їхню ефективність та актуальність.

Етичні аудити та оцінка ризиків в управлінні кібербезпекою гарантують, що прийняті стратегії не тільки ефективні та безпечні, але й відповідають високим етичним стандартам.

5. Співпраця з громадськістю:

Інформування громадськості: забезпечення доступу до інформації та проведення освітніх заходів допомагає підвищити етичну свідомість серед громадськості.

Розробка програм залучення: створення програм, що дозволяють громадськості брати участь у прийнятті рішень, пов'язаних з кібербезпекою.

Створення платформ для зворотнього зв'язку: забезпечення платформ для зворотного зв'язку дає громадськості можливість висловлювати свої погляди та враховувати їх.

Публікація звітів та результатів: регулярна публікація звітів та результатів управління кібербезпекою дозволяє громадськості слідкувати за етичними практиками.

Відкритий доступ до політик: забезпечення відкритого доступу до політик управління кібербезпекою для громадськості.

Співпраця з громадськістю в етичному управлінні кібербезпекою забезпечує більше об'єктивності та врахування інтересів різних груп.

6. Реакція на етичні порушення:

Виправлення моральних невідповідностей: Ефективна реакція на етичні порушення передбачає виправлення моральних невідповідностей та покарання винних. Це сприяє відновленню довіри та відповідності загальним цінностям.

Розслідування та аудит етичних справ: здійснення ретельних розслідувань та аудитів щодо етичних порушень.

Відсторонення від посад: відсторонення працівників, винних у серйозних етичних порушеннях, від відповідальних посад.

Вдосконалення етичних політик: регулярне оновлення та вдосконалення етичних політик відповідно до виявлених порушень та найкращих практик.

Розробка планів попередження: розробка та впровадження планів для попередження етичних порушень.

Етична освіта та тренінги: проведення освітніх програм та тренінгів для персоналу щодо етичної поведінки.

Реакція на етичні порушення включає в себе комплекс заходів, спрямованих на виявлення, виправлення та запобігання подібним ситуаціям в майбутньому.

Таким чином, врахування суспільних та моральних цінностей в управлінні кібербезпекою гарантує відповідність стратегій вимогам громадян та високий рівень етичності.

Наукові дослідження ролі етики в формуванні та реалізації політик управління кібербезпекою є важливим аспектом, оскільки ця тема стає все більш актуальною в умовах постійного зростання кількості кіберзагроз та залежності сучасного суспільства від інформаційних технологій. На сьогоднішній день існують дослідження, що аналізують вплив етичних аспектів на процеси управління кібербезпекою, враховуючи потреби як організацій, так і соціуму. Серед таких і дослідження «Offensive Cyberspace Operations and Zero-days: Anticipatory Ethics and Policy Implications for Vulnerability Disclosure» (Наступальні операції в кіберпросторі та Zero-days: передбачувана етика та політичні наслідки для розкриття вразливостей) від GAZMEND HUSKAJ - докторант з операцій у кіберпросторі Шведського університету оборони, та RICHARD L. WILSON - професором філософії та комп’ютерних та інформаційних наук в Університеті Тоусона, США.(див. рис.1.1)

Рис.1.1 Автори дослідження про роль етики у розкритті вразливостей Zero-day.

У цій статті розглядається роль етики в контексті використання "zero-day" вразливостей у наступальних кібероперація̈х. Основні ідеї щодо ролі етики:

- автори стверджують, що етичні міркування часто ігноруються при прийнятті рішень про використання вразливостей в кібероперація̈х.
- вони пропонують підхід "антиципативної етики", який передбачає аналіз етичних наслідків ще до початку операції.
- етичні принципи, такі як уникнення шкоди, повага до автономії, справедливість, повинні враховуватися при оцінці використання вразливостей.
- необхідний баланс між національною безпекою та етичними міркуваннями щодо наслідків для громадськості.
- важливо, щоб етичні норми визначалися на рівні політики та регулювання в галузі кібербезпеки.

Отже, автори наголошують, що етичні принципи повинні бути фундаментальною частиною прийняття рішень про кібероперації та розкриття вразливостей.

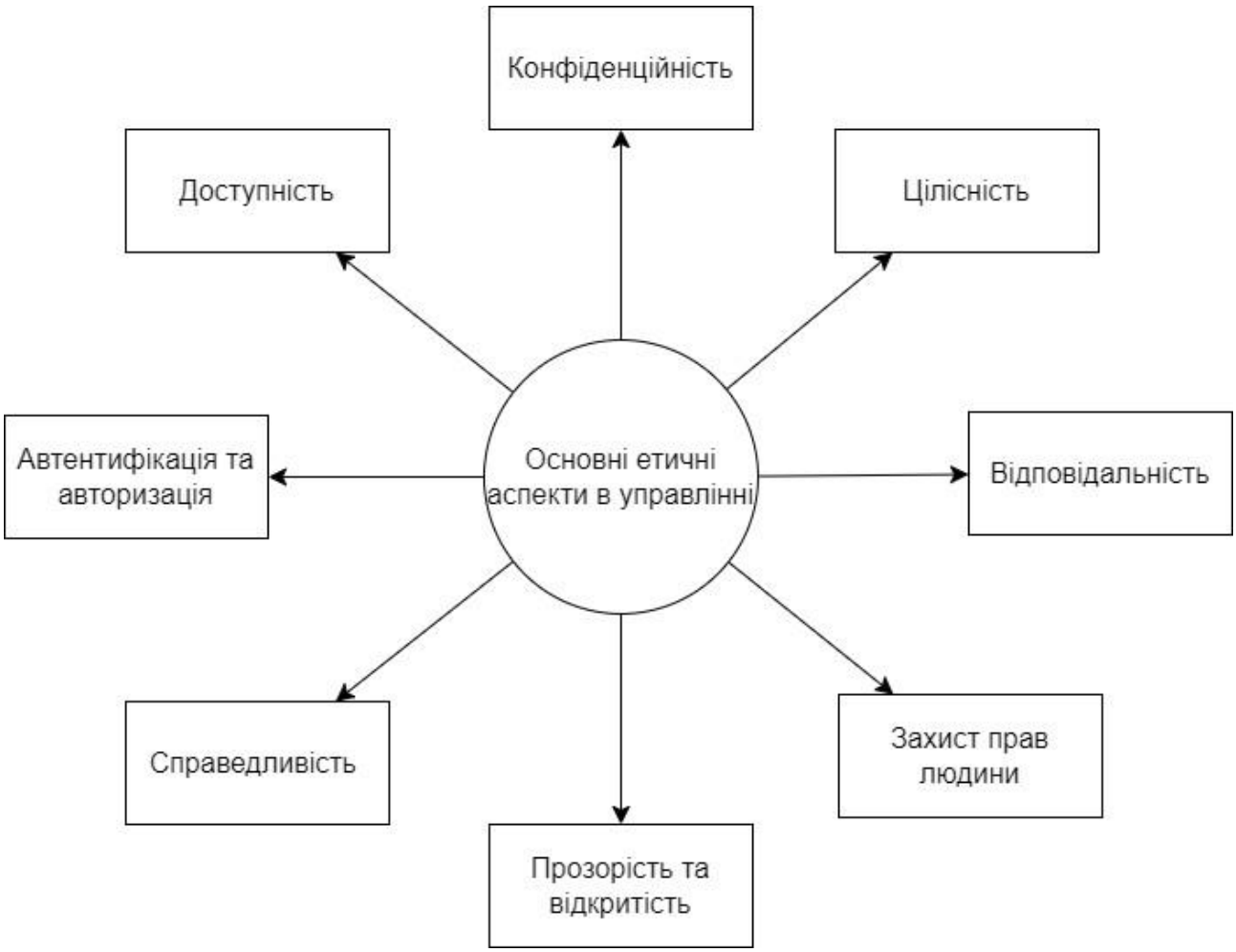


Рис.1.2. Основні етичні аспекти, пов’язані з управлінням кібербезпекою

У цьому розділі ретельно розглянуто основні етичні аспекти, пов'язані з управлінням кібербезпекою (Рис.1.2). Здійснивши аналіз та класифікацію етичних ситуацій і дилем, з’ясовано важливість визначення основних етичних понять, що становлять фундамент для подальшого розуміння та вирішення проблем у цій галузі.

Дослідження показало, що етичні визначення і вирішення ситуацій у кібербезпеці вимагають комплексного підходу та урахування різноманітних факторів. Розгляд етичних аспектів став важливим етапом для формування стратегій та політик управління кібербезпекою, які повинні враховувати не лише технічні аспекти, а й високий ступінь моральної та суспільної відповідальності.

# РОЗДІЛ 2

# ВПЛИВ КУЛЬТУРНИХ, ПРАВОВИХ І СОЦІАЛЬНИХ ЧИННИКІВ НА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

## 2.1. Дослідження впливу культурних, правових і соціальних факторів на етичні ситуації в кібербезпеці

У сучасному світі, де інформаційні технології відіграють ключову роль у всіх сферах життя, управління кібербезпекою стає надзвичайно важливим аспектом. Забезпечення конфіденційності, цілісності та доступності інформації в кіберпросторі вимагає не лише технічних рішень, але й уваги до етичних аспектів цього процесу.

Вплив культурних, правових і соціальних чинників на управління кібербезпекою визначається широким спектром факторів, включаючи різноманітність поглядів різних груп, встановлених законодавством норми та соціальні тенденції. Дослідження цих аспектів необхідно для забезпечення не тільки технічної безпеки, але і розробки ефективних та етичних стратегій управління кібербезпекою. Зрозуміння цих аспектів є ключовим для створення ефективних та суспільно відповідальних підходів до управління кібербезпекою.

2.1.1 Культурні аспекти визначають основні цінності, норми та переконання суспільства, включаючи підходи до етики в управлінні кібербезпекою. Порозуміння культурних відмінностей стає важливим для розробки ефективних стратегій управління кібербезпекою, які враховують місцеві особливості та відповідають вимогам етичних стандартів.

*Культурні особливості та їх вплив на розуміння безпеки в кіберпросторі*. Культурні особливості мають значний вплив на те, як суспільство розуміє та взаємодіє з поняттям безпеки в кіберпросторі. Різні культури вирізняються своїми

цінностями, нормами та переконаннями, що формують сприйняття загроз, а також визначають ступінь особистої відповідальності за кібербезпеку.

Індивідуалізм та колективізм. Країни, які виявляють велику нахиленину до індивідуалізму, надають перевагу захисту особистих даних та приватності в інтернеті. Вони можуть реагувати більш чутливо на випадки порушення конфіденційності та недостатнього захисту особистих інформаційних ресурсів. З іншого боку, колективістичні культури можуть більше цінувати групову безпеку, де важливіше колективне благополуччя, іноді за рахунок індивідуальної приватності.

Ставлення до ризиків. Сприйняття ризиків визначається не лише технічними аспектами, але й культурним фоном. Країни з високим ступенем невизначеності можуть реагувати обережно на нові технології та бути більш консервативними у впровадженні інновацій в області кібербезпеки. На відміну від цього, культури з низьким рівнем невизначеності можуть більше готуватися до ризиків і швидше приймати нові підходи в кіберпросторі.

Довіра до авторитетів. Рівень довіри до авторитетів із питань кібербезпеки також залежить від культурних особливостей. В деяких країнах люди можуть більше сподіватися, що державні структури візьмуть на себе відповідальність за їхню кібербезпеку, тоді як в інших культурах індивіди можуть вважати за краще самостійно забезпечувати свою безпеку.

Культурні аспекти етики хакера. Погляди на етичність хакінгу можуть варіюватися в залежності від культурного контексту. У деяких культурах хакерство може розглядатися як діяльність, спрямована на виявлення вразливостей для подальшого покращення безпеки, тоді як в інших це може вважатися кримінальним порушенням.

*Локальні практики та визначення відповідальності в кіберпросторі*. Визначення відповідальності та формування локальних практик у кіберпросторі має тісний зв'язок з культурними, правовими та соціальними впливами. Локальні

практики визначають стандарти поведінки, етичні норми та правила, які спрямовані на забезпечення безпеки в цифровому середовищі.

Розподіл відповідальності між суб'єктами кіберпростору. У різних культурах можуть існувати різні уявлення про те, як розподіляється відповідальність за кібербезпеку між різними суб'єктами. В індивідіалістичних суспільствах може бути високий рівень індивідуальної відповідальності за захист власної інформації, тоді як в колективістичних суспільствах більше акцентується на груповій відповідальності та взаємній підтримці.

Локальні стандарти безпеки та їх вплив на етичні ситуації. Різні культури можуть мати власні стандарти та норми щодо безпеки в кіберпросторі. Деякі суспільства можуть бути більш вимогливими до забезпечення конфіденційності, тоді як інші можуть приділяти більше уваги доступності та відкритості. Локальні стандарти можуть також визначати, як вирішуються етичні ситуації, пов'язані з порушенням цих норм.

Роль локальних спільнот та груп відповідальності. У багатьох культурах спільноти та групи відіграють ключову роль у визначенні відповідальності в кіберпросторі. Це може бути пов'язано із спільними практиками безпеки, обміном інформацією про загрози, а також спільною відповідальністю за захист колективної безпеки.

Адаптація до місцевих правових структур. Культурні відмінності також відображаються у сприйнятті та дотриманні місцевих правових норм. Деякі країни можуть бути більш схильними до виконання правових норм у сфері кібербезпеки, тоді як в інших культурах може існувати більша тенденція до обхідництва або невизнання певних аспектів законодавства.

Враховуючи ці аспекти, дослідження впливу локальних практик та визначення відповідальності в кіберпросторі є ключовим для розуміння етичних ситуацій, які можуть виникати в цифровому середовищі різних культур.

*Міжкультурні виклики в управлінні кібербезпекою.* Міжкультурні виклики в управлінні кібербезпекою становлять суттєвий аспект, оскільки кіберпростір не обмежується національними кордонами, і взаємодія різних культур в цьому середовищі може викликати численні етичні дилеми. Розглядаючи цей аспект, можна виділити декілька ключових напрямків.

Культурні розходження у визначенні загроз та підході до їх розв'язання. Різні культури можуть сприймати та оцінювати кіберзагрози по-різному. Наприклад, в індивідіалістичних культурах може бути важливе захищати особисті дані, тоді як в колективістичних культурах акцент може робитися на захист групової безпеки. Міжкультурні розходження можуть впливати на визначення пріоритетів у кібербезпеці та визначення етичних стратегій.

Виклики управління міжнародними кіберподіями. З розвитком глобальних технологій виникають міжнародні кіберподії, що створюють складність для етичного управління кібербезпекою. Суттєві культурні відмінності у підходах до кібербезпеки можуть ускладнювати співпрацю та реагування на події, що стосуються кібербезпеки між різними країнами.

Культурні різниці у відношенні до технологій та інновацій. Різні культури мають відмінне ставлення до технологій та інновацій, що може впливати на їхню готовність приймати нові рішення у сфері кібербезпеки. Наприклад, країни з високорозвиненими технологічними культурами можуть бути більш відкритими до впровадження нових кіберзаходів порівняно з традиційними суспільствами.

Важливість міжкультурного навчання. Міжкультурне навчання та розвиток навичок взаємодії у кіберпросторі стає ключовим для вирішення етичних викликів. Розуміння культурних особливостей та вивчення підходів різних національних груп може допомогти уникнути конфліктів та сприяти ефективному управлінню кібербезпекою.

Міжкультурні виклики в управлінні кібербезпекою є складним завданням, оскільки вони вимагають розуміння різних систем цінностей та культурних

особливостей. Ефективне врахування цих аспектів може покращити глобальне управління кібербезпекою та сприяти етичному розвитку цифрового суспільства.

2.1.2. Правовий вплив на етичні ситуації в кібербезпеці.

Правовий контекст визначає рамки та стандарти, які регулюють поведінку в кіберпросторі, впливаючи на етичні ситуації та вирішення етичних питань. Далі деякі аспекти правового впливу на етичні ситуації в області кібербезпеки.

*Міжнародні нормативні акти та угоди*. Міжнародні нормативні акти та угоди в сфері кібербезпеки визначають загальні принципи, стандарти та взаємні зобов'язання держав у цифровому просторі. Ці документи спрямовані на створення міжнародного правового фреймворку, який регулює питання кібербезпеки та вирішує етичні виклики. Докладніше деякі з цих нормативів:

1. Кібербезпекова стратегія Європейського Союзу: цей документ визначає основні принципи та стратегічні напрями у сфері кібербезпеки в країнах Європейського Союзу. Він закликає до розробки єдиної системи стандартів, яка б забезпечувала високий рівень кіберзахисту в усіх членів Союзу. Метою документа є підвищення рівня безпеки в цифровому просторі та ефективна взаємодія між країнами.

2. Будапештська конвенція про кіберзлочинність: ця конвенція, прийнята Радою Європи, визначає кіберзлочини та встановлює норми для боротьби з ними. Документ зобов'язує учасників приймати ефективні заходи щодо криміналізації кіберзлочинів та співпрацювати в їх розслідуванні та обміні інформацією. Крім того, конвенція закликає додержуватися етичних принципів в цифровому просторі.

3. Угода про створення міжнародних норм у кіберпросторі (Paris Call for Trust and Security in Cyberspace): ця угода була запропонована Францією та прийнята численними державами, компаніями та цивільним суспільством. Вона визначає принципи безпеки в кіберпросторі та закликає до співпраці у сфері кібербезпеки.

Угода визнає, що ефективна боротьба з кіберзагрозами потребує спільних зусиль та дотримання етичних норм.

4. Група G7+: вирізняється активною роботою у напрямку формування міжнародних стандартів кібербезпеки. Їхні спільні декларації та плани дій визначають етичні аспекти управління кібербезпекою та підкреслюють важливість співпраці для вирішення глобальних кіберзагроз.

5. Співпраця НАТО та Європейського Союзу в кіберпросторі: об'єднуючи свої зусилля, НАТО та Європейський Союз активно сприяють розвитку міжнародних норм та стандартів кібербезпеки. Ця співпраця спрямована на забезпечення етичних принципів у кіберпросторі та координацію заходів для протидії кіберзагрозам.

Міжнародні нормативні акти та угоди грають важливу роль у визначенні етичних стандартів управління кібербезпекою. Ці документи встановлюють спільні цілі, обов'язки та принципи, які сприяють ефективній та етичній роботі в цифровому просторі.

*Національне законодавство та регулювання.* Національне законодавство та регулювання в галузі кібербезпеки визначають правові норми та обов'язки, що стосуються цифрового простору в межах кожної держави. Етичні ситуації в кібербезпеці тісно пов'язані з правовими аспектами, і національне законодавство грає ключову роль у врегулюванні цих питань. Етичні ситуації в управлінні кібербезпекою в Україні часто визначаються та обмежуються відповідним законодавством.

Створення та актуалізація кіберзаконодавства. Держави активно розробляють та впроваджують нові закони та нормативні акти, щоб відповідати зростаючим загрозам у кіберпросторі. Ці документи визначають правові рамки для захисту інформації, персональних даних та кіберінфраструктури. Етичні аспекти управління кібербезпекою враховуються при формулюванні та аналізі цих правил.

Захист особистої інформації та приватності. Багато країн встановлюють закони, спрямовані на захист особистої інформації громадян та їхньої приватності в

цифровому середовищі. Етичні питання, пов'язані зі збором, зберіганням та обробкою даних, відображаються у відповідних правових нормах. Національні закони про захист особистих даних та приватності в Україні визначають права громадян на конфіденційність та контроль над своєю інформацією. Етичні аспекти включаються в регулювання обробки та зберігання особистих даних.

Кібербезпека критичної інфраструктури. Національне законодавство визначає обов'язки щодо захисту критичної інфраструктури від кіберзагроз. Закони в цій області регулюють дії та відповідальність суб'єктів, що управляють критичною інфраструктурою. Українське законодавство визначає критичну інфраструктуру та встановлює стандарти безпеки для її захисту від кіберзагроз. Принципи солідарності та відповідальності враховуються при визначенні обов'язків та заходів з кіберзахисту.

Кримінальна відповідальність за кіберзлочини. Законодавство визначає види кіберзлочинів та встановлює кримінальну відповідальність за їх вчинення. Українське законодавство передбачає кримінальну відповідальність за кіберзлочини. Кіберпростір регулюється таким чином, щоб запобігти порушенням етичних норм та покарати їхніх винуватців.

Міжнародна співпраця та екстрадиція. Законодавство також регулює питання міжнародної співпраці та екстрадиції у сфері кібербезпеки. Створення взаємних правових механізмів та процедур сприяє більш ефективній боротьбі з кіберзлочинами. Україна активно взаємодіє з іншими країнами у сфері кібербезпеки, що відображено в національному законодавстві. Забезпечення міжнародної співпраці та екстрадиції слугує етичним принципам колективної відповідальності та спільної боротьби з кіберзагрозами.

Національне законодавство та регулювання визначають контекст для етичних розмірів управління кібербезпекою, надаючи правовий фундамент для ефективного реагування на кіберзагрози та враховуючи принципи справедливості, прозорості та особистої відповідальності.

*Захист прав та свобод користувачів*. Забезпечення захисту прав та свобод користувачів у кіберпросторі має вирішальне значення для формування етичних стандартів управління кібербезпекою. Це питання включає різні аспекти, які забезпечують безпеку та конфіденційність в інтернеті та інших цифрових середовищах. Зокрема, розглянемо загальні принципи та правові норми, що стосуються цього аспекту:

Законодавчий захист персональних даних. Багато країн визнають необхідність законодавчого захисту персональних даних користувачів. Такі закони встановлюють правила для збирання, обробки та зберігання особистої інформації та надають користувачам контроль над її використанням. Українське законодавство визначає права та обов'язки користувачів в кіберпросторі. Зокрема, "Закон про захист персональних даних" та "Закон про інформацію" встановлюють принципи обробки даних та відповідальність за їх захист.

Право на конфіденційність комунікацій. Користувачі мають право на конфіденційність своїх комунікацій. Це включає захист особистих повідомлень, електронної пошти та інших форм електронного спілкування від несанкціонованого доступу та перегляду. Законодавство України передбачає обмеження стосовно збирання та використання персональних даних користувачів без їхнього відповідного дозволу. Це сприяє етичним аспектам управління кібербезпекою, забезпечуючи конфіденційність та прозорість.

Захист від дискримінації в інтернеті. Принципи рівності та захист від дискримінації в інтернеті є важливою складовою етичного управління кібербезпекою. Закони забороняють цифрову дискримінацію та передбачають відповідальність за порушення цих принципів.

Відповідальність платформ та сервісів. Законодавство передбачає відповідальність за безпеку користувачів для платформ та сервісів в інтернеті. Це включає заходи щодо захисту даних та забезпечення безпечного використання платформ.

*Визначення юридичної відповідальності за кіберзлочини.* В контексті кібербезпеки, питання юридичної відповідальності за кіберзлочини визначає ключові принципи і механізми виявлення та карантину кіберзлочинців. Основні аспекти цього питання:

- юридичні норми та кримінальне право: кожна країна має свої юридичні норми, які визначають кіберзлочини та передбачають за них відповідальність. Зазвичай, це включає в себе закони, спрямовані на боротьбу з несанкціонованим доступом, крадіжкою даних, кібертероризмом та іншими формами цифрового правопорушення.

- міжнародна співпраця та екстрадиція: у світі великої кількості кіберзлочинів, співпраця між країнами важлива для ефективного виявлення та карантину злочинців. Механізми екстрадиції та спільного слідства сприяють подоланню глобальних викликів кібербезпеки.

- роль міжнародних організацій: міжнародні організації, такі як Інтерпол та ООН, грають важливу роль у розробці міжнародних стандартів для боротьби з кіберзлочинами. Вони сприяють обміну інформацією та розробці сумісних стратегій для виявлення і притягнення до відповідальності кіберзлочинців.

- засоби виявлення та моніторингу: засоби виявлення та моніторингу, такі як системи інтрацеребернетичного аналізу, грають рішучу роль у виявленні кіберзлочинців. Ці інструменти забезпечують відстеження незаконної активності та допомагають правоохоронним органам у прийнятті ефективних заходів.

- кіберсуди та юридичні прецеденти: у деяких випадках для вирішення кіберзлочинів можуть створюватися спеціалізовані кіберсуди. Це може допомогти встановленню юридичних прецедентів та уніфікації практики розгляду справ в цифровому середовищі.

Визначення юридичної відповідальності за кіберзлочини включає в себе комплексний підхід, який охоплює законодавчий, міжнародний та технічний аспекти для ефективного контролю та протидії цифровим злочинам.

*Міждержавні відносини в кіберпросторі*. Міждержавні відносини в кіберпросторі визначаються комплексом політичних, економічних та технічних аспектів, які впливають на етичні ситуації та стратегії управління кібербезпекою. Основні з них :

- міжнародні організації та форуми: участь у міжнародних організаціях і форумах, таких як Інтернет-організації та конференції, сприяє обговоренню та розробці етичних принципів управління кібербезпекою на глобальному рівні.

- міждержавне співробітництво: співпраця між державами є важливим фактором ефективного управління кібербезпекою. Створення міждержавних механізмів співробітництва та обмін інформацією допомагає у виявленні та запобіганні кіберзагрозам.

Міждержавні відносини в кіберпросторі зумовлюють формування етичних норм та стратегій управління кібербезпекою, враховуючи геополітичні реалії та міжнародні стандарти.

*Цивільно-правовий захист власності в кіберпросторі*. Цивільно-правовий захист власності в кіберпросторі є важливою складовою управління кібербезпекою, оскільки визначає правові норми та механізми захисту прав власності в цифровому середовищі.

Авторські та патентні права: цифрове середовище створює нові виклики для захисту авторських та патентних прав. Розробники програмного забезпечення та винахідники повинні мати чіткі цивільно-правові механізми захисту своїх інтелектуальних власностей.

Контрактні зобов'язання: угоди та контракти в цифровому середовищі вимагають ретельного юридичного аналізу та чітко визначених правових зобов'язань. Етичний захист власності включає в себе дотримання умов контрактів та взаємної довіри між сторонами.

Цивільно-правова відповідальність: визначення цивільно-правової відповідальності за кіберзлочини є важливим етичним аспектом. Збитки, завдані

через кібератаки чи крадіжки даних, повинні бути відшкодовані відповідно до чинного законодавства.

Захист особистих даних: цивільно-правовий захист особистих даних визначає обов'язки організацій та користувачів щодо збереження конфіденційності особистої інформації. Законодавство повинно гарантувати право на приватність та контроль за власними даними.

Правовий вплив на етичні ситуації в кібербезпеці має велике значення, оскільки він створює основи для визначення моральних та етичних меж у цифровому просторі. Забезпечення консистентності та адаптабельності правових норм дозволить вирішувати етичні виклики в еволюційному середовищі кібербезпеки.

2.1.3. Соціальні аспекти управління етикою в кібербезпеці.

Управління етикою в кібербезпеці необхідно розглядати у широкому соціальному контексті, оскільки вплив на суспільство, культуру та взаємовідносини в Інтернеті може мати значущі наслідки. Ключові аспекти соціального впливу на управління етикою в кібербезпеці:

*Взаємодія з інтернет-спільнотою*. Соціальні мережі та онлайн-спільноти створюють нові виклики для етичного управління кібербезпекою. Важливо враховувати погляди та потреби користувачів, активно взаємодіючи з ними та створюючи прозорі правила безпеки.

*Вплив технологій на соціальні відносини*. Зростання технологій впливає на соціальні відносини та взаємодію між людьми. Управління етикою повинно враховувати вплив цифрового середовища на комунікацію та взаєморозуміння.

*Інформаційний простір як соціокультурний феномен*. Сучасний кіберпростір визначає соціокультурні тенденції. Управління етикою повинно враховувати культурні різниці та сприяти створенню умов для безпечної та етичної взаємодії.

Освіта та свідомість. Управління етикою включає в себе ініціативи щодо освіти та підвищення свідомості щодо кібербезпеки. Інформування громадськості про етичні аспекти та небезпеки в Інтернеті є важливим завданням.

*Безпека дітей та споживачів*. Особливу увагу варто приділити етичним аспектам управління безпекою дітей та споживачів в кіберпросторі. Визначення етичних стандартів та норм для захисту прав найвразливіших користувачів є невід'ємною частиною ефективного управління.

Враховуючи соціальні аспекти управління етикою в кібербезпеці, можна створити ефективні стратегії, спрямовані на забезпечення безпеки та захисту прав користувачів в онлайн-середовищі.

## 2.2. Аналіз різних підходів до етичного управління кібербезпекою у різних країнах та організаціях.

Розберемо підходи до етичного управління кібербезпекою на прикладі США, Німеччини, Великобританії та України.

Табл.2.1

Порівняння підходів до етичного управління кібербезпекою у різних країнах

| | США | Німеччина | Велика Британія | Україна |
|---|---|---|---|---|
| Нормативне регулювання | Найбільш відомими є Закон про кібербезпеку (Cybersecurity Act) та Закон про захист інформації в галузі кіберпростору | Закон про безпеку мереж та інформації (BSIG) визначає основні принципи безпеки в кіберпросторі та передбачає санкції за | Закон про мережі та інформацію (Network and Information Systems Regulations) встановлює вимоги до елементів | Закон "Про основні засади забезпечення кібербезпеки України" визначає основні принципи етичного |

| | | | | |
|---|---|---|---|---|
| | (Cyber Information Sharing and Protection Act). | порушення етичних норм. | інфраструктури, які впливають на безпеку. | управління кібербезпекою. |
| Культурні відмінності | високий рівень розвитку інформаційних технологій та швидкий темп їхнього впровадження формують особливості сприйняття етичних питань у кібербезпеці. Зокрема, велика увага приділяється захисту особистої інформації та приватності користувачів. | особиста приватність та захист особистих даних вважаються ключовими етичними питаннями. Регуляції GDPR визначають стандарти для обробки та захисту особистої інформації. | Британське суспільство високо цінує захист приватності та етичну обробку даних. | в Україні, подібно до інших країн, існують відмінності в розумінні кібербезпеки через різницю в культурних підходах та особливостях сприйняття технологій. |
| Взаємодія галузей | банківський сектор, технологічні компанії та урядові агентства активно обмінюються інформацією та співпрацюють для виявлення | співпраця між різними галузями, такими як промисловість, уряд та наука, відіграє ключову роль у розвитку ефективних | галузева співпраця визначається через Центр кібербезпеки Великої Британії (National Cyber Security Centre, NCSC). | Український центр кібербезпеки виступає ключовим органом для координації зусиль між урядовими органами, приватним |

| | | | | |
|---|---|---|---|---|
| | та запобігання загроз. | стратегій кібербезпеки. | | сектором та громадськістю. |
| Міжнародна співпраця | взаємодіють з іншими країнами у сфері кібербезпеки через міжнародні організації та форуми, такі як Об'єднані Нації та Група 7. | співпрацює на міжнародному рівні у галузі кібербезпеки через Європейський Союз, НАТО та інші міжнародні платформи. | активно співпрацює з іншими країнами та міжнародними організаціями у сфері кібербезпеки. | активно співпрацює з міжнародними організаціями та партнерами. |

Аналіз підходів до етичного управління кібербезпекою в різних контекстах є необхідним для створення єдиної системи стандартів, яка враховує різноманітність сучасного світу. Урахування цих різниць дозволить створити більш комплексну та ефективну систему етичного управління кібербезпекою на міжнародному рівні.

### 2.3. Визначення ролі етики в прийнятті стратегічних рішень та політик управління кібербезпекою.

Прийняття стратегічних рішень та формування політик у сфері кібербезпеки вимагає глибокого розуміння етичних аспектів, оскільки ці рішення можуть суттєво впливати на безпеку та приватність користувачів, а також визначати етичні межі в діяльності організацій та держав. Важливо дотримуватися принципів справедливості, прозорості та поваги до приватності працівників. Ось кілька аспектів, які демонструють важливість етики в управлінні:

1. Довіра і репутація: етичні рішення сприяють побудові довіри серед співробітників, клієнтів, партнерів та громадськості. Захист прав і свобод співробітників, дотримання прозорості в управлінні, справедливість при прийнятті рішень сприяють створенню довіри серед персоналу. Коли працівники вірять у справедливість і етичність внутрішнього управління, це позитивно впливає на робочий клімат і продуктивність. Дотримання етичних норм позитивно впливає на репутацію компанії в цілому. Добра репутація створює переваги в конкурентному середовищі, допомагає привертати талановитих співробітників та забезпечує стійкість бізнесу в довгостроковій перспективі.

2. Підвищення конкурентоспроможності: компанії, що дотримуються високих етичних стандартів, можуть привертати більше клієнтів і партнерів, оскільки багато людей обирають підтримувати саме такі підприємства. Організації створюють сприятливе середовище для праці, що збільшує залучення та утримання кваліфікованих співробітників. Це може впливати на продуктивність та інновації. Та споживачі все більше стають свідомими щодо етичних питань, і компанії, які активно демонструють свою соціальну відповідальність, можуть привертати більше уваги та викликати позитивний сприйняття на ринку.

3. Зменшення ризиків: Запровадження чітких етичних стандартів та процедур допомагає уникнути можливих порушень та їхніх наслідків. Це сприяє зменшенню ризиків щодо відповідальності, правопорушень та інших негативних сценаріїв. Законодавчі порушення можуть призвести до серйозних правових наслідків. Етичний підхід допомагає уникати таких порушень і є ефективним інструментом для запобігання конфліктам із законодавством. Правопорушення та інші негативні наслідки неетичної поведінки можуть призвести до серйозних фінансових втрат. Формування політик допомагає уникнути таких ситуацій та підтримує стійкість фінансового становища компанії.

4. Сталість та стійкість: Засновані на етиці стратегії сприяють побудові позитивної репутації компанії. Підтримка чесних та відкритих стосунків із споживачами, партнерами та іншими стейкхолдерами створює сталу платформу для

розвитку бізнесу. Етичне керівництво сприяє розробці стратегій, які враховують не тільки поточні, а й майбутні виклики. Це допомагає компанії адаптуватися до змін у бізнес-середовищі та залишатися стійкою в умовах конкуренції. Етика в управлінні допомагає створити довгострокові та стійкі відносини з партнерами, клієнтами та іншими зацікавленими сторонами. Це створює підґрунтя для сталого розвитку бізнесу та розширення його можливостей.

Етика грає важливу роль у прийнятті стратегічних рішень в управлінні кібербезпекою. При прийнятті рішень компаніям слід враховувати не лише технічні аспекти, а й етичні принципи, які забезпечують збалансований підхід до управління ризиками та захисту інформації. Етика передбачає прозорість та відповідальність у прийнятті рішень з управління. Прозорість включає розкриття основних положень стратегій безпеки перед публікою та зацікавленими сторонами, що допомагає побудувати довіру. Відповідальність передбачає узгоджені дії при управлінні та захисті інформації.

Важливим є врахування соціокультурного контексту при розробці стратегій. Різні культурні особливості можуть впливати на сприйняття заходів безпеки та реакцію споживачів і співробітників. Стратегії повинні бути узгоджені з цінностями компанії, відображаючи високі етичні стандарти в захисті даних і конфіденційності.

Аналіз етичних ризиків є необхідним етапом у прийнятті стратегічних рішень. Це включає обдумане управління можливими негативними впливами на приватність, свободу та інші аспекти життя користувачів. Співробітництво зі спільнотою та регуляторами є ключовим елементом етичного управління кібербезпекою, дозволяючи враховувати різноманітні погляди та забезпечувати широкий підхід до розробки стратегій.

Вплив етичних рішень на створення політик з управління кібербезпекою є важливим задля розвитку стійких та етичних стратегій в цій галузі. Етика в цьому контексті виступає визначальною силою, яка формує принципи, цінності та стандарти, що направляють створення та реалізацію політик управління.

Одним із важливих аспектів є визначення цілей та пріоритетів, що базуються на етичних принципах. Етика надає орієнтири для визначення основних цінностей, таких як приватність, свобода вираження та чесність, які повинні бути захищені в рамках політики з управління кібербезпекою.

Забезпечення прозорості у діяльності є також важливою складовою етичних рішень. Користувачам та іншим зацікавленим сторонам слід надавати зрозумілу інформацію щодо збирання, зберігання та обробки їхніх даних, щоб вони могли приймати обґрунтовані рішення.

Регулювання використання технологій є ще однією важливою складовою етичних рішень у сфері кібербезпеки. Етичні принципи визначають межі використання технологій для запобігання порушенням приватності.

Захист прав та свобод користувача також є обов'язковим врахуванням у політиці з управління кібербезпекою. Етичні рішення визначають стандарти для запобігання зловживань та незаконного використання інформації. Суспільна відповідальність визначається етичними цінностями та підкреслює важливість внеску компаній та організацій у розвиток безпечного та етичного кіберпростору.

Етичні аудити та оцінка ризиків стають необхідні для виявлення можливих етичних порушень та забезпечення їхньої своєчасної корекції.

Розглядаючи роль етики в прийнятті стратегічних рішень та формуванні політик управління кібербезпекою, очевидно, що етика є необхідною складовою для досягнення балансу між безпекою та захистом прав та свобод користувачів. Врахування етичних принципів сприяє створенню ефективних та справедливих стратегій, що враховують потреби всіх зацікавлених сторін.

# РОЗДІЛ 3

# МЕТОДИ ВИРІШЕННЯ СКЛАДНИХ ЕТИЧНИХ СИТУАЦІЙ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ

## 3.1. Етичні принципи та стандарти в управлінні кібербезпекою

Розглядаючи етичні принципи та стандарти, ми досліджуємо їхній вплив на прийняття рішень в умовах складних етичних ситуацій та оцінюємо їхню роль у створенні ефективної системи управління. Методи охоплюють не лише технічні аспекти кібербезпеки, але й глибокі етичні питання, які виникають в процесі прийняття стратегічних рішень та формування політик управління кібербезпеки.

*Принцип справедливості* в контексті управління кібербезпекою зосереджений на чесному та рівномірному розподілі ресурсів та відповідальності між усіма сторонами. В етичних ситуаціях, пов'язаних із кібербезпекою, цей принцип набуває особливої важливості, оскільки рішення та заходи безпеки можуть впливати на різні групи людей та організації.

Засади принципу справедливості в управлінні кібербезпекою:

- розподіл ресурсів: розподіл ресурсів в області кібербезпеки визначається принципом справедливості та відіграє ключову роль у забезпеченні ефективного та рівномірного захисту інформації. Цей аспект етичного управління стає критичним у світлі постійно зростаючих кіберзагроз та вимагає уважного врахування. Ресурси включають бюджетні кошти, технічні засоби, персонал і знання. Справедливий розподіл ресурсів є ключовим чинником для забезпечення адекватного рівня захисту для всіх аспектів організації. Це допомагає уникнути ситуацій, коли одні відділи чи проекти отримують значно більше, ніж інші, що може вести до виникнення слабких місць у безпеці. Визначення відповідальності за розподіл ресурсів може бути покладене на топ-менеджмент організації та керівників відділів.

Вони повинні враховувати конкретні потреби кожного підрозділу та ефективно розподіляти ресурси для максимального покращення загального рівня кібербезпеки. Узгоджений та етичний розподіл ресурсів є важливою передумовою створення ефективної системи кібербезпеки, яка не тільки враховує індивідуальні потреби кожного підрозділу, але й гарантує спроможність організації в цілому ефективно відповідати на виклики в кіберпросторі.

- доступ до інформації: доступ до інформації в контексті управління кібербезпекою визначається як етичний принцип, що забезпечує правильне використання та обмін інформацією в організації. Цей принцип є невід'ємною частиною етичної парадигми, оскільки він визначає обов'язки та відповідальність відповідних сторін щодо отримання, обробки та передачі інформації. Принцип доступу до інформації передбачає встановлення чітких правил та процедур, які регулюють, хто, як і для яких цілей може мати доступ до конкретних інформаційних ресурсів. Це включає в себе створення безпечних механізмів ідентифікації та автентифікації користувачів. Однією з ключових складових етичного управління є наявність чіткого керівництва та нагляду за процесами доступу до інформації. Відповідальні керівники повинні встановлювати прозорі правила та контролювати надання доступу, переконуючись, що це відбувається відповідно до етичних норм. При реалізації принципу доступу до інформації вкрай важливо дотримуватися етичних стандартів обробки та зберігання даних. Це означає використання безпечних технологій, які гарантують конфіденційність та цілісність інформації. Доступ до інформації передбачає встановлення процедур для делегування доступу відповідно до ролей та обов'язків. Керівники повинні визначити, кому та в яких випадках можна надавати доступ, а також повідомляти про це відповідних зацікавлених сторін. Принцип доступу до інформації створює етичний фундамент для ефективного та безпечного управління

кібербезпекою, де збалансованість, відповідальність та справедливість грають визначальну роль у взаємодії з інформацією в кіберпросторі.

- визначення відповідальності: визначення відповідальності в управлінні кібербезпекою є ключовим етичним принципом, що спрямований на визначення обов'язків, повноважень та відповідальності за безпеку кіберпростору в організації. Цей принцип спрямований на створення чіткої системи розподілу відповідальності для забезпечення ефективного управління ризиками та збереженням конфіденційності, цілісності та доступності інформації. Визначення відповідальності включає в себе чітке формулювання обов'язків та повноважень для кожного працівника в контексті кібербезпеки. Це визначення ролей та відповідальностей грає важливу роль у створенні ефективної системи управління кібербезпекою.
- визначення відповідальності: визначення відповідальності в управлінні кібербезпекою є ключовим етичним принципом, що спрямований на визначення обов'язків, повноважень та відповідальності за безпеку кіберпростору в організації. Цей принцип спрямований на створення чіткої системи розподілу відповідальності для забезпечення ефективного управління ризиками та збереженням конфіденційності, цілісності та доступності інформації. Визначення відповідальності включає в себе чітке формулювання обов'язків та повноважень для кожного працівника в контексті кібербезпеки. Це визначення ролей та відповідальностей грає важливу роль у створенні ефективної системи управління кібербезпекою.

  У контексті кібербезпеки, визначення відповідальності охоплює взаємодію різних команд та відділів в організації. Це може включати комунікацію між відділами IT, юридичним відділом, відділом з розробки політик та безпеки. Важливим аспектом є визначення, хто несе відповідальність за корпоративні дані. Це включає в себе розподіл відповідальності за зберігання, обробку та захист конфіденційної інформації від несанкціонованого доступу. У визначенні відповідальності важливо враховувати також здатність організації реагувати на інциденти. Це означає

визначення осіб або команд, відповідальних за негайне реагування та відновлення роботи системи після інциденту. Визначення відповідальності також передбачає наявність механізмів для обліку та врегулювання порушень етичних норм. Це може включати в себе внутрішні аудити та регулярне перегляд етичних процедур. Загальною метою принципу відповідальності в управлінні кібербезпекою є створення ефективної та безпечної кіберсереди, де всі учасники взаємодії мають чітку усвідомленість своїх обов'язків та спільну відповідальність за їх виконання.

- захист прав користувачів: захист прав користувачів є невід'ємною частиною етичного управління кібербезпекою та принципу справедливості, оскільки забезпечення конфіденційності, приватності та прав користувачів є основою довіри та легітимності кіберпроцесів. Враховуючи поширеність використання цифрових технологій, це набуває особливого значення для захисту інтересів користувачів та виключення можливостей зловживання їхніми правами. Однією з ключових складових захисту прав користувачів є забезпечення конфіденційності особистих даних та інформації користувачів. Організації повинні дотримуватися високих стандартів захисту приватності, уникати неправомірного збору та використання даних. Захист прав передбачає, що користувачі мають право на контроль за своєю інформацією та вибір, щодо того, як ця інформація використовується. Організації повинні надавати чітку інформацію про збір та обробку даних, а також забезпечувати можливість відмови від деяких видів обробки. Ефективний захист прав користувачів включає в себе заходи щодо забезпечення безпеки даних. Це включає в себе використання шифрування, захист від несанкціонованого доступу та системи моніторингу для виявлення інцидентів. Організації повинні забезпечувати адекватні та зрозумілі умови використання своїх сервісів та продуктів. Це включає в себе чесну та доступну інформацію про умови використання, правила конфіденційності та політику безпеки. Захист прав користувачів

передбачає уникнення будь-якої форми дискримінації, включаючи обробку даних, що може призвести до негативного впливу на користувачів через їхні особисті чи соціальні характеристики. Принцип захисту прав користувачів є важливим в управлінні кібербезпекою, адже він визначає основи довіри та взаєморозуміння між користувачами та організаціями. Забезпечення цих прав сприяє створенню етичного і безпечного інформаційного простору.

*Принцип прозорості* є важливим етичним компонентом управління кібербезпекою, спрямованим на створення відкритого та чесного середовища взаємодії між організаціями та користувачами. Прозорість визначається як якість чи стан того, що є доступним для загального розгляду та розуміння. В контексті кібербезпеки прозорість передбачає доступність та зрозумілість інформації щодо заходів безпеки та політик, що впливають на користувачів та організації. Прозорість є критичним аспектом, оскільки вона не лише сприяє побудові довіри, але й сприяє ефективному вирішенню етичних ситуацій та уникненню конфліктів із зацікавленими сторонами. Забезпечуючи доступність та зрозумілість інформації, організації можуть створити етичний фундамент для своєї діяльності в кіберпросторі.

Розглянемо детальніше основи цього принципу:

- публічність політик та стандарів: принцип прозорості в управлінні кібербезпекою визначає, що організації повинні публічно розголошувати свої політики та стандарти, пов'язані із забезпеченням інформаційної безпеки. Публічність політик та стандартів є ключовою складовою для забезпечення ефективності прозорості, і вона вносить вагомий внесок у розвиток довіри споживачів, партнерів та інших зацікавлених сторін. Публічне розголошення політик і стандартів сприяє побудові довіри серед користувачів, оскільки вони мають можливість ознайомитися із застосовуваними правилами та гарантіями безпеки. Організації можуть активно залучати фідбек від зацікавлених сторін та споживачів, реагуючи на їхні зауваження і вдосконалюючи свої підходи до кібербезпеки.

Публічність політик і стандартів важлива для внутрішніх співробітників, які повинні знати і дотримуватися встановлених правил та вимог безпеки. Публічність політик визначає очікування від споживачів та партнерів, створюючи ясність щодо стандартів безпеки, які будуть застосовані при обробці їхніх даних та інформації. Відповідальність за публічність політик та стандартів лежить на рівні вищого керівництва та відділу кібербезпеки. Це вимагає ретельного аналізу, розробки та узгодження документів, а також їхнього регулярного оновлення відповідно до змін у кіберзагрозах та стандартах безпеки. Прозорість стає керівною засадою, що визначає підходи до управління кібербезпекою.

- зрозумілість умов використання: в сфері кібербезпеки ставить за мету забезпечити, щоб користувачі чітко розуміли умови, які встановлюються для використання кіберпродуктів чи сервісів. Це виступає як важлива складова етичності управління кібербезпекою та враховує права та інтереси користувачів в цифровому середовищі. Зрозумілість умов використання передбачає їхню чіткість та простоту. Мова документів повинна бути доступною для широкого кола користувачів, уникати складних юридичних термінів, щоб умови були зрозумілі кожному. Умови використання повинні містити відомості про потенційні кіберзагрози, пов'язані із використанням продукту або сервісу, а також заходи безпеки, які призначені захистити користувачів від цих ризиків. Компанії повинні висвітлювати умови використання таким чином, щоб вони відповідали принципам честності та прозорості. Користувачі повинні бути проінформовані про всі умови, які можуть вплинути на їхні права чи конфіденційність. Компанії повинні робити умови використання доступними та зрозумілими для споживачів. Це може включати використання зручних форматів, дружніх інтерфейсів та детальних пояснень для роз'яснення складних пунктів. Враховуючи важливість зрозумілості умов використання, компанії виявляють свою етичну

відповідальність перед користувачами, сприяючи створенню довіри та забезпечуючи ефективний захист їхніх прав та інтересів в кіберпросторі.

- відкритість щодо інцидентів: прозорість в кібербезпеці, зокрема відкритість щодо інцидентів, визначається як здатність організацій чітко та вчасно інформувати громадськість, клієнтів та зацікавлених сторін про кібербезпекові інциденти, які можуть вплинути на конфіденційність, цілісність або доступність інформації. Відкритість у розкритті інформації про кіберінциденти підвищує довіру споживачів та інших стейкхолдерів до організації. Компанії, які визнають свої помилки та приймають заходи для виправлення, можуть зберігати лояльність клієнтів. Інформація про інциденти може включати в себе також деталі щодо того, як компанія збирає, обробляє та зберігає дані. Прозорість у цьому плані дозволяє користувачам зрозуміти, як їхні особисті дані будуть використані та захищені. Розкриття інформації про інциденти може бути частиною стратегії з підвищення культури безпеки в організації. Це може включати навчання персоналу щодо небезпек та превентивних заходів. Коли компанія стає жертвою кібератаки, вона може вжити заходів для інформування громадськості та клієнтів про вчинені дії, зазначити вартість інциденту, інформувати про покращення у системах безпеки та надавати рекомендації для захисту особистої інформації. Відкритість щодо інцидентів стає необхідним елементом етичного управління кібербезпекою, сприяючи створенню довіри та збереженню репутації організації.
- співпраця з громадськістю: у сфері кібербезпеки є ключовим аспектом прозорості, спрямованим на створення відкритого та взаємовідкритого середовища між організацією та громадськістю, що сприяє взаєморозумінню, підвищенню свідомості та довірі до заходів з кібербезпеки. Співпраця з громадськістю дозволяє надавати інформацію щодо загроз кібербезпеці, захисних заходів та практик безпеки. Це підвищує рівень свідомості у громадськості та освічає їх про важливість

збереження кібербезпеки. Спілкування з громадськістю дозволяє встановити двосторонній діалог, де організація може слухати погляди, питання та обурення громадськості. Це допомагає враховувати підтримку та відповідати на конкретні потреби та обурення. У випадку кіберінциденту взаємодія з громадськістю допомагає організації ефективно та етично взаємодіяти з постраждалими сторонами, надавати інформацію та виправдовувати вжиті заходи. Одним із прикладів ефективної співпраці з громадськістю є організація прес-конференцій та інших заходів, що спрямовані на роз’яснення загроз, захисних заходів та обговорення питань громадськості щодо кібербезпеки. Співпраця з громадськістю є необхідною частиною впровадження етичних принципів у сфері кібербезпеки, забезпечуючи взаєморозуміння та сприяючи створенню безпечного цифрового середовища.

*Принцип взаємовідповідальності* є ключовим аспектом етичних засад управління кібербезпекою. Цей принцип покликаний встановлювати взаємні зобов'язання та відповідальність між різними сторонами – як організаційними, так і індивідуальними – для спільного забезпечення безпеки в кіберпросторі. Взаємовідповідальність в управлінні кібербезпекою визнає необхідність спільних зусиль для забезпечення стійкості та безпеки в кіберпросторі. Цей принцип стає основою для створення етичного середовища, де всі сторони активно приймають участь у забезпеченні цифрової безпеки. Розглянемо деталі цього принципу в контексті кібербезпеки.

- між організаціями та користувачем: взаємовідповідальність означає чіткий розподіл зобов'язань та завдань між організаціями, що забезпечують кібербезпеку, та користувачами, які взаємодіють з цифровим середовищем. Організації несуть відповідальність за розробку та забезпечення ефективних стратегій та інструментів безпеки, тоді як користувачі повинні дотримуватися визначених правил безпеки та бути активно залученими до процесу захисту. Організації повинні забезпечити користувачів

необхідними знаннями та інструментами для ефективного захисту від кіберзагроз. Це включає надання регулярних тренінгів, оновлення користувачів щодо нових видів загроз та надання рекомендацій щодо безпеки в цифровому середовищі. В умовах взаємовідповідальності організації та користувачі повинні активно співпрацювати та обмінюватися інформацією про потенційні загрози та інциденти. Спільна взаємодія стає ключовою для створення спільних стратегій та ефективного реагування на кібератаки. Взаємовідповідальність між організаціями та користувачами є фундаментальним принципом, який формує етичну основу управління кібербезпекою. Цей підхід дозволяє створити ефективну систему захисту, яка враховує інтереси всіх сторін та сприяє створенню безпечного цифрового середовища.

- між організаціями: взаємовідповідальність між організаціями в контексті управління кібербезпекою є важливим елементом створення ефективних заходів забезпечення безпеки та захисту в кіберпросторі. Цей принцип передбачає активну взаємодію та співпрацю різних суб'єктів у сфері кібербезпеки для досягнення спільних цілей та забезпечення високого рівня захисту від кіберзагроз. Організації повинні спільно розробляти стандарти та процедури з кібербезпеки, які враховують сучасні та еволюційні виклики. Це може включати в себе визначення стандартів безпеки даних, процедур виявлення і реагування на інциденти, та інші аспекти забезпечення безпеки. Взаємовідповідальність передбачає обмін інформацією про виявлені загрози та інциденти між організаціями. Цей обмін сприяє покращенню загального рівня кіберзахисту, оскільки інформація про нові загрози може використовуватися для запобігання атак в інших організаціях. Організації можуть спільно працювати над розробкою та впровадженням технічних рішень у сфері кібербезпеки. Це може включати в себе створення загальних інструментів для виявлення загроз, захисту від атак та відновлення після інцидентів. Взаємовідповідальність між організаціями створює сприятливі умови для

ефективного управління кібербезпекою, підвищуючи загальний рівень захисту від кіберзагроз у всьому галузі.

- в управлінні інцидентами: Взаємовідповідальність в управлінні інцидентами в сфері кібербезпеки визначається необхідністю спільних зусиль та співпраці між організаціями для ефективного виявлення, вирішення та подальшого управління кіберінцидентами. Важливою є відкритість, активний обмін інформацією та взаємопідтримка між різними суб'єктами, які можуть бути як потенційними жертвами, так і експертами в сфері кібербезпеки. Організації повинні спільно працювати над виявленням потенційних загроз інформаційній безпеці. Це може включати обмін інформацією про підозрілу активність, аномалії та інші індикатори компрометації. Коли виникає інцидент, організації повинні спільно реагувати на нього, обмінюючи інформацією про виявлені загрози та способи їхнього ліквідації. Це може включати спільне розслідування, спільне розгортання заходів безпеки та інші кроки для відновлення стану безпеки. Взаємовідповідальність в управлінні інцидентами не тільки полегшує ефективне реагування на кіберзагрози, але й допомагає узгоджувати дії різних організацій для забезпечення високого рівня кібербезпеки в цілому.

*Принцип безпеки інформації* в управлінні кібербезпекою становить одну з ключових складових етичного підходу. Він спрямований на забезпечення конфіденційності, цілісності та доступності інформації. Давайте розглянемо деталі цього принципу:

- конфіденційність: основний аспект безпеки інформації полягає в збереженні конфіденційності даних. Це означає, що інформація повинна залишатися доступною лише тим, хто має право отримати до неї доступ. В управлінні кібербезпекою це передбачає використання шифрування, управління доступом і заходів контролю доступу.
- цілісність: принцип цілісності вказує на те, що інформація має залишатися непошкодженою та недоступною для модифікацій чи змін без належного

дозволу. Для забезпечення цілісності використовуються методи перевірки цілісності даних, цифрові підписи та інші технічні заходи.

- доступність: принцип доступності гарантує, що інформація буде доступна для тих, хто має до неї легальний доступ, у відповідний момент часу. Заходи для забезпечення доступності включають в себе резервне копіювання, застосування високодоступних систем та інші технічні та організаційні заходи.
- технічні середовища: для реалізації принципу безпеки інформації важливо створювати безпечні технічні середовища. Це включає в себе використання безпечних мереж, застосування файрволів, виявлення загроз та інші технічні засоби.
- освіта та свідомість: практично важливим є підвищення освіти та свідомості серед персоналу щодо збереження безпеки інформації. Навчання співробітників виявлятиме соціальні інженерні атаки та інші методи атак, що враховує людський фактор.

Ці аспекти принципу безпеки інформації управління кібербезпекою визнаються важливими для забезпечення етичного та ефективного управління кіберзаходами. Організації повинні бути особливо уважні до цих принципів, оскільки вони визначають загальний стандарт етичної практики в цій області.

У сфері управління кібербезпекою інсценізується велика кількість стандартів та рамок, які допомагають організаціям ефективно управляти своєю кібербезпекою. Деякі з найбільш визнаних та використовуваних стандартів включають:

1. ISO/IEC 27001:2013 (Information Security Management System - ISMS). ISO/IEC 27001:2013 є міжнародним стандартом, який визначає вимоги до систем управління інформаційною безпекою (Information Security Management System - ISMS). Основний зміст стандарту орієнтований на забезпечення конфіденційності, цілісності та доступності інформації в організації.


Рис.3.1. Емблема ISO

2. NIST Cybersecurity Framework.

   Стандарт NIST Cybersecurity Framework розроблений Національним Інститутом стандартів і технологій (NIST) США. Його метою є надання керівництву засобів для розуміння, визначення та зменшення кібербезпекових ризиків для критично важливих інфраструктур та організацій. Framework складається з п'яти основних елементів: Цілей, Визначень та Відомостей, Фреймворку розробки, Реалізації та Сертифікації. Кожен елемент спрямований на певний аспект кібербезпеки. Цілі визначаються інтегровані ініціативи забезпечення кібербезпеки, спрямовані на захист організаційної інфраструктури та даних.

3. CIS Controls (Center for Internet Security).

   Стандарт управління кібербезпекою CIS Controls розроблений організацією Center for Internet Security (CIS). Цей фреймворк визначає 20 конкретних контролів безпеки, спрямованих на забезпечення ефективного захисту інформації та систем в організаціях. Контролі поділені на три групи: Основні, Рекомендовані та Розширені. CIS Controls адресують різноманітні аспекти кібербезпеки, включаючи ідентифікацію, захист, виявлення, відповідь та відновлення. Фреймворк містить конкретні рекомендації та вказівки щодо впровадження кожного з контролів.


Рис.3.2. Емблема CIS

4. COBIT (Control Objectives for Information and Related Technologies).

   COBIT є стандартом управління та контролю за інформаційними технологіями, розроблений ISACA (Information Systems Audit and Control Association) та IT Governance Institute. Його основною метою є забезпечення ефективного управління та контролю над інформаційними технологіями в організаціях. COBIT визначає чотири основних домени (планування та організація, отримання, впровадження та відслідковування), які поділяються на 37 процесів. Встановлює контрольні об'єкти для оцінки та забезпечення ефективності контролю в області інформаційних технологій. COBIT надає фреймворк для визначення та реалізації інформаційних технологій в організації. COBIT використовується організаціями для: покращення управління інформаційними технологіями, забезпечення відповідності із стандартами безпеки та управління та моніторингу та забезпечення якості процесів в інформаційних технологіях. COBIT є універсальним інструментом для керівників інформаційних технологій та внутрішнього аудиту для досягнення стратегічних цілей через ефективне управління та контроль.


Рис.3.3. Стандарт COBIT

5. ISO/IEC 27002 (Code of practice for information security controls).

   ISO/IEC 27002 є стандартом, який визначає практичні рекомендації та контрольні заходи для впровадження і забезпечення ефективності систем управління інформаційною безпекою. Він є доповненням до стандарту ISO/IEC 27001, який визначає вимоги до систем управління інформаційною безпекою. Стандарт включає загальні принципи управління інформаційною безпекою, такі як конфіденційність, цілісність та доступність інформації. Визначаються політики, процедури та відповідальності для ефективного управління інформаційною безпекою. Включають технічні засоби та заходи для захисту фізичних та технічних аспектів інформаційної безпеки. Стандарт надає рекомендації щодо ідентифікації, оцінки та управління ризиками інформаційної безпеки.

6. ITIL (Information Technology Infrastructure Library).

   ITIL (Information Technology Infrastructure Library) є набором передових практик у сфері управління інформаційною технологією (IT). Стандарт складається з набору керівництва та найкращих практик з управління IT-сервісами. Його головною метою є поліпшення якості та ефективності обслуговування IT в організації. ITIL визначає п'ять основних етапів у життєвому циклі сервісу: стратегія, дизайн, впровадження, експлуатація та удосконалення. Визначаються ключові процеси, такі як управління змінами,

управління проблемами, управління конфігурацією тощо. Визначаються ролі та відповідальності для ефективного управління IT-сервісами.

Ці стандарти є лише частиною широкого спектру інструментів, які організації можуть використовувати для забезпечення кібербезпеки. Кожен стандарт має свої особливості та використовується залежно від конкретних потреб та характеру бізнесу.

### 3.2. Методи визначення етичних критеріїв в управлінні кібербезпекою

Обмеження прав користувачів, парольна політика та контроль за її дотриманням. Визначення та впровадження парольної політики в організації вимагає ретельного розгляду етичних аспектів. При встановленні стандартів та вимог до паролів, необхідно дотримуватися принципів приватності та діалогу з користувачами. Етичний підхід передбачає розробку політики, що враховує як безпеку, так і права та зручність користувачів. При впровадженні систем контролю за дотриманням парольної політики, етичні аспекти включають в себе збалансований підхід до безпеки та приватності. Забезпечення конфіденційності особистих даних користувачів під час моніторингу є ключовим етичним аспектом. Важливо враховувати права та свободи користувачів при впровадженні механізмів контролю. Етичний підхід передбачає індивідуальне врахування потреб та прав кожного користувача при визначенні параметрів парольної політики. Справедливість та прозорість у встановленні вимог до паролів для різних категорій користувачів є ключовими етичними аспектами цього процесу. Етичний обов'язок включає публічну відповідальність та звітність стосовно використання та ефективності заходів парольної політики. Забезпечення прозорості та активної інформаційної взаємодії з користувачами дозволяє визначити публічне сприйняття заходів забезпечення кібербезпеки та їхніх етичних аспектів. Розглядаючи ці питання з

етичного погляду, можна забезпечити баланс між безпекою та правами користувачів, підвищуючи загальний рівень кібербезпеки організації.

У контексті забезпечення кібербезпеки, втручання в трафік користувачів визнається ефективним інструментом, але його використання повинно бути суворо обґрунтованим та етично виправданим. Втручання в трафік користувачів, незважаючи на свою ефективність в забезпеченні кібербезпеки, потребує пристосування до етичних стандартів та уваження до прав та приватності користувачів. Розглянемо деякі конкретні сценарії втручання в трафік:

- моніторинг та аналіз персонального трафіку: витриманий моніторинг персонального трафіку користувачів може виявитися важливим для виявлення можливих загроз та кібератак. Однак, важливо чітко обґрунтувати мету такого моніторингу, забезпечуючи високий ступінь прозорості та довіри.
- фільтрація шкідливих доменів та вмісту: ефективна фільтрація доменів і вмісту може допомогти уникнути доступу до шкідливих ресурсів та захистити користувачів від потенційних кіберзагроз. Але, при цьому, важливо уникати безпідставних обмежень та забезпечити можливість апеляцій для користувачів.
- блокування трафіку із заборонених регіонів: блокування трафіку з певних географічних регіонів може стати ефективним заходом уникнення кібератак, але водночас може супроводжуватися питаннями етичності та може викликати обурення з точки зору дискримінації.
- перехоплення та аналіз спаму та фішингових атак: виявлення та блокування спаму та фішингових атак може врятувати користувачів від великої кількості шахрайства, але важливо уникати надмірного втручання в особистий простір користувачів та ретельно захищати їхню конфіденційність.

Збалансоване та обґрунтоване втручання в трафік визначається конкретним контекстом та завданнями організації. Важливо поєднувати заходи з етичними

принципами, дозволяючи забезпечити безпеку, залишаючи при цьому недоторканність прав та приватності користувачів.

Етичність втручання в трафік визначається його впливом на права користувачів та приватність. Забезпечення конфіденційності особистих даних та захист від неправомірного втручання є критичними аспектами, щоб зберегти довіру та підтримати приватність користувачів. Етичне втручання в трафік повинно бути обґрунтованим в контексті забезпечення безпеки. Заходи повинні спрямовуватися на виявлення та запобігання кібератак, вірусів та інших загроз, забезпечуючи при цьому справедливий та прозорий підхід. Для забезпечення довіри користувачів і громадськості важливо проводити публічні інформаційні кампанії щодо втручання в трафік. Прозорість та відкритість стосовно заходів допомагає утримувати сприйняття таких заходів як етично виправданих. Враховуючи різноманітність етичних стандартів, важливо визначити їхню відповідність конкретним сценаріям втручання в трафік. Це допомагає встановити норми та вимоги, які дозволяють ефективне та етичне втручання в інтересах безпеки та приватності.

Управління трафіком та правами користувачів у кіберпросторі вимагає високих етичних стандартів для забезпечення гармонійного збалансованого підходу між безпекою, приватністю та основними правами користувачів.

Ключовим етичним принципом є прозорість взаємин з користувачами. Користувачі повинні бути повністю інформовані про те, яким чином здійснюється втручання в їхні права та приватність. Це включає розкриття політики втручання, його мети та методів моніторингу.

Етичне управління трафіком базується на принципах справедливості для уникнення будь-якої форми дискримінації. Важливо гарантувати рівні права для всіх користувачів та уникати будь-яких форм нерівності у втручанні та моніторингу трафіку.

Основний етичний принцип передбачає абсолютне право користувачів на конфіденційність та захист особистого простору. Управління трафіком повинно

гарантувати захист особистої інформації та уникати будь-якого неправомірного збирання та використання даних.

### 3.3. Аналіз важливості побудови етичного клімату в організаціях, що займаються кібербезпекою

Для забезпечення ефективності, довіри та високого стандарту професійності в кібербезпеці важливий етичний клімат. Аналіз того, наскільки важливо створити етичний клімат, дозволяє зрозуміти його вплив на розвиток і діяльність організації. Він підвищує довіру як внутрішньо, так і зовнішньо серед клієнтів і партнерів. Кібербезпека залежить від довіри, оскільки вона значною мірою ґрунтується на внутрішньому співробітництві та обміні даними. Умови, які є етичними, підвищують моральну мотивацію працівників. Працівники, які відчувають, що їхня робота важлива та мають високі моральні стандарти, більш залучені до діяльності, що впливає на якість кібербезпеки. Правильно спрямований етичний клімат компанії допомагає їй уникати ризиків, пов’язаних із порушенням її моральних принципів, що може призвести до юридичних наслідків. Дотримання етичних норм сприяє дотриманню законів і запобіганню санкціям.

Етичний клімат створює сприятливе середовище для прогресу та винахідливості. Професіонали кібербезпеки, які працюють в етичному середовищі, більш сприйнятливі до новаторських ідей і швидше адаптуються до нових технологій. Етична атмосфера в організації допомагає запобігти конфліктам і внутрішнім розбіжностям. Коли у всіх працівників є спільні етичні цінності, вони працюють разом у згоді та співпраці. Збільшує лояльність співробітників і сприяє збереженню талантів. Кібербезпековці шукають підприємства, де їхні етичні принципи відповідають цілям.

Аналіз побудови етичного клімату в організаціях, що займаються кібербезпекою, вказує на його визначальну роль у формуванні успішної та етичної діяльності. Етичний клімат впливає на всі аспекти роботи, сприяючи довірі, розвитку та уникненню ризиків.

# РОЗДІЛ 4

# ДОСЛІДЖЕННЯ РІЗНИХ МЕТОДІВ ТА ПІДХОДІВ ДО ВИЗНАЧЕННЯ ЕТИЧНИХ КРИТЕРІЇВ ДЛЯ ОЦІНКИ ДІЙ ТА РІШЕНЬ В КІБЕРБЕЗПЕЦІ

## 4.1. Кейси та сценарії вирішення етичних ситуацій. Порівняння їхньої ефективності та можливості застосування

Розглянемо на прикладі декількох ситуацій.

*Кейс 1*: "Доступ до корпоративної інформації"

Ситуація: програміст з високим рівнем доступу вирішив переглянути конфіденційну корпоративну інформацію, щоб виявити можливі недоліки в системі безпеки.

Позитивний сценарій: програміст вчинив дію з метою виявлення слабких місць у системі безпеки. Після виявлення проблем він повідомив відповідні служби безпеки та запропонував шляхи виправлення. Організація визнала його добросовісність та вдячність за виявлення потенційних загроз.

Негативний сценарій: програміст використовує отриману інформацію для особистої вигоди, зловживаючи своїм рівнем доступу. Виявляється, що це порушення корпоративних правил та законів про захист даних. Організація реагує негайно, вживаючи заходів від відсторонення програміста до правових кроків.

Отже, у даному кейсі важливо розрізняти добросовісне вчинення з метою покращення безпеки від зловживання доступом для особистої вигоди. Ефективне етичне управління включає в себе визнання та винагородження доброчесної поведінки, а також негайні заходи при порушенні етичних норм. Цей кейс підкреслює важливість чітких правил користування корпоративними ресурсами та акцентує на потребі ведення свідомої політики етичного управління, що враховує різні можливі сценарії та реагує на них відповідно.

*Кейс 2*: "Публічне розголошення вразливості"

Ситуація: безпековий експерт виявив серйозну вразливість в популярному програмному забезпеченні. Розголошення цієї інформації може призвести до серйозних наслідків для користувачів та розробників.

Публічне повідомлення: експерт повідомляє розробників про вразливість та надає їм строк для виправлення. Якщо виправлення не виконано вчасно, експерт оприлюднює інформацію для захисту користувачів.

Конфіденційне повідомлення: експерт повідомляє про вразливість конфіденційно розробникам, надаючи докладну інструкцію по виправленню. Розробники виправляють вразливість до того, як інформація стає загальнодоступною.

У цьому кейсі розглядається дилема між публічним та конфіденційним повідомленням вразливості.

Публічне повідомлення: переваги - забезпечує широкий доступ до інформації та може прискорити виправлення. Недоліки - може створити паніку серед користувачів та залишити систему вразливою, якщо виправлення затримається.

Конфіденційне повідомлення: переваги - надає розробникам можливість виправити проблему до публічного розголошення. Недоліки - може створити вікно для зловживання вразливістю до виправлення.

Цей кейс акцентує на важливості визначення чіткої та розгорнутої політики відгуку на виявлені вразливості в програмному забезпеченні. Здатність ефективно реагувати на такі ситуації є критичною для забезпечення безпеки користувачів та довіри до продуктів та послуг.

*Кейс 3*: "Конфлікт інтересів у кібербезпеці"

Ситуація: співробітник кібербезпеки виявив вразливість у власній системі, але вирішив не повідомляти про це. Ця вразливість може бути використана для особистої вигоди.

Позитивний сценарій: співробітник повідомляє вищий рівень управління про конфлікт інтересів та вразливість. Вище керівництво вживає заходів для вирішення ситуації та виключення можливості зловживання.

Негативний сценарій: проводиться внутрішнє розслідування для визначення обсягу конфлікту інтересів та його наслідків. Застосовуються внутрішні санкції та заходи для усунення проблеми.

У цьому кейсі виокремлюється етичний конфлікт, коли співробітник кібербезпеки має можливість зловживати своїм становищем для особистої вигоди. Вирішення конфліктів інтересів зберігає довіру персоналу та створює прозорий етичний стандарт. Перевірка та усунення вразливостей, використовуваних для особистої вигоди, сприяє загальній безпеці даних та систем. Цей кейс підкреслює важливість прозорості, етичної поведінки та ефективного вирішення конфліктів інтересів для забезпечення безпеки та довіри в області кібербезпеки.

Усі ці кейси та сценарії допомагають розглянути різні варіанти вирішення етичних ситуацій у сфері кібербезпеки. Аналіз подібних ситуацій дозволяє розробити ефективні стратегії та методи, що сприяють покращенню етичного управління.

### 4.2. Аналіз важливості етичних аспектів у кібербезпеці

Етичні аспекти в галузі кібербезпеки стають не лише моральним вибором, але й стратегічно важливим елементом управління кібербезпекою. Розглянемо важливість та їхній вплив на прийняття рішень у цій комплексній області.

Довіра є основою взаємодії між організацією та користувачами. Репутація безпеки визначає ставлення споживачів до продуктів та послуг. Недостатня увага до етичних аспектів може призвести до витоку даних, порушень конфіденційності, і загрозити репутації компанії.

Відповідність законодавчим вимогам та етичній природі заходів визначає легітимність та законність діяльності організації. Недодержання законодавства та етичних стандартів може призвести до юридичних проблем, штрафів, та втрати легітимності.

Етичне відношення до персональних даних гарантує їхню конфіденційність та відповідність правам користувачів. Недбале ставлення до обробки персональних даних може призвести до порушень приватності та порушення законодавства.

Етичні аспекти визначають стратегії та рішення в галузі кібербезпеки, враховуючи можливі соціальні та етичні наслідки. Розробка технічних рішень без врахування етичних аспектів може призвести до виникнення нових етичних проблем та конфліктів.

Етичне планування управління кібербезпекою дозволяє уникнути конфліктів інтересів та забезпечити відповідність дій етичним стандартам. Відсутність узгодженості між стратегічним плануванням та етичними принципами може призвести до внутрішніх конфліктів та неефективності стратегій.

Врахування різноманітних поглядів експертів та громадськості підсилює процес управління кібербезпекою. Відсутність залучення громадськості може призвести до обмеженості поглядів та пропущених можливих ризиків.

Створення культури професійної відповідальності формує високий стандарт поведінки та професіоналізму. Відсутність професійної відповідальності може призвести до використання влади в особистих інтересах та загрожувати ефективності управління.

Аналіз важливості етичних аспектів у кібербезпеці підкреслює їхню критичну роль у формуванні стійкої та довірливої кібербезпечної екосистеми. Кожен аспект етики визначає та впливає на стратегії управління кібербезпекою, надаючи їм етичну основу та сприяючи їхній ефективності. Довіра користувачів, легітимність діяльності, захист персональних даних та вплив на технічні рішення є лише кількома аспектами, що демонструють, як етика переплітається з кожним аспектом

управління кібербезпекою. Стратегічне планування, залучення експертів, та професійна відповідальність є важливими елементами, які формують відмінність та високий рівень професіоналізму в цій галузі. Недоліки в будь-якому з цих аспектів можуть вести до етичних проблем, порушень довіри, та загроз для безпеки в цифровому просторі.

Отже, етика в кібербезпеці є необхідною. Забезпечуючи відповідність етичним принципам, організації сприяють створенню екосистеми, яка не лише забезпечує захист, але і підтримує довіру, легітимність та стабільність в цифровому світі.

### 4.3. Формулювання рекомендацій для організацій

Вирішення складних етичних ситуацій в управлінні кібербезпекою вимагає високого рівня осмисленості, компетентності та врахування різноманітних факторів. Це може бути досягнуто за допомогою різних методів та стратегій, спрямованих на етичне та відповідальне прийняття рішень, які ми розглянули раніше. Ось кілька рекомендацій для покращення цих методів, які необхідно враховувати при прийнятті рішень у складних етичних питаннях:

Застосування встановлених етичних принципів та стандартів: застосування встановлених етичних принципів та стандартів дозволяє оцінити етичність різних ситуацій та вибрати оптимальний шлях дії. Розробка та впровадження політики, що базується на загальноприйнятих етичних принципах та стандартах.

Етичні комітети та консультації: створення етичних комітетів та залучення консультантів допомагає вирішувати етичні питання колективно та за участю різних груп. Впровадження системи консультацій та створення етичних комітетів для аналізу та вирішення етичних дилем.

Засоби навчання: організація тренінгів та навчань з етики в кібербезпеці сприяє підвищенню свідомості персоналу щодо етичних викликів та надає їм необхідні

інструменти для прийняття правильних рішень. Впровадження систем навчання та регулярних тренінгів для персоналу на основі конкретних етичних сценаріїв.

Етичні аудити та моніторинг: роведення регулярних етичних аудитів та моніторингу дозволяє виявляти та вирішувати етичні проблеми у реальному часі. Впровадження системи аудитів та моніторингу для визначення етичних відхилень та реагування на них.

Діалог та залучення громадськості: активний діалог з громадськістю та залучення до розв'язання етичних питань сприяє уникненню конфліктів із зацікавленими сторонами. Організація публічних обговорень та регулярних зустрічей для обговорення етичних аспектів управління кібербезпекою.

Регулярне оновлення політик: регулярне оновлення політик етики відповідно до змін у кібербезпеці та законодавстві.

Співпраця з експертами: укладення партнерств з етичними експертами та організація регулярних консультацій.

Створення інтерактивних сценаріїв: розробка інтерактивних сценаріїв етичних ситуацій для тренінгів та навчань, що дозволяють персоналу взаємодіяти з реальними ситуаціями.

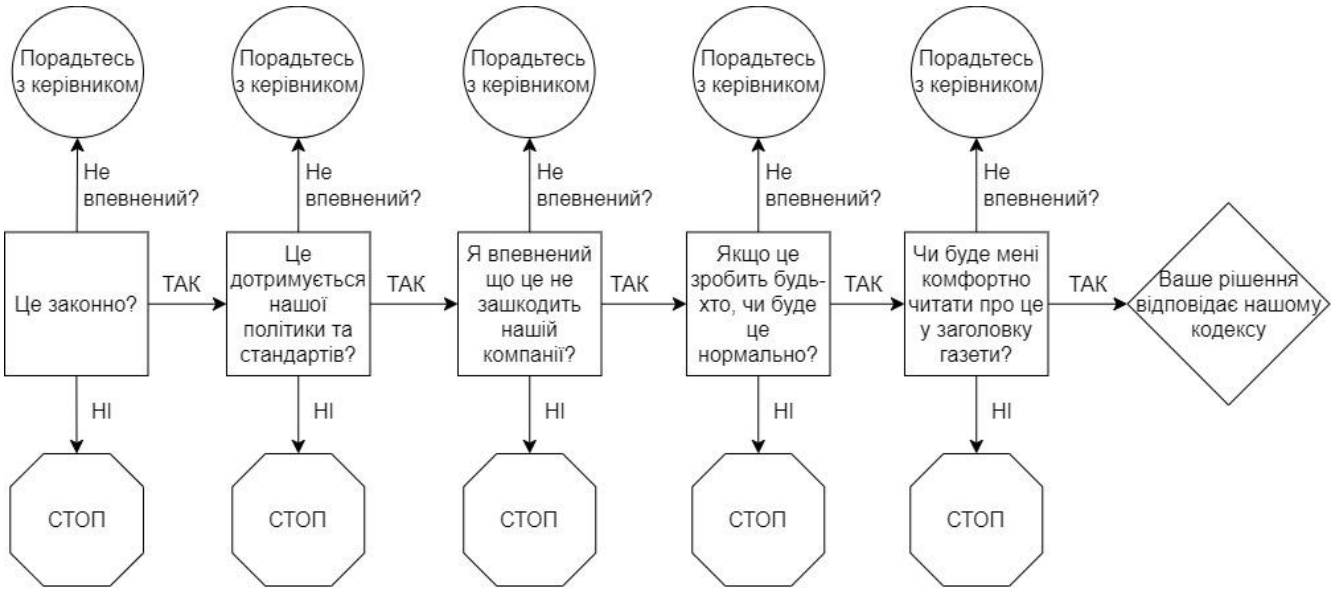


Рис.4.1. Алгоритм вирішення етичних ситуацій в управлінні

На рис.4.1. показаний алгоритм для вирішення складних етичних ситуацій в управлінні кібербезпекою. Зроблений враховуюючи всі основні принципи та етичні аспекти: безпеки інформації, взаємовідповідальності, довіри та прозорості, справедливості, зв’язків з громадськістю та інших. Та обов’язково враховуюючи стандартів та політик безпосередньо компанії.

Методи вирішення етичних ситуацій в управлінні кібербезпекою потребують інтеграції новаторських та гнучких підходів. Рекомендації, наведені вище, можуть слугувати основою для покращення цих методів, забезпечуючи ефективний та етичний управлінський підхід у кібербезпеці.

# ВИСНОВКИ

Управління кібербезпекою в сучасному світі вимагає не лише технічних знань і стратегій, але й уважного врахування етичних аспектів. Етика в управлінні кібербезпекою відіграє ключову роль у забезпеченні справедливості, прозорості, взаємовідповідальності та безпеки інформації. Розгляд етичних принципів та стандартів, вивчення культурних, правових і соціальних впливів, а також аналіз ролі етики в управлінні кібербезпекою дозволяє сформулювати ефективні стратегії та політики, які враховують високі стандарти етичності.

Важливість етичної складової в управлінні кібербезпекою є вкрай великою. Врахування етичних аспектів підвищує рівень довіри як серед персоналу, так і серед клієнтів. Добра репутація є ключовим активом в управлінні кібербезпекою. Етичні рішення допомагають уникнути порушень приватності та забезпечують права користувачів. Організації, які дотримуються етичних стандартів, вважаються більш привабливими для співробітників та клієнтів, що сприяє підвищенню їх конкурентоспроможності. Етична орієнтація дозволяє уникнути ситуацій, що можуть призвести до порушень безпеки та втрати даних. Організації, що враховують етичні принципи, мають стійку основу та здатні впоратися з викликами кібербезпеки на тривалий термін.

У першому розділі проведено аналіз основних етичних понять у галузі кібербезпеки . Розглядались не лише теоретичне визначення термінів, але й їхнє практичне застосування у сучасному інформаційному середовищі.

У другому розділі здійснювалось дослідження впливу культурних, правових і соціальних чинників на етичні ситуації в управлінні кібербезпекою. Висвітлюватимуться різноманітні підходи до етичного управління в різних контекстах, регіонах та організаціях.

Третій розділ фокусувався на розгляді методів вирішення складних етичних ситуацій. Аналіз етичних принципів та стандартів в управлінні кібербезпекою дозволив визначити основні критерії для вирішення етичних конфліктів.

У четвертому розділі проведено детальне дослідження різних методів та підходів до визначення етичних критеріїв для оцінки дій та рішень в кібербезпеці. Кейси та сценарії вирішення етичних ситуацій допомогли порівняти ефективність різних методів.

Рекомендації щодо ефективного вирішення складних етичних ситуацій в кібербезпеці наступні: розробити чіткі етичні принципи та стандарти, якими керуватиметься організація в сфері кібербезпеки. Вони мають базуватися на загальнолюдських моральних цінностях та нормах. Регулярно проводити навчання та тренінги для персоналу з питань етики в кібербезпеці на основі практичних кейсів. Запровадити процедури внутрішнього аудиту та моніторингу дотримання етичних норм в діяльності з кібербезпеки. Налагодити консультації із зовнішніми експертами та громадські обговорення складних етичних питань. Регулярно оновлювати внутрішні політики з урахуванням змін у законодавстві, технологіях, суспільних нормах. У разі виникнення складної ситуації застосовувати алгоритм аналізу на основі етичних принципів та цінностей. Забезпечити прозорість та підзвітність діяльності з кібербезпеки шляхом регулярних звітів та інформування громадськості. Дотримання цих рекомендацій сприятиме прийняттю етично виважених рішень в складних ситуаціях кібербезпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Когут Ю.І. Корпоративна безпека: навч. посіб. Київ : Дакор, 2021. 460 с.

2. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології: навч. посіб. Київ : Сідкон , 2022. 284 с.

3. Гриценко Т.Б., Гриценко С.П., Іщенко Т.Д., Мельничук Т.Ф., Чуприк Н.В., Анохіна Л.П. Етика ділового спілкування: навч. посіб. Київ : Центр учбової літератури , 2021. 344 с.

4. Schneier, B. "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." 2015. 448c.

5. Clarke, R., & Knake, R. K. "Cyber War: The Next Threat to National Security and What to Do About It." 2010. 320c.

6. Brenner, J. "America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare." 2007. 320c.

7. Goodman, M. S. "Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It." 2019. 464c.

8. Greenberg, A. (2014). "This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information." 2014. 384c.

9. Стовпець В.Г., Стовпець О.В., Гловацька С.М. Корпоративна етика та психологія: навч. посіб. Київ : Олді , 2021. 236 с.

10. OWASP (Open Web Application Security Project). https://owasp.org/

11. ISO/IEC 27001:2013 (Information Security Management System - ISMS). https://www.iso.org/standard/54534.html

12. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

13. Schmidt, E., & Cohen, J. "The New Digital Age: Reshaping the Future of People, Nations, and Business." 2013. 336c.

14. Zetter, K. "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon." 2014. 448c.

15. Rid, T. "Cyber War Will Not Take Place." 2013. 218c.

16. Applegate, S. D. "Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions." 2019. 316c.

17. Бралатан В., Гуцаленко Л., Здирко Н. Професійна етика: навч. посіб. Київ : Центр учбової літератури , 2021. 252 с.

18. CIS Controls (Center for Internet Security). https://www.cisecurity.org/controls/

19. PCI DSS (Payment Card Industry Data Security Standard). https://www.pcisecuritystandards.org

20. Скоринський, В., Масленіков Ю. Кібербезпека для всіх: захисти себе від хакерів та мошенників: навч. посіб. 2018. 258с.

21. Шинкарук В. Кіберзлочини: монографія. 2018. 234с.

22. Грінберг, М. Кібербезпека: історії, поради, приклади навч. посіб. 2018. 304с.

23. Скоринський, В., Масленіков Ю. Кібербезпека для користувачів. практ.посіб 2017. 266с.

24. Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2015. 448с.

25. Попов, О. Кібербезпека: теорія та практика застосування: навч. посіб. Київ: КНУБА, 2018. 230с.

26. Іванюк, І. Кіберзахист: від теорії до практики: навч. посіб. Київ: АСК, 2019.246с.

27. Іванов В. Ф., Сердюк В. Є. Журналістська етика. 2007. 316 с.

28. Кононович В.Г. Математичні моделі процесів забезпечення соціальнопсихологічної кібербезпеки 2016. 286с.

29. Кононович В.Г., Кононович І.В., Романюков М.Г. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2016. 314с.

30. Кононович В. Г. Адаптивні підходи до забезпечення кібербезпеки розподілених систем Київ: НАУ, навч. посіб, 2016. 260с

31. Кононович В.Г., Стайкуца С.В., Кононович І.В., Копитін Ю.В., Безпека інформації. Київ: НАУ, навч. посіб, 2016. 260с

32. Smith J. The Digital Transformation of Public Administration: Balancing Innovation and Security. Public Administration Review, 2020. 466с.

33. Баранов О. А., Жиляєв І. Б., Демкова М. С., Малюкова І. Г. Електронне врядування в Україні: аналіз та рекомендації. Київ : Поліграф-Плюс, 2007. 254 с.

34. Кириченко М. Вплив цифрових технологій на розвиток людського і соціального капіталу. 2019. 263с.

35. Биков В.Ю. , Спірін О.М. , Пінчук О.П. Проблеми та завдання сучасного етапу інформатизації освіти: Інститут інформаційних технологій і засобів навчання НАПН України. 2017 URL: http://lib.iitta.gov.ua.

36. Burov O. Ju. Educational Networking: Human View to Cyber Defense. Інформаційні технології і засоби навчання. 2016. 156с.

37. Пінчук, О.П., Литвинова, С.Г., Буров О.Ю. Синтетичне навчальне середовище – крок до нової освіти. Інформаційні технології і засоби навчання. 2017.345с.

38. Veltman H., Wilson G., Burov O. Cognitive load. NATO Science Series RTOTR-HFM-104, Brussels, 2004. 186с.

39. Гібалова Н. Реалізація компетентнісного підходу в підготовці майбутніх фахівців електронного навчання. Суми: Суми, 2018. 238с.

40. Морзе Н. Підготовка менеджерів е-навчання: компетентнісний підхід. 2017. 424с.

41. Морзе Н., Глазунова О., Кузьмінська О. Інформаційні технології і засоби навчання 2017. 248с.

42. Овчарук О. В. Інформаційно-комунікаційна компетентність як предмет обговорення. 2013. 136с.

43. ITIL (Information Technology Infrastructure Library). https://www.axelos.com/best-practice-solutions/itil

44. Lukas G. Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare 2016. 208с.

45. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity 2020. 384с.

46. Buchanan B. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. 2017. 304с.

47. Pfeffer G. Cybersecurity Ethics: An Introduction. 2018. 254с.

48. Missisl D. Professionalizing Hackers: Computer Security as a Social Problem 2020. 274с.

49. Каленський А.А. Розвиток професійно-педагогічної етики у майбутніх викладачів спеціальних дисциплін. Київ: ЦП «Компринт», 2016. 424с.

50. Решетилов Г. О. Фінансування циркулярної економіки: європейський погляд, 2022, 186с.

51. Нахара М. Б. (2022). Бізнес-моделі циркулярної економіки, 2021. 166с.

52. Варченко О., Артимонова І., Герасименко І. Формування системи управління результатами ринкової діяльності. 2020. 174с.

53. Кузьмін О. Є., Мельник О. Г. Основи менеджменту. Київ: Академвидав, 2007. 464 с.

54. Захарчин Г. М., Андрійчук Ю. А. Планування інноваційної діяльності: альтернативи і етапи планування інноваційної діяльності. 2012. 152с.

55. Яценко О., Швиданенко О., Швиданенко Г. Циркулярна економіка як основа забезпечення сталого розвитку країни . 2022. 194с.

56. Квасній Л. Г., Попівняк О. М., Щербань О. Я. Стратегічне і тактичне планування діяльності підприємства. 2015. 154с.

57. Буров О. Ю., Камишин В. В., Поліхун Н. І., Ашеров А. Т. Технології використання мережевих ресурсів для підготовки молоді до дослідницької діяльності. Київ : ТОВ «Інформаційні системи». – 2012. – 416 с.

58. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. 2018. 282с.

59. Кількість кіберзлочинів в Україні зросла вдвічі за останні п’ять років - Opendatabot. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot

60. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. 2018. 186с.

61. Ткаченко О. Конфіденційність даних користувачів у сучасних месенджерах. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2019. 268с.

62. Карпенко Ю. В. Етичні принципи застосування штучного інтелекту в публічному управлінні. 2019. 296с.

63. Шраменко О. В., Савчук І. Н. Інфраструктурна безпека в епоху цифрової економіки. 2020. 284с.

64. Mitnick K. D. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Back Bay Books. 2012. 446с.