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: “ ПІДХОДИ ДО ПЛАНУВАННЯ І РЕАЛІЗАЦІЇ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ”

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

_____ Віталій ВАСИЛЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Віталій ВАСИЛЕНКО

Керівник:
к.т.н. Юрій ЯКИМЕНКО

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 Василенко Віталію Вікторовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: " Підходи до планування і реалізації заходів інформаційної безпеки на підприємстві "

керівник кваліфікаційної роботи Юрій ЯКИМЕНКО, к.т.н., доцент
(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: *управління інформаційною безпекою, планування інформаційної безпеки, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література*

4. Перелік питань, які потрібно розробити:
   1. Розглянути основи планування інформаційної безпеки на підприємстві.
   2. Сформувати методики планування заходів інформаційної безпеки на підприємстві.
   3. Провести дослідження і розробити рекомендації у реалізації підходів до планування інформаційної безпеки на підприємстві.

5. Перелік ілюстративного матеріалу: *презентація*

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

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	21.10.2023	
3.	Теоретичні основи планування інформаційної безпеки підприємства	25.10.2023	
4.	Проведення аналізу загальних принципів інформаційної безпеки та їхнього значення для підприємств	05.11.2023	
5.	Формування методики планування заходів інформаційної безпеки на підприємстві	10.11.2023	
6.	Практична реалізація заходів планування інформаційної безпеки	17.11.2023	
7.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	
8.	Оформлення роботи.	04.12.2023	
9.	Оформлення презентації.	14.12.2023	
10.	Отримання рецензії на роботу.	18.12.2023	
11.	Захист в ДЕК.	18.01.2024	

Здобувач вищої освіти _____ Віталій ВАСИЛЕНКО_
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО_
(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 Василенко В.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

Освітньо-професійної програми Управління інформаційною безпекою
(назва)

на тему: “ Підходи до планування і реалізації заходів інформаційної безпеки на підприємстві ”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ВАСИЛЕНКО Віталій** у кваліфікаційній роботі дослідив сучасний стан планування і реалізації заходів інформаційної безпеки на підприємстві. Запропонував нові підходи до планування та впровадження заходів інформаційної безпеки на підприємстві, які ґрунтуються на комплексному врахуванні організаційних, технічних заходів, розробив комплексні критерії і метрики для оцінювання ефективності реалізації заходів інформаційної безпеки. Удосконалив методику планування інформаційної безпеки конкретними етапами формування стратегії і застосуванням визначених метрик. Розроблені рекомендації керівникам підприємств та керівникам структурних підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки значно підвищать ефективність запланованих заходів інформаційної безпеки на підприємстві. **ВАСИЛЕНКО Віталій** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ВАСИЛЕНКА Віталія** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

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

“____“_____2024 року

Висновок кафедри про кваліфікаційну роботу

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

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Василенко Віталія Вікторовича
на тему " ПІДХОДИ ДО ПЛАНУВАННЯ І РЕАЛІЗАЦІЇ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ "

Актуальність

Сучасні технології створюють нові можливості для кіберзлочинців, які вони використовують для різноманітних кібератак. Інциденти інформаційної безпеки можуть призвести до серйозних втрат репутації підприємства. Тому питання управління інформаційною безпекою та планування заходів для її забезпечення є надзвичайно актуальним, як правильно визначено в даній роботі

Позитивні сторони

В магістерській роботі запропоновані нові підходи до планування та впровадження заходів інформаційної безпеки на підприємстві, які відрізняються від відомих комплексним врахуванням організаційних, технічних заходів та розробленими комплексними критеріями і метриками для оцінювання ефективності реалізації заходів інформаційної безпеки, що дозволяє якісно оцінювати та визначати успішність стратегій, вчасно виявляти можливі ризики.

Удосконалена методика планування інформаційної безпеки включає етапи формування стратегії, визначення метрик ефективності, розроблення плану заходів та систему моніторингу і оцінки. Розроблені рекомендації керівникам підприємств та керівникам структурних підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки значно підвищать ефективність запланованих заходів інформаційної безпеки на підприємстві.

Недоліки

У роботі також доцільно було б визначити заходи застосування штучного інтелекту при плануванні, але вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Василенко Віталій Вікторович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

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

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 стор., 12 рис., 2 табл., 66 джерел. 1 додаток.

Метою роботи є вивчення підходів до планування і реалізації заходів інформаційної безпеки на підприємстві.

Об'єктом дослідження є процеси планування і реалізації заходів інформаційної безпеки на підприємстві.

Предмет дослідження – підходи до планування і реалізації заходів інформаційної безпеки на підприємстві.

Методи дослідження. Для вирішення визначених наукових завдань в роботі при дослідженні способів планування використані аналіз, синтез, анкетування і опитування, моделювання, кейс-стаді, методи теорії управління.

Короткий зміст роботи. Здійснено аналіз наукової літератури та публікацій, пов'язаних із плануванням і реалізацією заходів інформаційної безпеки

У першому розділі були розглянуті ключові аспекти, що становлять теоретичну базу для ефективного планування інформаційної безпеки на підприємстві. Ретельне вивчення основних понять та принципів інформаційної безпеки виявило їхню важливість та взаємозв'язок із загальною стратегією організації. Аналіз моделей та методів планування виявив потребу у створенні ефективної методики планування з урахуванням міжнародних нормативно-правових документів та системного підходу до планування.

У другому розділі на основі вивчених підходів розроблена нова удосконалена методика планування інформаційної безпеки, яка передбачає системний аналіз потреб, ризиків та ресурсів підприємства. Вона включає етапи формування стратегії, визначення метрик ефективності, розроблення плану заходів та систему моніторингу та оцінки. Методика розглядає всі аспекти, від технічних аспектів до людського фактору, для забезпечення повноцінних інтегрованих заходів інформаційної безпеки. Вона покликана бути гнучкою та адаптивною, щоб враховувати зміни в кіберзагрозах, технологічних парадигмах

та стратегічних цілях підприємства.

У третьому розділі вперше сформований комплекс критеріїв і метрик оцінювання ефективності реалізації заходів інформаційної безпеки та ключові показники, які дозволяють якісно оцінювати та визначати успішність стратегій, вчасно виявляти можливі ризики інформаційної безпеки підприємства.

***Галузь застосування*.** Розроблені рекомендації керівникам підприємств та керівникам структурних підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки та ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ з урахуванням особливостей функціонування підприємства, що значно підвищать ефективність запланованих заходів інформаційної безпеки на підприємстві та будуть сприяти підвищенню культури безпеки серед персоналу і зменшенню внутрішніх загроз.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, ПЛАНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 68 pages, 12 figures, 2 tables, 66 sources, 1 appendix.

The purpose of the work is the study of approaches to planning and implementation of information security measures at the enterprise.

Object of research is processes of planning and implementation of information security measures at the enterprise.

Subject ***of research*** is approaches to planning and implementation of information security measures at the enterprise.

Research methods. Analysis, synthesis, questionnaires and surveys, modeling, case studies, methods of management theory were used to solve the identified scientific tasks in the study of planning methods.

Brief content of research. An analysis of scientific literature and publications related to the planning and implementation of information security measures was carried out

In the first chapter, the key aspects that constitute the theoretical basis for effective planning of information security at the enterprise were considered. A careful study of the main concepts and principles of information security revealed their importance and relationship with the overall strategy of the organization. The analysis of planning models and methods revealed the need to create an effective planning methodology taking into account international regulatory documents and a systematic approach to planning.

In the second chapter, based on the studied approaches, a new and improved method of planning information security is developed, which involves a systematic analysis of the needs, risks and resources of the enterprise. It includes the stages of strategy formation, determination of performance metrics, development of an action plan and a monitoring and evaluation system. The methodology considers all aspects, from technical aspects to the human factor, to ensure full-fledged integrated measures of information security. It is designed to be flexible and adaptive to take into account

changes in cyber threats, technological paradigms and strategic goals of the enterprise.

In the third section, for the first time, a set of criteria and metrics for evaluating the effectiveness of the implementation of information security measures and key indicators that allow qualitative assessment and determination of the success of strategies, timely detection of possible risks of information security of the enterprise is formed.

Field of research. Developed recommendations for heads of enterprises and heads of structural divisions of information security for the development of the Information Security Policy and PROVISIONS ON COMMERCIAL SECRETS, taking into account the peculiarities of the functioning of the enterprise, which will significantly increase the effectiveness of planned information security measures at the enterprise and will contribute to the improvement of the security culture among personnel and the reduction of internal threats.

KEYWORDS: INFORMATION SECURITY, INFORMATION SECURITY PLANNING, ENTERPRISE INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасні технології створюють нові можливості для кіберзлочинців, із якими пов'язані ризики для підприємств. Злочинці використовують різноманітні атаки, такі як фішинг, розкрадання даних, вторгнення в системи та інші, для отримання несанкціонованого доступу до конфіденційної інформації. Інциденти інформаційної безпеки можуть призвести до серйозних втрат репутації підприємства. Клієнти та партнери очікують, що їхні дані будуть безпечними, і будь-яке порушення може викликати недовіру і втрату бізнесу. Підприємства, які впроваджують інновації та цифрову трансформацію, стають більш залежними від інформаційних технологій. Це робить їх більш вразливими до кіберзагроз, і вимагає ефективних стратегій інформаційної безпеки. Тому багато країн встановлюють законодавчі вимоги щодо інформаційної безпеки та визначають штрафи за їхнє порушення. Виконання цих вимог стає необхідністю для уникнення правових проблем і фінансових втрат. Планування та реалізація заходів інформаційної безпеки на підприємстві стає необхідністю для збереження довіри зацікавлених сторін, уникнення фінансових втрат і відповідності законодавчим вимогам у світлі зростання загроз та швидкого розвитку технологій. У зв’язку із постійною зміною загроз планування та реалізація заходів інформаційної безпеки потребує постійного вдосконалення та наукових пошуків нових підходів

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

Об’єктом дослідження є процеси планування і реалізації заходів інформаційної безпеки на підприємстві.

Предмет дослідження – підходи до планування і реалізації заходів інформаційної безпеки на підприємстві.

Мета роботи полягає у вивчення підходів до планування і реалізації заходів інформаційної безпеки на підприємстві.

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

1. Розглянуті основи планування інформаційної безпеки на підприємстві.

2. Сформована методика планування заходів інформаційної безпеки на підприємстві.

3. Проведено дослідження і розроблені рекомендації для реалізації підходів до планування інформаційної безпеки на підприємстві.

Методи дослідження. При вирішенні визначених наукових завдань в роботі при дослідженні способів планування використані аналіз, синтез, моделювання, кейс-стаді, як метод активного проблемно-ситуаційного аналізу при створенні методики планування інформаційної безпеки, методи теорії управління: імперативний та диспозитивний - при формуванні рекомендацій для відпрацювання Положення та Політики безпеки.

Наукова новизна одержаних результатів.

1. В магістерській роботі вперше запропоновані нові підходи до планування та впровадження заходів інформаційної безпеки на підприємстві, які відрізняються від відомих комплексним врахуванням організаційних, технічних заходів та комплексом розроблених критеріїв і метрик для оцінювання ефективності реалізації заходів інформаційної безпеки, що дозволяє якісно оцінювати та визначати успішність стратегій, вчасно виявляти можливі ризики.

2. Удосконалена методика планування інформаційної безпеки, яка відрізняється від відомих тим, що передбачає системний аналіз потреб, ризиків та ресурсів підприємства та включає етапи формування стратегії, визначення метрик ефективності, розроблення плану заходів та систему моніторингу і оцінки.

3. Дістали подальшого розвитку способи процесу моніторингу ефективності реалізації заходів інформаційної безпеки із застосуванням визначених критеріїв і метрик.

Практичне значення одержаних результатів. Розроблені рекомендації керівникам підприємств та керівникам структурних підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки та ПОЛОЖЕННЯ

ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ з урахуванням особливостей функціонування підприємства, що значно підвищить ефективність запланованих заходів інформаційної безпеки на підприємстві та буде сприяти підвищенню культури безпеки серед персоналу і зменшенню внутрішніх загроз.

Апробація результатів кваліфікаційної роботи. Результати дослідження було оприлюднено на Всеукраїнській науково-практичної Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (м. Київ, 23 лютого 2023 року), яка проведена в Навчально-науковому інституті захисту інформації ДУІКТ.

.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПЛАНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Основні правові та регуляторні аспекти у плануванні інформаційної безпеки

Зростання використання цифрових технологій та перехід до електронного ведення бізнесу і комунікацій роблять інформаційну безпеку важливою для захисту великої кількості конфіденційної інформації, яка знаходиться в електронному вигляді.

Зловживання кіберзлочинців та загрози кібербезпеки стають все більш вдосконаленими та поширеними. Компанії та організації щодня стикаються з новими та еволюційними загрозами, що підкреслює важливість ефективних заходів інформаційної безпеки.

Збільшення обсягу особистих даних в Інтернеті та їхнє використання в різних контекстах (від онлайн-покупок до медичної інформації) робить захист цих даних важливим етичним та законодавчим завданням.

Зростання обов'язків та стандартів щодо захисту інформації, таких як Загальний регламент з захисту даних (англ. GDPR - General Data Protection Regulation) в Європі та інші подібні законодавчі акти в інших регіонах, створює обов'язок організаціям дотримуватися високих стандартів інформаційної безпеки. GDPR покликаний насамперед надати громадянам та резидентам Європейського Союзу (ЄС) контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС [1] .

Юридичні аспекти планування інформаційної безпеки включають закони, нормативні акти та політику, які наказують або забороняють певну поведінку.

У низці досліджень [2-3] здійснений розгляд міжнародної концепції інформаційної безпеки, що склалася на глобальному та регіональному рівнях,

аналіз правових інструментів її реалізації та вирішення проблем регулювання відносин у глобальному інформаційному суспільстві. Було розроблено комплекс загальнонаукових і філософських методів, що включає формально-логічний, порівняльно-правовий, формально-юридичний, системно-структурний і проблемно-теоретичний методи, а також методи аналізу й синтезу, узагальнення й опису, порівняння. використаний у дослідженні. У результаті дослідження встановлено, що на глобальному та регіональному рівнях склалася єдина концепція забезпечення міжнародної інформаційної безпеки, яка потребує правових інструментів для її реалізації на глобальному рівні. У розробці та прийнятті міжнародних договорів на глобальному рівні слід використовувати досвід Ради Європи щодо переслідування кіберзлочинців та захисту приватного життя. Отримані результати можуть бути використані в діяльності міжнародних організацій при виконанні ними функцій з уніфікації та гармонізації міжнародного права інформаційної безпеки та національними телекомунікаційними операторами у процесі виходу на міжнародні та зовнішні ринки.

Планування інформаційної безпеки є критично важливим аспектом діяльності будь-якої організації. Це передбачає розробку політики, процедур і вказівок для забезпечення конфіденційності, цілісності та доступності інформації. Юридичні та нормативні аспекти планування інформаційної безпеки мають важливе значення для забезпечення дотримання організаціями відповідних законів і правил.

Організації повинні мати чітке розуміння своїх зобов’язань у будь-який момент часу та бути готовими адаптувати свої практики інформаційної безпеки відповідно до своєї ролі відповідального обробника даних. Документом планування інформаційної безпеки є план, у якому задокументовано план та процедури захисту особистої інформації та конфіденційних даних компанії. Цей документ допомагає підприємству (організації) захистити цілісність, конфіденційність і доступність своїх даних, а також пом'якшити загрози. Він також надає контекст, конкретні інструкції для дій у надзвичайних ситуаціях,

разом із індивідуальними обов'язками та наслідками невідповідності, а також надає доступ або посилання на пов'язані або супровідні документи. Стратегічний план інформаційної безпеки може допомогти компанії мінімізувати, передати, прийняти або запобігти інформаційним ризикам, пов'язаним з людьми, процесами та технологіями. Успішний план інформаційної безпеки має значні економічні переваги та може забезпечити конкурентну перевагу. Дотримання галузевих стандартів, запобігання руйнівному інциденту безпеки, підтримка репутації компанії та дотримання зобов'язань перед акціонерами, клієнтами, партнерами та постачальниками – це лише кілька прикладів.

План інформаційної безпеки зазвичай включає обсяг заходів, класифікацію всієї інформації, що залучається, цілі управління в разі порушення безпеки.

Згідно зі статтею CSO Online, існує кілька законів, нормативних актів і вимог до відповідності, про які організації повинні знати, коли йдеться про планування інформаційної безпеки. Стаття містить вичерпний посібник із цих законів і нормативних актів, включаючи посилання на повний текст кожного закону чи нормативного акту.

Вітчизняні дослідження зосередженні на вдосконаленні нормативно-правових актів інформаційної безпеки, які призначені для забезпечення безпеки інформації підприємств України. Основні положення інформаційного забезпечення знаходяться у низці Законів України [4-8], що стосуються інформаційної та кібернетичної безпеки.

У дослідженні [9] встановлено, що нормативно-правова та доктринальна база інформаційної безпеки в Україні розвивалася симптоматично та хаотично. Багато в чому це пов’язано з тим, що сучасні методи дослідження базуються на різних світоглядних позиціях, по-різному вирішують дослідницькі проблеми, а також використовують відмінні дослідницькі стратегії.

Крім того, інформаційна безпека розглядалася насамперед як інформаційна безпека держави. У подальшому активізація процесів інформатизації в усіх сферах, особливо зростання значення технічного захисту інформації, призвела до формування правового забезпечення захисту інформації

як невід'ємної складової безпеки підприємств, установ і організацій, а також окремі галузі економіки.

На межі тисячоліть гостро постало питання міжнародної інформаційної безпеки, а також кібербезпеки як складової інформаційної безпеки.

Проаналізовано етапи становлення українського законодавства в інформаційній сфері загалом та інформаційної безпеки зокрема, і встановлено, що на кожному з цих етапів інформаційна безпека особи залишалася другорядною проблемою. Підвищення ефективності адміністративно-правового забезпечення інформаційної безпеки в Україні можливе шляхом реалізації комплексу правових заходів, які передбачають: чітке відображення в законодавстві та державних установах орієнтації на поєднання суспільних і приватних економічних інтересів в інформаційній сфері; постійне та послідовне використання всіх правозахисних механізмів і процедур для подолання конфліктів в інформаційній сфері; підвищення правового рівня свідомості та діяльності державних службовців, представників усіх гілок і рівнів влади, населення країни.

Кібератаки можуть призвести до серйозних економічних втрат для компаній через втрату даних, припинення роботи систем, порушення бізнес-процесів та погіршення репутації.

Значна частина операцій та обміну інформацією в сучасному бізнесі відбувається в цифровому форматі, що підкреслює необхідність ефективних засобів захисту цієї інформації. Актуальність інформаційної безпеки враховує не тільки технологічні та юридичні аспекти, але й економічні та етичні фактори. Інформаційна безпека стає важливою частиною стратегічного управління будь-якою організацією чи підприємством, допомагає забезпечити стійкість та відповідати сучасним викликам цифрового середовища.

Розвиток інформаційної структури підприємств тягне за собою неконтрольоване збільшення кількості інформаційних загроз і вразливостей інформаційних ресурсів. Тому актуальність планування і реалізації заходів інформаційної безпеки підприємств обумовлена сьогодні сучасним розвитком

інформаційних технологій, якими користуються кіберзлочинці та зростанням кількості кібератак. Запропонована методика планування заходів інформаційної безпеки підприємства допомагає забезпечити ефективність захисту від кіберзагроз, виконати регуляторні вимоги та зберігати конфіденційність даних [10].

Відомості, які є предметом зловживань кіберзлочинців і підлягають захисту від порушення конфіденційності, цілісності та доступності відповідно до вимог нормативно-правових актів, відносять до основних активів підприємств. Сукупність технічних і програмних засобів, призначених для виконання функцій з обробки інформації обмеженого поширення складає допоміжні активи. Тому перед кожним підприємством, як стверджують науковці [11], постає питання комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів інформаційно-комунікаційних систем та мереж підприємств.

1.2 Аналіз загальних принципів інформаційної безпеки та їхнє значення для підприємств

Розгляд теоретичних основ планування та реалізації заходів інформаційної безпеки підприємства необхідно починати із основних понять та принципів, визначених у нормативно-правових документах з інформаційної безпеки.

Під інформаційною безпекою розуміють стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації») [12].

Враховуючи застосування інформаційних технологій, під інформаційною

безпекою (англ. InfoSec) розуміють набір практик, спрямований на захист конфіденційних даних та інформації разом із пов'язаними з ними центрами обробки даних і хмарними програмами. Протоколи інформаційної безпеки призначені для блокування несанкціонованого доступу, використання, розкриття, порушення або видалення даних.

Інститут SANS (англ. SysAdmin, Audit, Network, and Security) пропонує дещо ширше визначення: *інформаційна безпека* – це процеси та методології, розроблені та впроваджені для захисту друкованої, електронної чи будь-якої іншої форми конфіденційної, приватної та конфіденційної інформації чи даних від несанкціонованого доступу, використання, неправильного використання, розкриття, знищення, зміни або порушення [13].

Як зазначено в Стратегії Національної безпеки України, Інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [14].

Інформаційна безпека підприємства - це система заходів, спрямованих на захист інформаційного середовища від стороннього втручання та дій із злим наміром. Її мета полягає в тому, щоб дані компанії, які їй належать, виявилися мінімально сприйнятливими до втручання з мінімальним завданням збитків з боку третіх осіб. Існує велика кількість визначення «інформаційна безпека підприємства».

Наприклад, в роботі [15] під інформаційною безпекою підприємства автор

визначив як суспільні відносини щодо створення і підтримки на належному рівні життєдіяльності інформаційної системи суб'єкта.

У дослідженнях [16-18] визначено, що інформаційна безпека підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів з планового досягнення стану захищеності інформаційного середовища організації господарської діяльності.

У дослідженні [19] науковець характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації (рис. 1.1).

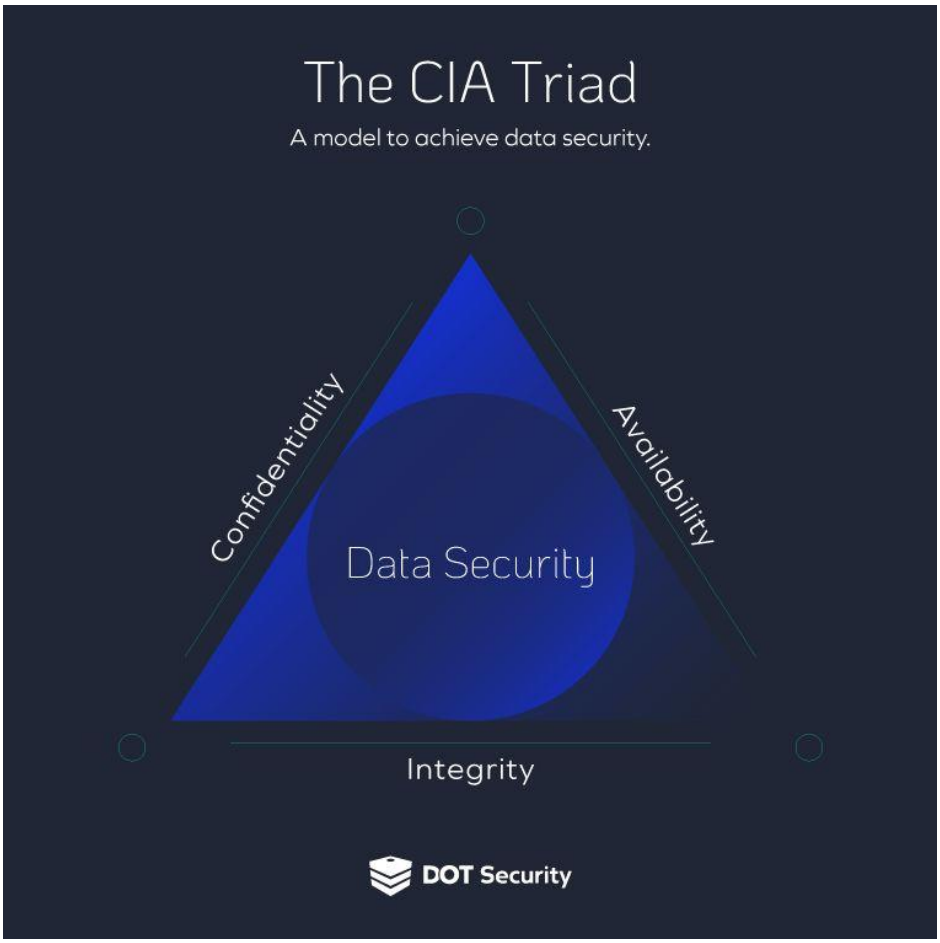

Рис.1.1. Тріада інформаційної безпеки

Під *конфіденційністю* (Confidentiality) розуміють стан, при якому інформація повинна бути захищена від несанкціонованого доступу, використання та розголошення. Конфіденційність даних означає, що дані мають

бути доступні лише тим, хто має авторизований доступ [20].

Сьогодні в умовах цифрової економіки інформація може складати основний актив бізнесу підприємства, за яким полюють конкуренти. Їх цікавить майже все: від розміру заробітної плати працівників до технології виробництва товарів і це буде складати комерційну таємницю для конкретного підприємства та є частиною політики конфіденційності. Тому дуже важливо спланувати заходи забезпечення інформаційної безпеки, направлені на попередження порушення конфіденційності. Одним із таких інструментів є розроблення та доведення до працівників ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ на підприємстві (додаток А).

Однак збереження конфіденційності даних означає, що співробітники мають доступ лише до тих даних, які їм абсолютно необхідні. Обмеження кількості людей, які мають доступ до різних наборів даних, покращує здатність вашої організації зберігати конфіденційну інформацію. Конфіденційність даних також є важливим фактором у стандартах управління ідентифікацією та доступом. Щоб досягти конфіденційності, підприємство може скористатися перевагами технології шифрування даних і впровадити багатофакторну автентифікацію (англ. MFA – Multi-Factor Authentication) (рис. 1.2).

Рис. 1.2. Структура багатофакторної автентифікації

Шифрування даних, як визначено у дослідженнях [21-23] - це процес «зашифровки» даних, щоб зробити їх нечитабельними, доки вони не будуть доставлені потрібній особі або користувачеві, після чого використовується ключ

розшифровки. MFA вимагає, щоб користувач підтверджував свою особу кількома методами, наприклад, за допомогою коду, доставленого на пристрій, або біометричних даних, як-от відбитків пальців.

Цілісність (Integrity, рис.1.1) означає, що інформація повинна бути захищена від несанкціонованого змінення і повинна бути цілісною, повною і точною. Наприклад, в дослідженнях [24-27] виявлені класифікаційні характеристики інформаційних ресурсів підприємства та взаємозв'язки між досконалістю системи управління та інформаційною системою і окреслено зовнішні та внутрішні інформаційні ресурси підприємства цілісність яких потрібно захищати. Щоб забезпечити цілісність даних, компанії можуть підтримувати та оптимізувати свою IT-інфраструктуру, створювати резервні копії даних і створювати план запобігання втраті даних, який захистить їх у разі серйозного витоку даних. Цілісність даних має вирішальне значення для співробітників, які використовують інформацію, отриману на основі цих даних у своєму повсякденному прийнятті рішень. У свою чергу, цілісність даних має вирішальне значення для підприємств, які прагнуть залишатися ефективними, вимірювати такі речі, як продуктивність, і хочуть отримати конкурентну перевагу. Якщо дані, що потребують захисту, пошкоджені, змінені без дозволу або іншим чином неточні, у підприємства не буде реального способу дізнатися, чи працює те, що робить ваш бізнес.

Доступність (Availability, рис. 1.1) означає, що інформація повинна бути доступна для користувачів, які мають на це право. Це означає, що мережа, система та необхідні пристрої готові до використання за призначенням уповноваженого персоналу [28-30]. По суті, доступність даних означає здатність співробітників отримати доступ до потрібних їм даних у будь-який момент без затримок. Є кілька факторів, які можуть перешкоджати доступу до даних навіть авторизованим користувачам, особливо в епоху хмарних технологій, коли так багато даних розміщується за межами офісу. Кібератаки, витоки даних і навіть нехтування стеками IT-технологій можуть призвести до затримок у доступі до даних або, що ще гірше, до простоїв у неробочому стані. Надаючи пріоритет

інформаційній безпеці як ключовому аспекту стратегії кібербезпеки, підприємство може значно покращити досвід співробітників і загальну безпеку вашої мережі.

Інформаційна безпека підприємства має кілька принципів, які визначені в дослідженнях [31-35]. Основні з них включають універсальність, надійність, постійність, модернізованість та комплексність (рис. 1.3).

Рис. 1.3 Принципи інформаційної безпеки підприємства

Універсальність передбачає, що заходи інформаційної безпеки повинні охоплювати всі аспекти діяльності підприємства, включаючи технічні, організаційні та людські ресурси. Це може включати захист інформаційних систем, процесів бізнесу, а також навчання та свідомість і медіаграмотність персоналу [33]. Універсальність також передбачає готовність заходів інформаційної безпеки адаптуватися до змін у діловому середовищі, технологічних інновацій, а також до нових видів кіберзагроз. Принцип універсальності покликаний вбудовувати заходи інформаційної безпеки в управлінські процеси підприємства. Це може означати включення аспектів безпеки в стратегічне планування, бюджетування та управлінські рішення. Універсальність передбачає включення всіх рівнів персоналу у заходи з безпеки, включаючи високий та низький рівні. Свідомий та відповідальний персонал є важливим елементом успішної стратегії інформаційної безпеки. Для забезпечення універсальності важливо використовувати стандарти та рамки безпеки, а також проводити регулярні аудити та перевірки для визначення ефективності заходів і їх відповідності стандартам. Принцип універсальності

допомагає забезпечити те, що інформаційна безпека вбудовується в основи підприємства, стає нероздільною частиною його культури та ефективно захищає його від різноманітних загроз [34].

Принцип *надійності* в інформаційній безпеці підприємства означає здатність систем, процесів та заходів забезпечити стабільну та неперервну роботу, а також виконання своїх функцій у будь-яких умовах та в обличчі різноманітних загроз [36]. Цей принцип, як визначають науковці [37-43], покликаний забезпечити доступність та стійкість інформаційних ресурсів підприємства. Надійність в контексті інформаційної безпеки означає, що інформаційні системи та дані повинні бути доступними для авторизованих користувачів у будь-який момент часу. Це важливо для підтримки нормальної діяльності підприємства та недопущення призупинення роботи через кібератаки, технічні несправності чи інші причини. Надійність також передбачає високий рівень стійкості до різних видів кіберзагроз, включаючи віруси, хакерські атаки, фішинг, DDoS-атаки та інші загрози, які можуть впливати на доступність інформації [22]. Забезпечення надійності також включає в себе використання резервних копій та планів відновлення для забезпечення можливості швидкої відновлення роботи підприємства в разі втрати даних або перебоїв у роботі систем.

Системи інформаційної безпеки повинні постійно моніторити та виявляти помилки, несправності чи несанкціоновану активність для забезпечення реагування та виправлення проблем до того, як вони стануть критичними. Підприємство повинно мати надійно побудовану інфраструктуру безпеки, включаючи застосування сучасних технологій, протоколів та стандартів для захисту від сучасних кіберзагроз. Використання сучасних інструментів штучного інтелекту та аналітики для виявлення аномальної поведінки та автоматичного реагування на потенційні загрози для забезпечення надійності. Принцип надійності в інформаційній безпеці є фундаментальним для підтримки бізнес-процесів та забезпечення стійкості організації у сучасному цифровому середовищі [42-43].

Принцип *постійності* в інформаційній безпеці підприємства означає, що заходи і стратегії безпеки повинні залишатися актуальними та ефективними протягом тривалого часу, незалежно від змін в оточуючому середовищі та технологічних інноваціях [44-46]. Цей принцип покликаний забезпечити сталість та довготривалість заходів інформаційної безпеки для забезпечення стійкості в умовах постійних змін та еволюції кіберзагроз. Організації повинні постійно вдосконалювати свої стратегії та заходи інформаційної безпеки, враховуючи нові загрози, технології та вимоги. Це включає в себе оновлення політик безпеки, впровадження нових заходів захисту та проведення регулярних аудитів безпеки. Процес стратегічного планування інформаційної безпеки з трьома ключовими рівнями (рис. 1.4) повинен враховувати довгострокові та короткострокові цілі підприємства, а також швидкі та повільні зміни в інформаційному середовищі [47-48].

Рис. 1.4. Рівні стратегічного планування

Регулярна оцінка ризиків дозволяє визначити нові потенційні загрози та визначити, які заходи безпеки потрібно прийняти для їхнього запобігання чи управління. Постійний розвиток та навчання персоналу у сфері інформаційної

безпеки важливі для того, щоб забезпечити їхню компетентність в обличчі постійно мінливих технологій та загроз.

Забезпечення постійності також передбачає використання сучасних технологій та інструментів, які відповідають сучасним стандартам і є ефективними у забезпеченні захисту інформації. Забезпечення постійності включає в себе готовність до реагування на кіберінциденти, шляхом розробки та вдосконалення планів відновлення та відновлення.

Постійний моніторинг та врахування змін в законодавстві та регуляторних вимогах є важливим для забезпечення відповідності та безпеки інформаційних процесів підприємства. Принцип постійності в інформаційній безпеці дозволяє підприємствам зберігати ефективний рівень захисту та готовності до реагування на виклики, які представляють нові технології та кіберзагрози.

Принцип *модернізованості* в інформаційній безпеці підприємства вказує на необхідність постійного вдосконалення технологій, процесів та стратегій інформаційної безпеки для реагування на сучасні кіберзагрози та мінливі вимоги бізнес-середовища [49].

Більшість науковців [50-51] відзначають, що цей принцип покликаний забезпечити ефективний захист інформаційних ресурсів підприємства в умовах мінливого технологічного та кібербезпечного ландшафту. Підприємство повинно використовувати найсучасніші технології та інструменти для захисту від кіберзагроз. Це може включати в себе використання штучного інтелекту, аналітики поведінки, машинного навчання та інших передових технологій [52].

Підприємство повинно постійно аналізувати нові кіберзагрози та розробляти стратегії захисту, враховуючи нові методи атак та ризики, які можуть виникнути внаслідок розвитку технологій. Заходи безпеки та політики повинні регулярно оновлюватися, враховуючи зміни в законодавстві, вимогах стандартів безпеки та специфічних внутрішніх потребах підприємства. Принцип модернізованості також охоплює важливість впровадження сучасних підходів до культури безпеки в організації, включаючи постійне навчання персоналу та підтримку усвідомленості щодо кіберзагроз.

Системи безпеки повинні бути гнучкими та адаптованими до змін в інфраструктурі підприємства, робочих процесах та технологічному стеку. Інтеграція принципів безпеки в розробку та впровадження програмного забезпечення забезпечує постійне вдосконалення заходів безпеки протягом всього циклу розробки. Важливо регулярно проводити тестування систем та мереж, а також аудити безпеки для виявлення слабких місць та можливих вразливостей.

Принцип модернізованості дозволяє підприємствам залишатися вперед у кіберпросторі та ефективно захищати свої інформаційні ресурси в умовах швидкого технологічного розвитку та зростання кіберзагроз [53-55].

Принцип *комплексності* в інформаційній безпеці підприємства означає необхідність розглядати заходи та стратегії безпеки як єдину інтегровану систему, яка охоплює всі аспекти діяльності організації [46, 56-58]. Цей принцип визнає, що ефективна інформаційна безпека вимагає комплексного підходу, який враховує технічні, організаційні та людські аспекти. Комплексний підхід передбачає інтеграцію технічних засобів безпеки (наприклад, антивірусного програмного забезпечення, файрволів) з організаційними заходами (наприклад, політиками безпеки, процедурами контролю доступу) для створення єдиної системи захисту.

Підприємство повинно враховувати людський фактор у своїй стратегії безпеки, забезпечуючи навчання та підвищення свідомості персоналу щодо кіберзагроз та етичного використання інформації. Комплексний підхід включає ефективне управління ризиками, враховуючи як технічні вразливості, так і організаційні аспекти, що можуть впливати на інформаційну безпеку. Комплексна система безпеки передбачає наявність системи моніторингу та виявлення інцидентів, яка охоплює як технічні, так і організаційні аспекти. Ефективний підхід включає синергію між різними заходами безпеки, забезпечуючи, щоб вони взаємодіяли між собою для створення більш ефективної системи захисту. Комплексний підхід вимагає включення інформаційної безпеки в стратегічне планування підприємства, забезпечуючи відповідність стратегії

безпеки загальним бізнес-цілям.

Організація повинна взаємодіяти з екосистемою безпеки, включаючи партнерів, постачальників та стандартизаційні організації, для створення єдиної та взаємодіючої системи безпеки. Комплексний підхід передбачає систематичний аналіз ефективності заходів безпеки та постійне вдосконалення стратегій відповідно до змін у середовищі.

Перераховані принципи, яких потрібно дотримуватись, надзвичайно важливі для створення надійної та ефективної системи інформаційної безпеки, яка враховує всі аспекти діяльності підприємства та взаємодіє з різноманітними чинниками.

Існує кілька моделей інформаційної безпеки підприємства, які можуть бути використані для створення ефективної стратегії безпеки. Основні моделі перераховані на рисунку 1.5.

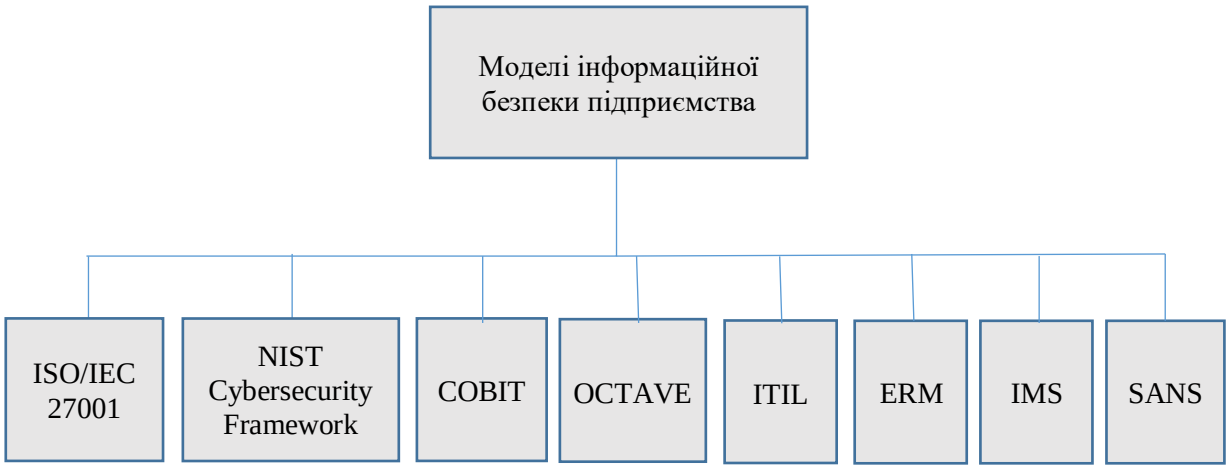

Рис.1.5. Перелік основних моделей планування інформаційної безпеки

Модель ISO/IEC 27001 [59] є міжнародним стандартом для управління інформаційною безпекою. Вона надає систематичний підхід до впровадження, утримання та постійного вдосконалення системи управління інформаційною безпекою. Стандарт визначає вимоги до встановлення, реалізації, експлуатації, моніторингу, перегляду, підтримки та покращення системи управління інформаційною безпекою в контексті організації.

Сімейство стандартів ISO/IEC, опубліковане в рамках спільного

підкомітету ISO/IEC, окреслює сотні механізмів контролю, які допомагають організаціям усіх типів і розмірів забезпечувати безпеку інформаційних активів. Ці глобальні стандарти забезпечують основу для політик і процедур, які включають усі юридичні, фізичні та технічні засоби контролю, пов'язані з процесами управління інформаційними ризиками організації. ISO/IEC 27001 – це стандарт безпеки, який офіційно визначає систему управління інформаційною безпекою (СУІБ), яка призначена для підпорядкування інформаційної безпеки під чіткий контроль керівництва. Як формальна специфікація, вона встановлює вимоги, які визначають, як впроваджувати, контролювати, підтримувати та постійно вдосконалювати СУІБ. Він також передбачає набір найкращих практик, які включають вимоги до документації, розподіл відповідальності, доступність, контроль доступу, безпеку, аудит, а також коригувальні та профілактичні заходи. Сертифікація за стандартом ISO/IEC 27001 допомагає організаціям дотримуватися численних нормативних і правових вимог, пов'язаних із безпекою інформації.

NIST Cybersecurity Framework – як модель кібербезпеки, Національний інститут стандартів і технологій (NIST) США пропонує широкий підхід до планування заходів кібербезпеки, включаючи такі компоненти як ідентифікація, захист, виявлення, відповідь та відновлення. Ця рамка може бути використана для розробки стратегій та планів інформаційної безпеки [60].

COBIT (Control Objectives for Information and Related Technologies) - це набір практичних інструментів для управління та контролю інформаційними технологіями. Він надає рекомендації з управління, моніторингу та оцінювання інформаційної безпеки та інших аспектів управління IT [61]. COBIT є структурою, яка має на меті допомогти організаціям, які прагнуть розробляти, впроваджувати, контролювати та покращувати управління IT та управління інформацією. COBIT була заснована ISACA, що розшифровується як Information Systems Audit and Control Association. Його публікують як ISACA, так і Інститут управління IT (ITGI). Остання версія COBIT ґрунтується на п'яти принципах:

1. Задоволення потреб ключових стейкхолдерів.

2. Наскрізне і всебічне охоплення всього підприємства.

3. Інтеграція декількох фреймворків в один уніфікований фреймворк.

4. Звільнення місця для цілісного підходу до ведення бізнесу.

5. Відокремлення управління від підпорядкування.

ITIL (англ. Information Technology Infrastructure Library - Бібліотека інфраструктури інформаційних технологій) - це рамка управління послугами, яка включає в себе набір процесів і практик для управління IT-службами. Вона включає аспекти безпеки, такі як управління інцидентами, управління змінами та управління конфігурацією [62]. Однією з головних цілей ITIL є забезпечення відповідності IT-послуг бізнес-цілям, навіть якщо бізнес-цілі змінюються. Однією з найважливіших частин ITIL є база даних керування конфігурацією (CMDB), яка забезпечує центральні повноваження для всіх компонентів, включаючи служби, програмне забезпечення, IT-компоненти, документи, користувачів та обладнання, якими необхідно керувати для надання IT-послуги. CMDB відстежує місцезнаходження та зміни всіх цих активів і процесів, а також їхні атрибути та зв'язки один з одним. Дотримання принципів ITIL допомагає гарантувати, що підприємство зможе якомога швидше дістатися до першопричини проблем у своєму інформаційному середовищі та мати правильну видимість систем і людей, щоб запобігти майбутнім проблемам.

SANS Institute's Critical Security Controls - ця модель визначає 20 критичних безпекових контролів, які повинні бути реалізовані для покращення безпеки інформації на підприємстві. Вона допомагає ідентифікувати та зменшити ризики, пов'язані з використанням технологій [63].

Розроблена Software Engineering Institute, методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) допомагає організаціям оцінити, ідентифікувати та управляти ризиками інформаційної безпеки. Вона акцентує увагу на розумінні конкретних ризиків та потреб організації [64]. Це структура, яка використовується для оцінки середовища організації та визначення IT-ризиків. Оскільки OCTAVE є гнучкою, її можна адаптувати до потреб практично будь-якої організації, залучаючи лише невелику

команду професіоналів з кібербезпеки, IT та операцій для спільної роботи над завданням. Застосовуючи фреймворк OCTAVE до бізнесу, важливо знати, що стандартна модель не завжди підходить організації. Таким чином, було розроблено кілька варіацій, включаючи OCTAVE-S (використовується, коли вся команда вже має великі знання про середовище організації), OCTAVE Allegro (яка простіша і більш підходить для невеликих команд) і OCTAVE Forte (найбільш адаптивна варіація). Кожне підприємство може розробити гібридний підхід, щоб знайти те, що найкраще підходить для його бізнесу. Впровадження моделі загроз OCTAVE вимагає сотень сторінок для ретельного пояснення і ще більше для заглиблення в складнощі адаптації та застосування фреймворку в будь-якій організації..

Крім того, багато підприємств використовують інтегровані системи управління, такі як Enterprise Risk Management (ERM) або Integrated Management Systems (IMS), які включають аспекти інформаційної безпеки в загальний управлінський підхід.

Загальний порівняльний аналіз визначений в табл. 1.1.

Таблиця 1.1

Порівняння моделей інформаційної безпеки

Модель	**Організація, які створила**	**Фокус**	**Аудит та сертифікація**
ISO/IEC 27001	Міжнародна організація зі стандартизації (International Organization for Standardization/International Electrotechnical Commission)	Зорієнтований на створення та управління системами управління інформаційною безпекою (ISMS)	Можливість отримання сертифікації згідно з ISO/IEC 27001 за допомогою зовнішнього аудиту
NIST Cybersecurity Framework	National Institute of Standards and Technology (NIST) в США	Пропонує підходи до ідентифікації, захисту, виявлення, відповіді та відновлення	Стандарт не передбачає аудит та сертифікацію, але може бути використаний як основа для розробки власних безпечних практик

Продовження таблиці 1.1

Модель	Організація, які створила	Фокус	Аудит та сертифікація
COBIT (Control Objectives for Information and Related Technologies)	Information Systems Audit and Control Association (ISACA)	Визначає контрольні об'єктиви для забезпечення ефективного управління IT-ресурсами	COBIT маю власний процес сертифікації COBIT-5, також може бути використаний як керівництво для інших стандартів
ITIL (Information Technology Infrastructure Library)	Офіс кабінету з технологій та процесів Великої Британії (Office of Government Commerce, UK)	Забезпечує рамки для управління інфраструктурою технологій інформаційної системи	ITIL має кілька рівнів сертифікації; зазвичай використовується як набір рекомендацій та кращих практик
SANS Institute's Critical Security Controls	SANS Institute	Фокусується на реалізації конкретних контрольних заходів для підвищення безпеки	Не передбачає процесу аудиту та сертифікації; використовується як набір безпечних практик
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	CERT Coordination Center (CERT/CC) в Карнегі-Меллонському університеті	Спрямований на оцінку загроз, активів і вразливостей для розробки стратегій забезпечення безпеки	Не передбачає процесу аудиту та сертифікації
Enterprise Risk Management (ERM)	Існує кілька фреймворків для ERM, таких як COSO ERM та ISO 31000	ERM спрямований на ідентифікацію, оцінку, управління та моніторинг ризиків, що можуть впливати на досягнення стратегічних цілей підприємства	COSO ERM та ISO 31000 не передбачають процесу сертифікації, але можуть використовуватися як настанови для внутрішнього аудиту та оцінки ризиків

Продовження таблиці 1.1

Модель	Організація, які створила	Фокус	Аудит та сертифікація
Integrated Management Systems (IMS)	Немає одного стандарту для IMS. Організації можуть обрати використання декількох стандартів, таких як ISO 9001, ISO 14001, ISO 45001, тощо	IMS об'єднує різні системи управління (наприклад, якість, середовище, охорона праці) в одну, забезпечуючи інтегрований підхід до управління бізнес-процесами та стандартами	Зазвичай використовується процес сертифікації за окремими стандартами, наприклад, ISO 9001 для системи управління якістю

Вибір конкретної моделі чи методу залежить від потреб, розміру та специфіки підприємства, його галузі діяльності та регуляторних вимог. Багато організацій комбінують різні підходи для досягнення комплексного та ефективного планування інформаційної безпеки.

Висновки до першого розділу. У даному розділі були розглянуті ключові аспекти, що становлять теоретичну базу для ефективного планування інформаційної безпеки на підприємстві. Ретельне вивчення основних понять та принципів інформаційної безпеки виявило їхню важливість та взаємозв'язок із загальною стратегією організації.

Поняття та принципи інформаційної безпеки є фундаментальними складовими будь-якої стратегії захисту інформації. Ключові поняття, такі як конфіденційність, цілісність та доступність, є основоположними для визначення цілей та завдань в області інформаційної безпеки.

Принципи інформаційної безпеки, такі як принцип надійності, універсальності та постійності, стають основою для розроблення конкретних стратегій та тактик у сфері інформаційної безпеки підприємства. Вони сприяють створенню системи, яка не лише відповідає поточним вимогам, але й готова до викликів майбутнього.

Вивчення моделей інформаційної безпеки підтверджує важливість системного підходу до планування та реалізації заходів інформаційної безпеки.

Регуляторне середовище визначає рамки та обмеження для планування та реалізації заходів інформаційної безпеки. Врахування правових вимог та стандартів, таких як GDPR чи ISO/IEC 27001, є необхідним елементом стратегії інформаційної безпеки.

Врахування цих аспектів у плануванні створює правову стійкість та допомагає уникнути можливих штрафів чи інших негативних наслідків. Крім того, вони можуть служити основою для розвитку етичних стандартів у галузі обробки інформації.

Загалом, теоретичні основи планування інформаційної безпеки на підприємстві визначають стратегічний курс дій та надають необхідний фундамент для практичної реалізації заходів забезпечення безпеки інформації. Вони є основою для розроблення конкретних планів, спрямованих на досягнення високого рівня інформаційної безпеки та відповідності вимогам сучасного бізнес-середовища.

Інформаційна безпека важлива для підприємства, оскільки її основним призначенням є захист найбільш конфіденційних даних, які вони зберігають.

Для багатьох організацій побудова надійної архітектури інформаційної безпеки повинна бути на першому місці щоб допомогти захистити критично важливі IT-активи від загроз безпеці з меншою кількістю зусиль і турбот.

Витрати на безпеку та управління інформаційною безпекою стрімко зростають у всьому світі. Тому перед керівниками підприємств постає питання на яких саме покращеннях слід зосередитися, щоб найкраще зміцнити свою програму інформаційної безпеки.

Організації повинні включати обізнаність співробітників про кібербезпеку як частину своїх ініціатив з інформаційної безпеки та загальної стратегії кібербезпеки. Якщо співробітники зрозуміють цілі нових технологій і протоколів безпеки, це допоможе їм дотримуватися цих процедур, які захищають дані та формують мислення, орієнтоване на безпеку.

Для сучасного бізнесу дуже важливо розуміти роль інформаційної безпеки, її складові та які стандарти та нормативно-правові акти повинні бути запроваджені, щоб позиціонувати себе для ефективної безпеки даних.

РОЗДІЛ 2
ФОРМУВАННЯ МЕТОДИКИ ПЛАНУВАННЯ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Підходи до планування і реалізації заходів інформаційної безпеки на підприємстві

Розглянуті у першому розділі (табл. 1.1) моделі інформаційної безпеки дозволяють їх застосовувати при плануванні захисту інформації на кожному підприємстві, де потрібно захищати інформацію з обмеженим доступом.

Інформаційна та кібербезпека має вирішальне значення для підприємств будь-якого типу та розміру. В одному опитуванні більше половини учасників назвали кібербезпеку головною проблемою для своєї організації. Компрометація даних і мережі може мати руйнівні наслідки, від яких багато компаній ніколи повністю не оговтаються. У 2019 році кібератаки коштували окремим підприємствам у середньому 200 000 доларів.

Для того, щоб визначити безпеку даних підприємства від потенційних порушень та кібератак, важливим етапом є впровадження моделі безпеки. З метою забезпечення цілісності модель безпеки може бути спроектована за допомогою кількох підходів:

1. Підхід «*знизу-вгору*» (рис.2.1): модель безпеки підприємства застосовується системними адміністраторами або людьми, які працюють у сфері мережевої безпеки або кіберінженерами. Основна ідея цього підходу полягає в тому, щоб люди, які працюють у цій галузі інформаційних систем, використовували свої знання та досвід у сфері кібербезпеки для гарантування розробки високозахищеної моделі інформаційної безпеки.

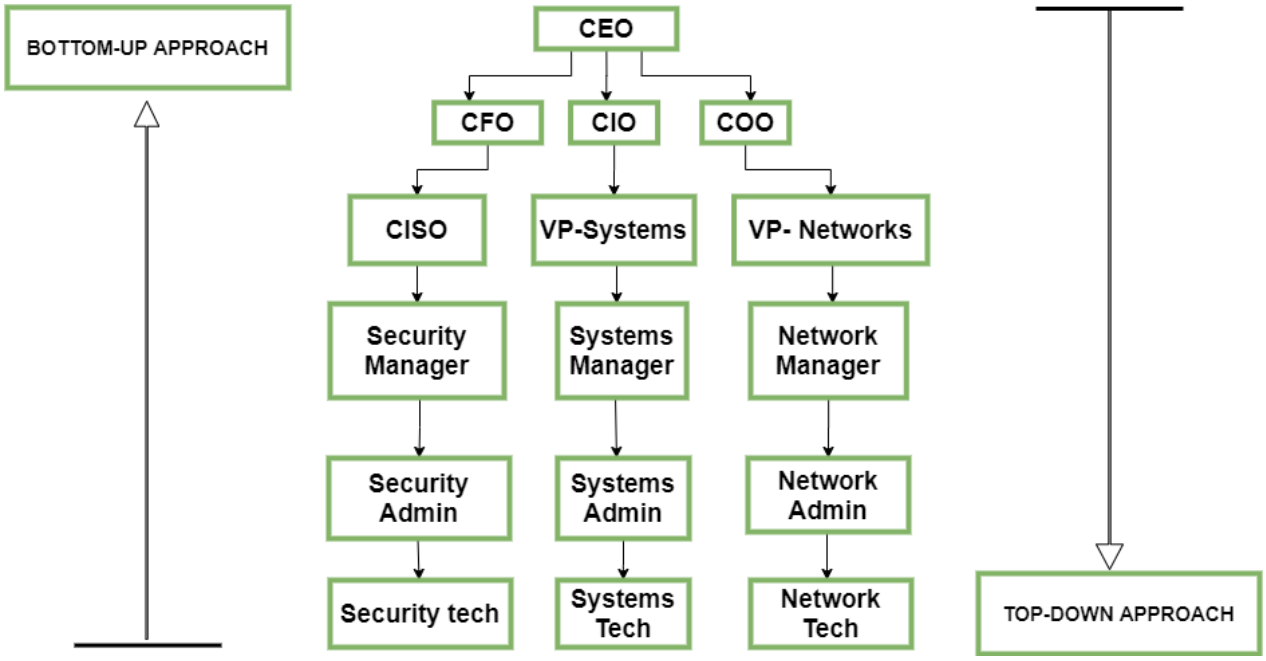

Рис. 2.1 Підходи до плануванні і організації інформаційної безпеки

Основні переваги – технічний досвід людини у своїй галузі гарантує, що кожна вразливість системи буде усунена, а модель безпеки зможе протистояти будь-яким потенційним загрозам.

Недолік – у зв'язку з відсутністю співпраці між вищими керівниками та відповідними директивами, вона часто не відповідає вимогам та стратегіям організації. Найбільшим недоліком - і причиною, через яку багато галузевих експертів рекомендують уникати цього підходу - є те, що він не передбачає допомоги чи внеску з боку керівництва вищого рівня. Через це програма інформаційної безпеки не матиме такої ж довговічності та ретельності, якби застосувати підхід «*зверху-вниз*».

2. Підхід «*зверху-вниз*» (рис.2.1): цей тип підходу ініціалізується та ініціюється керівниками організації. Вони формулюють політику та окреслюють процедури, яких слід дотримуватися.

Цей підхід розглядає дані кожного відділу та досліджує, як вони пов'язані для пошуку вразливостей. Менеджери мають повноваження видавати інструкції для всієї компанії, дозволяючи кожній людині відігравати невід'ємну роль у збереженні даних. Переваги та недоліки впровадження «зверху-вниз»:

- у порівнянні з окремою особою або відділом, підхід, заснований на управлінні, включає в себе більше доступних ресурсів і більш чіткий огляд активів і проблем компанії;

- підхід «зверху-вниз», як правило, має більш тривалу силу та ефективність, ніж підхід «знизу-вгору», оскільки він робить захист даних пріоритетом для всієї компанії, а не покладає всю відповідальність на одну людину чи команду. Уразливості даних існують у всіх офісах і відділах, і кожна ситуація унікальна.

Питання управління безпекою вирішуються організаціями різними способами. Традиційно компанії застосовують підхід «знизу-вгору», коли процес ініціюється операційними співробітниками, а їхні результати згодом поширюються на вище керівництво відповідно до запропонованої політики. Оскільки керівництво не має інформації про загрозу, наслідки, уявлення про ресурси, можливу віддачу та метод безпеки, такий підхід іноді призводить до раптового та насильницького колапсу. Навпаки, підхід «зверху-вниз» є дуже успішним зворотним поглядом на всю проблему. Керівництво розуміє всю серйозність і запускає процес, який згодом систематично збирається з кіберінженерів та експлуатаційного персоналу.

Єдиний спосіб для того, щоб програма інформаційної безпеки працювала - це довести до кожного керівника, філію, відділ і співробітника план для всієї компанії.

3. Впровадження *багаторівневого підходу* до інформаційної безпеки.

Оскільки єдина система безпеки часто не може гарантувати безпеку від витоку даних, багаторівневий підхід до безпеки став основною вимогою Підхід багаторівневої безпеки (MLS) має вирішальне значення в організаціях, які піклуються про конфіденційність, приділяючи першочергову увагу безпеці даних. Це забезпечує безперешкодну співпрацю, зберігаючи при цьому найвищий рівень безпеки. Роблячи безпеку даних герметичною, цей підхід також обмежує доступ до інформації для певної особи або групи. Дві основні цілі

багаторівневої безпеки полягають у наступному: запобігання несанкціонованому доступу до інформації; стримувати осіб від розсекречення інформації.

Атаки бувають різних форм, таких як фішингове шахрайство, хакерство, несанкціонований доступ до фізичних місць, троянські віруси, програми-вимагачі та атаки на паролі. Оскільки існує дуже багато можливих вразливостей, багаторівневий підхід є найкращим методом для впровадження повного захисту в різних відділах.

Багаторівневість Infosec враховує всі стандартні засоби захисту даних, а також інші аспекти кібербезпеки, включаючи веб-безпеку, мережу, пристрій, додатки, програмне забезпечення та фізичну безпеку. Він також включає наявність плану аварійного відновлення та резервного копіювання даних. Багаторівневий захист розбиває більші проблеми безпеки на менші, більш керовані частини. Він дозволяє налаштувати тип і рівень захисту залежно від конкретних потреб, таких як відділ, пристрій або збережені дані. Багаторівневі підходи переплітаються разом, тому кожна область інформаційної безпеки покладається на іншу, створюючи більш міцну та захисну ковдру захисту, яка ускладнює доступ зовнішніх зловмисників.

Управління безпекою інформаційних систем в організаціях ускладнюється явною відсутністю включення цілей організаційної безпеки в традиційний процес стратегічного планування. Для того, щоб удосконалити стратегічне планування безпеки інформаційної безпеки, дослідники вважають, що необхідно знову приділити увагу цілям планування безпеки [65].

2.2 Визначення методики планування інформаційної безпеки

Спосіб планування інформаційної безпеки підприємства є найважливішим аспектом його діяльності. Він передбачає розробку комплексного плану, який окреслює вимоги безпеки для інформаційної системи, описує засоби контролю безпеки, які були вибрані, і представляє обґрунтування категоризації безпеки, як

реалізуються засоби контролю та як можна обмежити використання систем у високих умовах. ризикові ситуації.

Процес розробки плану інформаційної безпеки включає кілька етапів, включаючи оцінку та планування ризиків, моделювання архітектури безпеки та опис поточних послуг IT-безпеки та методів контролю (рис. 2.2).

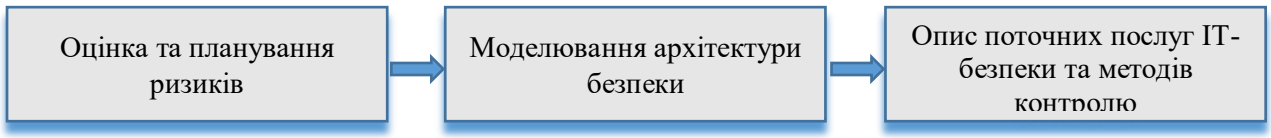

Рис. 2.2. Основні етапи розробки плану інформаційної безпеки підприємства

Наприклад, університет штату Айова має комплексну програму інформаційної безпеки, яка забезпечує адміністративні, операційні та технічні гарантії безпеки, які повинні бути реалізовані в інформаційних системах, залучених до обробки та зберігання конфіденційної або приватної інформації. Програма використовує практику «глибокого захисту», що забезпечує кілька різних рівнів захисту, кожен з яких сприяє загальному захисту інформаційних активів:

- цілісність інформації та контроль доступу;
- логіка програми, перевірка помилок і перевірка даних;
- логічний і фізичний захист на основі серверів і клієнтів;
- захист на внутрішньому та периметральному рівнях мережі;
- політика, практика та процедури для співробітників.

Відповідальність за управління Програмою інформаційної безпеки університету описана в Політиці безпеки. Цей опис програми буде щорічно переглядатися та оновлюватися за необхідності головним спеціалістом з інформаційної безпеки університету.

Планування інформаційної безпеки є важливим аспектом діяльності будь-якої організації. За своєю суттю план інформаційної безпеки - це набір політик і процедур, які регулюють те, як обробляється інформація на підприємстві. Політика може варіюватися від пом'якшених, загальних вказівок до суворо

виконуваної політики, необхідної для високих рівнів регулювання стосовно інформації з обмеженим доступом (конфіденційної, комерційної таємниці). Фактори, які слід враховувати в рамках такого плану, включають заходи безпеки для особистої ідентифікаційної інформації і те, як підприємство планує реагувати на інциденти порушення. Для багатьох вони є необхідною частиною демонстрації відповідності галузевим нормам і корисним для загального успіху вашої організації.

План інформаційної безпеки в кінцевому підсумку приносить користь організації, допомагаючи запобігти викриттю, втраті або пошкодженню даних. Фірми також можуть отримати вигоду від репутаційних переваг за рахунок уникнення негативного впливу на витік даних, а також економічної вигоди від уникнення штрафів і судових розглядів через недотримання вимог.

Планування передбачає розробку та впровадження стратегій для захисту конфіденційності, цілісності та доступності інформаційних систем. Деякі з методів, які використовуються в плануванні інформаційної безпеки, включають (рис. 2.3):

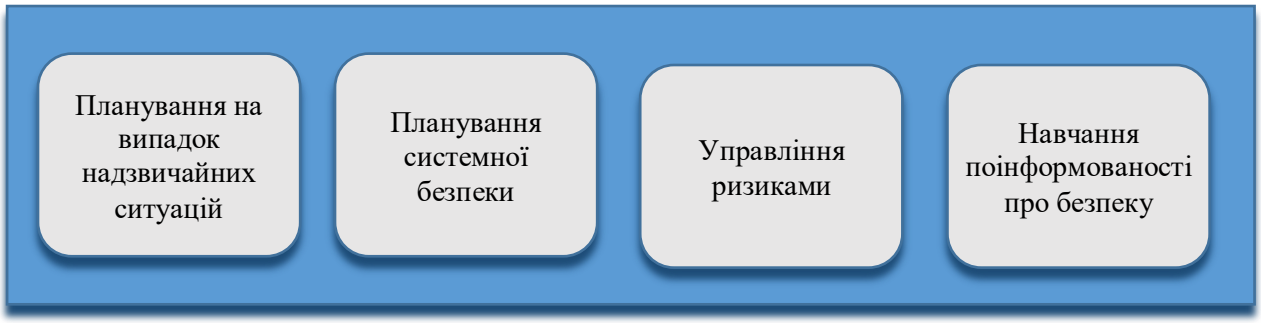

Рис. 2.3. Основні методи плануванні інформаційної безпеки підприємства

Планування на випадок надзвичайних ситуацій передбачає створення плану, який гарантує відновлення критично важливих систем і даних у разі збою або аварії. План має включати інформацію про апаратне та програмне забезпечення системи, програми та резервне копіювання даних, залежні процеси, інтерфейси даних, персонал служби підтримки та постачальників, пріоритети

відновлення та план обслуговування.

Планування системної безпеки передбачає розробку плану захисту конфіденційності, цілісності та доступності інформаційних систем. План має містити інформацію про вимоги безпеки системи, засоби контролю безпеки та тестування безпеки.

Управління ризиками передбачає ідентифікацію, оцінку та пом'якшення ризиків для інформаційних систем. Процес включає визначення активів, загроз, уразливостей і впливів, а потім вибір і впровадження відповідних засобів контролю для зменшення ризику.

Навчання поінформованості про безпеку передбачає навчання співробітників ризикам інформаційної безпеки та найкращим практикам. Навчання має охоплювати такі теми, як керування паролями, фішинг, соціальна інженерія та фізична безпека.

Це лише деякі з методів, які використовуються для планування інформаційної безпеки. Кожна організація повинна розробити план, адаптований до її конкретних потреб і ризиків.

Більшість планів інформаційної безпеки стосуються цих трьох компонентів (рис.2.4):

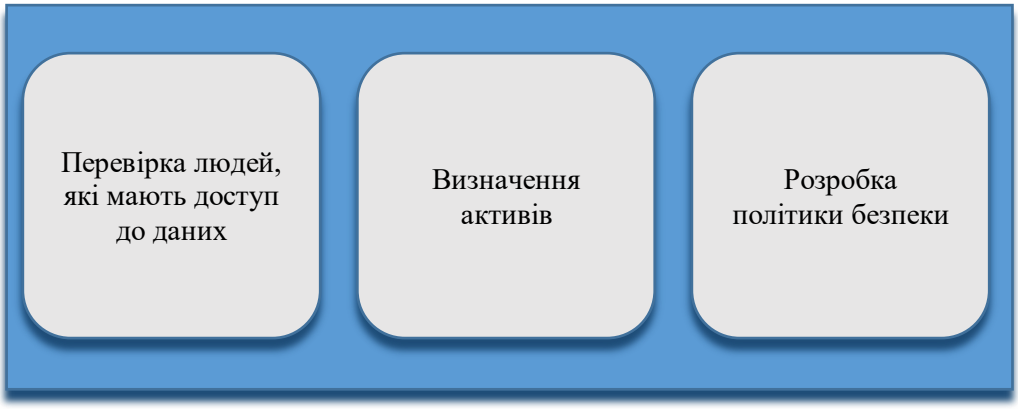

Рис 2.4. Компоненти планування інформаційної безпеки підприємства

Перевірка людей, які мають доступ до даних фірми, зменшує ризик того, що вони використовуватимуть їх зловмисно або несвідомо створюватимуть

проблеми. Шукайте попередні проблеми з безпекою та попередні записи під час процесу найму.

Визначення активів потрібно, щоб точно визначити ризики безпеки, пов'язані з корпоративними даними, і розробити відповідні політики обробки, інформація повинна бути організована та класифікована.

Розробка політики в масштабах всієї компанії допомагає створити всеосяжну стратегію та ядро для стратегії IT-безпеки.

Створюючи план інформаційної безпеки, необхідно переконатися, що він є комплексним і відповідає потребам підприємства.

Початок роботи починається з організаційних питань, необхідно створити групу фахівців інформаційної безпеки. Вони відповідатимуть за створення та впровадження політики, реагування на мінливості загроз кібербезпеці, визначення порогових значень ризику та навіть організацію фінансування.

Створена команда при плануванні буде оцінювати ризики, загрози та вразливості безпеки інформаційної системи, визначати запобіжні заходи для попередження, оцінювати, як проблеми та порушення кібербезпеки вплинуть на систему: чи призведе порушення до зупинки операцій? Чи спричинить це за собою контроль пошкоджень? А як щодо регуляторних штрафів?

Крім оцінювання командою планування доцільно також провести оцінку ризиків третьою стороною.

Важливо стежити також за сторонніми постачальниками, які також можуть становити загрозу. Їх потрібно відвідувати принаймні раз на рік, щоб перевірити, чи відповідають їхні політики та практики плану інформаційної безпеки. підприємства Потрібно скласти список критеріїв, яким повинні відповідати потенційні партнери, перш ніж працювати з ними. Цей список повинен включати такі основи, як відповідність System and Organization Controls (SOC) II. (Системний та організаційний контроль (SOC) для організацій, що надають послуги, – це звіти внутрішнього контролю, створені Американським інститутом сертифікованих бухгалтерів (AICPA). Вони призначені для перевірки послуг, що надаються сервісною організацією, щоб кінцеві користувачі могли оцінити та

усунути ризики, пов'язані з аутсорсинговою послугою).

При визначенні активів їх потрібно оцінити на основі таких факторів, як вразливість, вимоги до доступу та зберігання. Ця інформація необхідна для написання політик і процедур, які враховують відносний ризик і потреби в поводженні з різними активами.

Вся робота з планування повинна бути організована у відповідності з існуючими нормативно-правовими актами у сфері інформаційної безпеки. Необхідно при плануванні визначити застосовні нормативні стандарти, окреслити, як план буде відповідати нормативним вимогам.

Після складання своїх потреб та ризиків, необхідно створювати план реагування. Для цього потрібно ретельно окреслити процес, щоб команда могла спокійно та систематично реагувати на порушення кібербезпеки, коли вони виникають. Обов'язково включити у свій план різні відділи, треті сторони та клієнтів, щоб кожен міг зробити все необхідне для усунення порушення.

Співробітники можуть бути величезним активом у боротьбі з кіберзагрозами, але вони також можуть становити загрозу, якщо вони не навчені належним чином. Необхідно організувати постійне навчання та регулярне тестування співробітників, щоб переконатися, що вони знають, на що звертати увагу.

Вибір конкретної методики планування інформаційної безпеки може залежати від багатьох факторів, таких як розмір підприємства, галузь діяльності, регуляторні вимоги і конкретні ризики. Однак загальний підхід може включати кроки які складають методику планування інформаційної безпеки підприємства (рис. 2.5)

Ці кроки можуть слугувати загальним керівництвом для розробки плану інформаційної безпеки, але вони повинні бути адаптовані відповідно до конкретних умов і вимог конкретного підприємства.

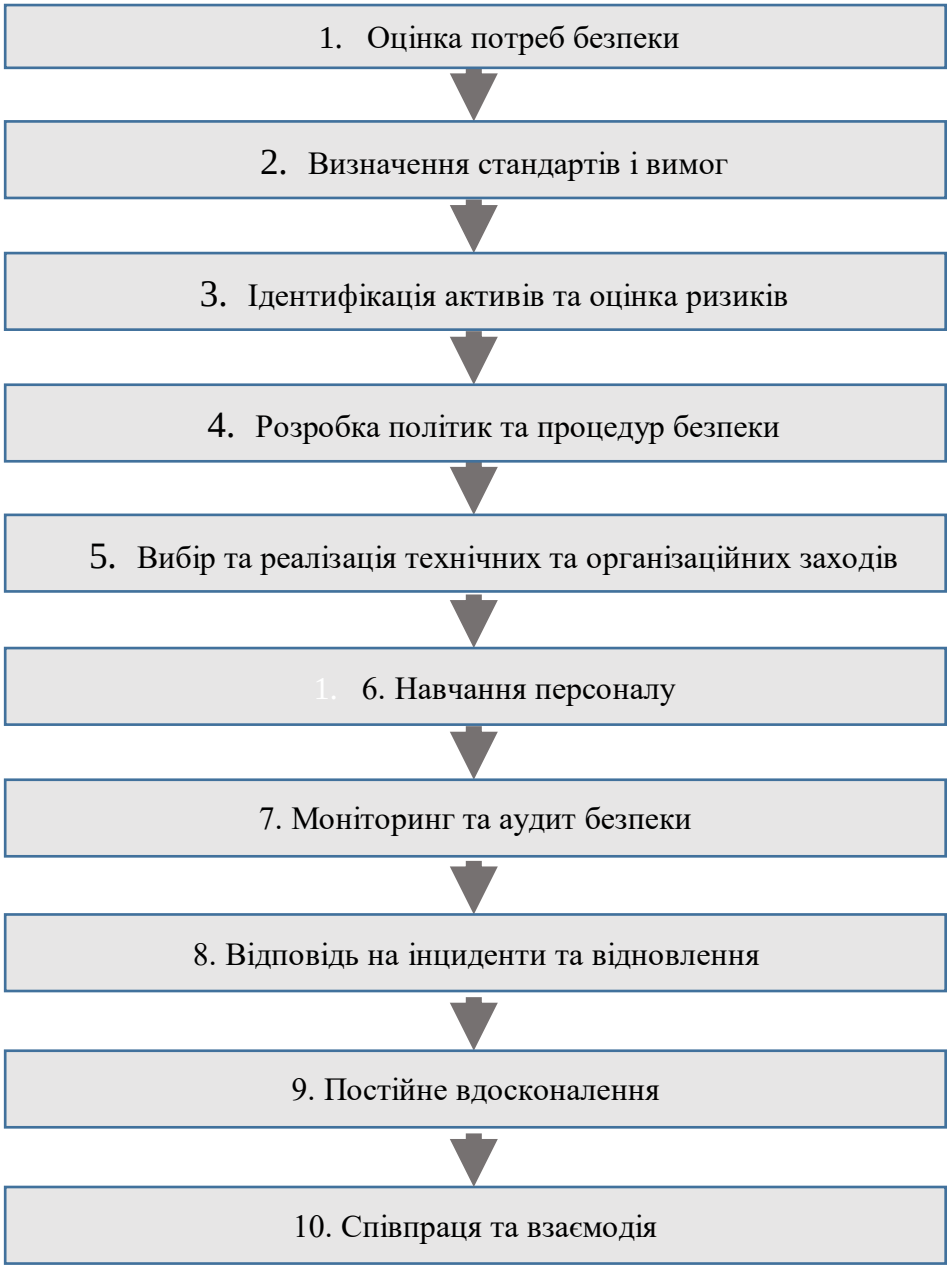

Рис. 2.5. Алгоритм методики планування інформаційної безпеки

ВИСНОВКИ до другого розділу. У розділі проведено докладний аналіз підходів до планування та реалізації заходів інформаційної безпеки на підприємстві, а також визначено методику планування, спрямовану на створення ефективної стратегії забезпечення інформаційної безпеки.

В процесі вивчення різних підходів було виявлено, що інформаційна безпека на підприємстві вимагає комплексного та системного підходу. Кожен підхід, чи то технічний, організаційний, чи людський, має своє місце і важливу

роль у створенні інтегрованої системи захисту інформаційної безпеки на підприємстві.

Стратегічне планування, орієнтоване на бізнес-процеси, забезпечує вирішення завдань інформаційної безпеки в контексті стратегічних цілей підприємства. Технічне планування визначає вибір імплементації технічних засобів та систем для захисту інформації. Організаційне планування стосується формування ефективних політик та процедур, а людський фактор враховує залучення персоналу та навчання з питань кібербезпеки.

Методика планування інформаційної безпеки, розроблена на основі вивчених підходів, передбачає системний аналіз потреб, ризиків та ресурсів підприємства. Вона включає етапи формування стратегії, визначення метрик ефективності, розроблення плану заходів та систему моніторингу та оцінки.

Методика розглядає всі аспекти, від технічних аспектів до людського фактору, для забезпечення повноцінних інтегрованих заходів інформаційної безпеки. Вона покликана бути гнучкою та адаптивною, щоб враховувати зміни в кіберзагрозах, технологічних парадигмах та стратегічних цілях підприємства.

Розроблена методика дозволить підприємствам ефективно і системно підходити до планування і реалізації заходів інформаційної безпеки, забезпечуючи високий рівень захисту та враховуючи всі необхідні аспекти цього складного процесу.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХОДІВ ПЛАНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Впровадження заходів інформаційної безпеки

Для впровадження заходів інформаційної безпеки важливо мати чітке розуміння ризиків і загроз, з якими стикається ваша організація. Визначивши ці ризики, можна розробити план їх пом’якшення. Стандарт ISO/IEC 27001 забезпечує основу для впровадження системи управління інформаційною безпекою (ISMS), яка може допомогти вам керувати цими ризиками та захистити інформаційні активи вашої організації.

Загрози не залишаються статичними. Підприємствам доведеться активно підтримувати свої можливості інформаційної безпеки в умовах мінливих вразливостей, а також змін у власному бізнес-середовищі. Щоб впоратися з цим завданням, керівники підприємств або підрозділів інформаційної безпеки підприємств повинні виробити звичку розділяти практики інформаційної безпеки на компетенції, включаючи ідентифікацію та класифікацію активів, впровадження та управління кіберінцидентами.

Відправною точкою повинні стати наступні заходи для практики інформаційної безпеки підприємства:

- постійна ідентифікація та класифікація інформаційних активів, у тому числі тих, якими керують інші сторони, за критичністю та чутливістю, ця класифікація повинна відображати ступінь, до якого інцидент інформаційної безпеки, що впливає на інформаційний актив, потенційно може вплинути, фінансово чи нефінансово, на клієнта або інтереси його зацікавлених сторін;
- впровадження постійних планових контролів, мати засоби контролю інформаційної безпеки для захисту інформаційних активів, у тому числі тих, якими керують інші сторони, які впроваджуються своєчасно та які є співмірними з уразливістю та загрозами, критичністю і чутливістю, потенційними наслідками

можливого інциденту;

- впровадження надійних механізмів для своєчасного виявлення та реагування на інциденти інформаційної безпеки, ведення планів реагування на інциденти інформаційної безпеки, які, на думку клієнта, можуть виникнути (плани реагування на інформаційну безпеку). Плани повинні включати механізми для управління всіма відповідними етапами інциденту, від виявлення до перевірки після інциденту, порядок повідомлення про інциденти інформаційної безпеки вищому керівництву та Раді директорів, іншим керівним органам та особам, відповідальним за управління та нагляд за інцидентами інформаційної безпеки, залежно від обставин. Щорічно переглядати та тестувати плани реагування на інформаційну безпеку, щоб переконатися, що вони залишаються ефективними та відповідають поставленим цілям.

Не зважаючи на витрати на впровадження, дотримання найкращих практик інформаційної безпеки та управління інцидентами саме по собі є вигідним для клієнтів. Більше того, технологія управління цифровою безпекою може допомогти клієнтам планувати та керувати своєю інформацією, операціями та комунікаціями, пов'язаними з інформаційною безпекою, скорочуючи деякі початкові витрати.

Окрім цих стандартів, важливо впроваджувати засоби контролю для захисту ваших інформаційних активів відповідно до критичності та чутливості інформаційних активів. Проведення систематичного тестування та впевненість щодо ефективності цих засобів контролю також є важливими. Нарешті, є важливим сповіщення ключових регуляторів про суттєві інциденти інформаційної безпеки.

Розглянуті в розділі 1, 2 теоретичні питання планування заходів інформаційної безпеки підприємства визначали, що одним із інструментів забезпечення конфіденційності є багатофакторна автентифікація.

Багатофакторна автентифікація може допомогти запобігти доступу до мережі організації тим, хто неправомірно отримав дані для входу. Хоча спочатку цей інструмент повільно приживався, зараз він вважається будівельним блоком

кібербезпеки, як на індивідуальному, так і на організаційному рівні, і набув широкого поширення. Фактично, MFA настільки широко визнана, що Національний альянс з кібербезпеки назвав MFA одним із чотирьох ключових напрямків поведінки в центрі уваги Національного місяця обізнаності про кібербезпеку (NCAM).

Багатофакторна автентифікація не обов'язково виглядатиме однаково для кожної організації, але процеси багатофакторної автентифікації можуть стати жертвами багатьох однакових загроз: фішингу та соціальної інженерії. Мотивовані хакери можуть спробувати перехопити код автентифікації через підроблений веб-сайт, наприклад, за допомогою атаки типу "людина посередині". Або вони можуть спробувати перехопити сесійний файл cookie під час так званої атаки pass-the-cookie.

Зловмисники можуть використовувати агресивні підходи, щоб обійти багатофакторну автентифікацію. Наприклад, якщо зловмисник націлиться на співробітника, чия організація використовує SMS-автентифікацію, зловмисник може отримати контроль над номером телефону працівника, пов'язаним із процесом автентифікації, за допомогою шахрайства із заміною SIM-карти. Крім того, хакер може використовувати техніку, відому як MFA fatigue – атака, під час якої пристрій цілі бомбардується безперервними сповіщеннями MFA зловмисником, доки він не підтвердить свою особу, таким чином надаючи зловмиснику доступ.

Однак, як і інші типи рішень безпеки, багатофакторна автентифікація ніколи не повинна розглядатися як рішення за принципом «встановив і забув». Для того, щоб багатофакторна автентифікація забезпечувала ефективний рівень безпеки, організації повинні дотримуватися найкращих практик, їм пропонується кілька практичних порад щодо багатофакторної автентифікації.

1. Обирайте прозорого та чесного постачальника. Успішне впровадження MFA починається задовго до того, як співробітники підприємства почнуть використовувати його або навіть навчаться ним користуватися. Керівництво інформаційної безпеки підприємства повинно спочатку переконатися, що

постачальники багатофакторної автентифікації, яких вони розглядають, чесні та прозорі щодо своїх продуктів. Навіть якщо керівники служби безпеки не зіткнуться з червоними прапорцями, чи буде продукт легко розгорнути в усій організації та масштабувати в міру його зростання? Все це важливі питання, які слід задати перед вибором рішення MFA.

2. Навчайте та підтримуйте співробітників. Як до, так і під час розгортання рішення MFA підприємства надзвичайно важливо ознайомити своїх співробітників із тим, що таке багатофакторна автентифікація (за умови, що підприємство ніколи раніше не мало рішення), як воно допомагає захистити критично важливі активи та чому працівники повинні відчувати потребу в його використанні. Розгляньте можливість проведення ґрунтовних тренінгів, які служать вступом до багатофакторної автентифікації, детально розповімо про те, чому деякі фактори вважаються більш безпечними, ніж інші, навчіть співробітників, як уникнути фішингу та атак соціальної інженерії, а також покажіть, як на практиці виглядатиме використання MFA-рішення. Це допоможе забезпечити підтримку співробітників до та під час його розгортання.

3. Розгорніть багатофакторну автентифікацію по всій організації. Впровадження багатофакторної автентифікації в усій організації, а не в ізольованих приміщеннях, вважається безпечнішим і допомагає зменшити поверхню атак на організацію. Це особливо актуально для організацій з великою кількістю віддалених працівників, співробітники яких отримують доступ до серверів і обробляють конфіденційні дані з-за меж корпоративної мережі.

4. Надавайте пріоритет простоті використання MFA. На цьому етапі впровадження MFA у організації керівники служб безпеки, можливо, вже вибрали рішення, знають, як застосувати це рішення в кожній сфері бізнесу, і, можливо, навіть розпочали процес навчання співробітників. Але перш ніж впроваджувати рішення для багатофакторної автентифікації, важливо правильно його налаштувати, приділяючи першочергову увагу простоті використання для ваших співробітників.

Коли співробітникам важко використовувати систему багатофакторної

автентифікації, може виникнути кілька проблем, включаючи втому від багатофакторної автентифікації, обхідний шлях, перевантажений IT-персонал і загальну відсутність підтримки в організації. Зрештою, якщо рішення MFA є занадто складним або проблематичним для співробітників, воно може призвести до більшої кількості проблем, ніж рішень.

Коли MFA буде вперше розгорнуто, для співробітників майже неминуче настане період адаптації, але початкові розчарування співробітників можна пом'якшити, переконавшись, що ваше рішення MFA налаштовано так, щоб воно було зручним для користувача. Цього можна досягти, наприклад, об'єднавши багатофакторну автентифікацію з програмою єдиного входу (SSO), щоб запобігти вигоранню, пов'язаному з необхідністю входити в кілька програм окремо. Працівникам також слід надати вибір щодо того, які фактори вони можуть використовувати, будь то використання біометрії для підтвердження своєї особи, код, отриманий через SMS або додаток для автентифікації, або фізичний ключ безпеки, серед інших факторів.

5. Розгляньте можливість використання факторів, стійких до атак. Простота використання має бути великим пріоритетом при впровадженні багатофакторної автентифікації у організації, але вона ніколи не повинна відбуватися за рахунок безпеки. Хоча працівникам має бути надана можливість вибирати між різними факторами автентифікації, вони також повинні бути обізнані про відмінності в безпеці між факторами. Наприклад, співробітники повинні розуміти ризики, пов'язані з SMS-автентифікацією, і, зокрема, ймовірність стати жертвою шахрайства із заміною SIM-карти. І коли керівники служб безпеки обмірковують, з яких факторів дозволити співробітникам вибирати, варто поставити собі запитання: «Яким співробітникам потрібна достатньо хороша, краща та найкраща безпека?».

Співробітників слід заохочувати до використання факторів, стійких до атак. Наприклад, автентифікація FIDO, яка використовує криптографію з відкритим і закритим ключем, була названа Агентством з кібербезпеки та безпеки інфраструктури (CISA) золотим стандартом і найбезпечнішою формою

MFA.

Результатом планування і впровадження спланованих заходів є Політика інформаційної безпеки або ISP, вона відноситься до набору правил або «політик», що стосуються інформаційної безпеки. Особливо це стосується роботи з IT-активами. Основна мета Політики, як набору правил, – забезпечити їх дотримання, наприклад, дотримання співробітниками або користувачами протоколів і процедур безпеки.

Політики інформаційної безпеки не тільки допомагають компанії дотримуватися законів, в більш широкому масштабі ця політика слугує ранніми кроками щодо пом'якшення наслідків потенційних порушень безпеки.

Хоча політика інформаційної безпеки може відрізнятися від однієї компанії до іншої, вона має спільні елементи. У списку нижче розглянуто вісім важливих елементів при розробці політик інформаційної безпеки та основні приклади їх визначення.

1. *Мета*. По-перше, сформулюйте мету політики. Наприклад:

- для виявлення або пом'якшення порушень інформаційної безпеки;
- для підтримки репутації компанії;
- крім того, поважати права клієнтів і підтримувати дотримання федеральних законів.

2. *Аудиторія*. Має бути зрозуміло, на кого поширюється вимоги правил політики. Наприклад:

- усім співробітникам або певним відділам.

3. *Цілі політики* повинні відповідати принципам стандартів InfoSec, а саме:

- конфіденційність;
- цілісність;
- доступність.

4. *Повноваження та політика контролю доступу*. Посилається на те, кому можуть бути надані дані. Наприклад, вона може складатися з двох категорій.

- ієрархічна структура;

- політика мережевої безпеки.

5. *Класифікація даних*. У цьому елементі чітко розділіть дані відповідно до рівня їх конфіденційності. Наприклад:

- цілком таємно;
- таємно;
- конфіденційний;
- відкритий доступ.

6. *Підтримка даних та операцій*, мається на увазі практика зберігання та передачі даних. Вона може складатися з трьох категорій:

- правила захисту даних;
- резервне копіювання даних;
- переміщення або передача даних.

7. *Обізнаність та поведінка щодо безпеки*. Проведення тренінгів серед співробітників має сприяти поширенню кіберобізнаності, закони та етика безпеки мають бути зрозумілими для них під час цього тренінгу.

8. *Права та обов'язки*. Кожен персонал повинен знати свою частку в безпеці. Таким чином, кожен повинен чітко знати свій обов'язок.

3.2 Моніторинг ефективності реалізації заходів інформаційної безпеки

Інформаційне забезпечення, як і всі важливі рішення, рясніє компромісами. Ризик, який приймається простим управлінням інформаційною системою в сучасній глобально пов'язаній інформаційній інфраструктурі, повинен бути збалансований з потребами організації для виконання її наміченої місії, а також з витратами, пов'язаними з інформаційними технологіями та практикою, які забезпечують інформаційні системи та інформацію в них.

Визначення ефективності реалізації заходів інформаційної безпеки підприємства є важливим етапом, оскільки дозволяє оцінити ефективність

впроваджених заходів та виявити можливі області для покращень.

Існує три основні способи реалізації процесів моніторингу ефективності та ефективності контролю кібербезпеки:

- встановлення та регулярний перегляд показники безпеки;
- проведення оцінки вразливостей і тестування на проникнення, щоб перевірити конфігурацію безпеки;
- проведення внутрішнього аудиту (або інша об'єктивна оцінка) для оцінювання роботи з контролю безпеки.

Визначивши конкретні цілі програми безпеки, можна розробити конкретні заходи та контролювати ці заходи з часом, щоб оцінити ефективність процесу. Показники ефективності безпеки можна розділити на три основні категорії:

- *операційна статистика* включає в себе підрахунки активності в навколишньому середовищі. Вони не обов'язково відображають дії організації, але вони допомагають сформувати загальну обізнаність про діяльність, пов'язану з безпекою в організації.
- *показники ефективності* - це похідні або обчислені показники, які кількісно оцінюють поведінку організації або результати діяльності відповідно до заявленої мети, їх розглядають з точки зору конкретних дій, які вживають працівники, щоб допомогти підтримувати безпеку організації.
- *цілі відповідності* - це специфічний тип вимірювання ефективності, спрямований на демонстрацію того, чи дотримується організація встановленої політики безпеки.

Для того, щоб перевірити ефективність налаштування безпеки, всі організації повинні провести оцінку вразливостей і тестування на проникнення. Метою оцінки вразливостей є виявлення виправлень безпеки системи, які організація могла пропустити, або будь-яких слабких конфігурацій безпеки, які організація застосувала. Охоронні фірми використовують різноманітні автоматизовані інструменти сканування для порівняння конфігурацій системи з опублікованими списками відомих вразливостей.

Тестування на проникнення виводить сканування вразливостей на новий

рівень. Досвідчений, етичний хакер використовує виявлені вразливості та моделює реальні сценарії атак, щоб визначити, чи можуть ці вразливості бути використані та призвести до фактичного злому. Організація може використовувати результати сканування вразливостей і тестування на проникнення, щоб виявити будь-які прогалини в безпеці, а також розглянути першопричину того, що дозволило цим вразливостям впровадитися в організації.

З огляду на поточний стан інформаційної безпеки та постійну еволюцію загроз безпеці, вкрай важливо, щоб відділи внутрішнього аудиту діяли як третя лінія захисту та перевіряли ефективність контролю кібербезпеки, щоб допомогти підвищити загальну безпеку організації.

Використовуючи результати оцінки ризиків кібербезпеки, хороший процес перевірки починається з перегляду організаційних політик, процедур, інструкцій і стандартів кібербезпеки. Успішний внутрішній аудит кібербезпеки потребує спонсорства з боку виконавчого керівництва для полегшення процесу. Внутрішній аудит розпочинає процес аудиту шляхом проведення інтерв'ю з ключовими зацікавленими сторонами, щоб підтвердити розуміння діяльності, що відбувається щодо задоволення цілей контролю кібербезпеки.

В рамках аудиту типовим було б проведення аналізу прогалин у політиці та стандартах безпеки підприємства незалежній системі контролю, щоб визначити, чи засоби контролю інформаційної безпеки належним чином розроблені для досягнення мети безпеки, і чи вони наявні та узгоджені з оцінкою ризиків організації. Крім того, важливо оцінити, чи чітко визначені та належним чином розподілені ролі персоналу та відповідальність за безпеку на співробітників, які мають достатні навички та повноваження для виконання цих засобів контролю.

Ґрунтуючись на результатах оцінки проєкту, підприємство може забезпечити вищий рівень впевненості, визначивши, чи ефективно працюють засоби контролю безпеки. Аудиторська група використовуватиме задокументовані політики та процедури безпеки для встановлення процедур аудиту, тестування контролю безпеки.

Потім отримуються та перевіряються докази ефективності контрольної діяльності для всіх елементів керування, які мають ручний компонент, наприклад, керування обліковими записами користувачів, керування змінами в інфраструктурі та програмах, а також резервне копіювання систем. Нарешті, для системних елементів керування, наприклад, налаштувань брандмауера, антивірусу, налаштувань шифрування даних, внутрішній аудит перевіряє конкретні конфігурації систем, щоб визначити, чи встановлені вони належним чином. За відсутності можливостей внутрішнього аудиту для усунення ризиків кібербезпеки, розгляньте можливість залучення об'єктивної третьої сторони для проведення аналогічної оцінки.

Після впровадження засобів контролю підприємство повинно контролювати своє середовище контролю, щоб переконатися, що засоби контролю залишаються ефективними. Поєднуючи показники безпеки, тестування внутрішнього аудиту та регулярне тестування на вразливість/проникнення, підприємство може допомогти гарантувати, що його програма інформаційної і кібербезпеки залишається ефективною та розвивається належним чином разом з підприємством.

Запропоновані в дослідженні [66] ключові показники ефективності управління безпекою дозволяють детально оцінити стан управління інформаційною безпекою. В цьому дослідженні були визначено наступні категорії метрики і запропоновані класифікації:

- фінансові показники – пов'язані з фінансовими Вплив засобів контролю безпеки;
- оцінка зрілості – оцінює стан Безпека в цілому або в якійсь конкретній сфері такі як кібербезпека, безперервність, застосування Безпека або керування;
- моделювання – має намір спростити аналіз у відсутність реальних даних;
- вимірювання на основі припущень – складається з Обмеження та фокусування вимірювальних зусиль;
- прогрес у досягненні цілей – складається з встановлення KPI для вимірювання ступеня прогрес у досягненні поставлених цілей;

- операційні показники – формулює ефективність засобів контролю та процесів безпеки;

- аналіз витрат – надає релевантні показники для Управління витратами на безпеку;

- бенчмаркінг – дає змогу порівнювати процес, що відбувається разом з іншими організацій або кодексів належних практик.

Із перерахованих позицій класифікації заслуговує на увагу метод моделювання для оцінки рентабельності інвестицій у контексті технології або зміни рішення, з візуальним зображенням критерію ефективності (рис. 3.1).

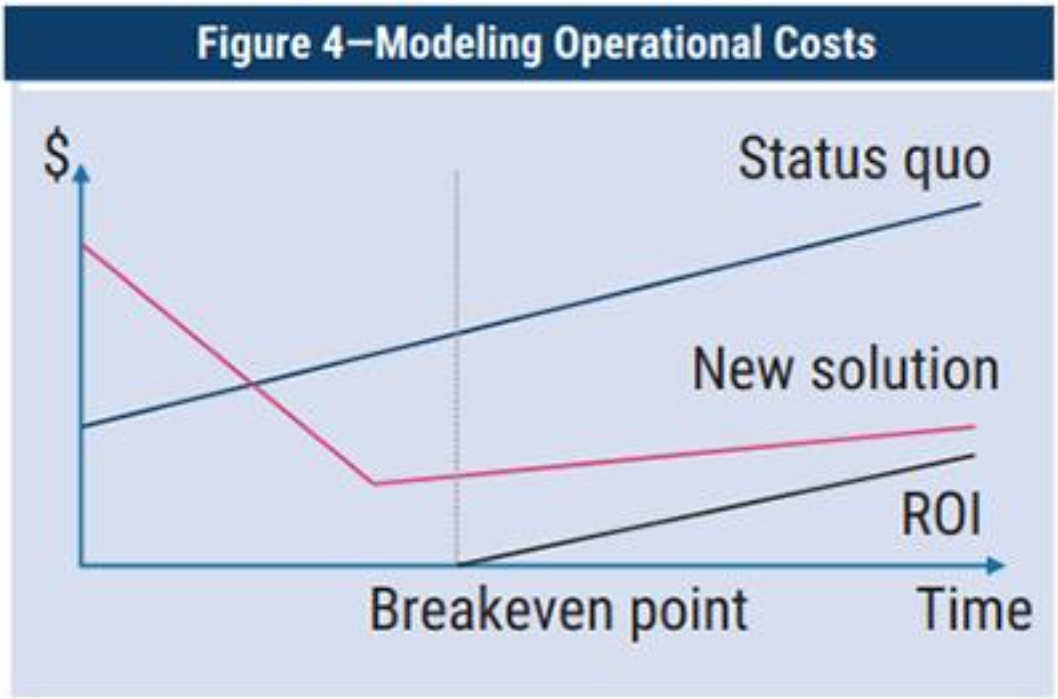

Рис.3.1. Результат моделювання для оцінки рентабельності інвестицій [66]

Графічні зображення показників допомагають відповісти на питання, які задають менеджери, і, таким чином, полегшують коригування програми інформаційної безпеки.

На рисунку 3.2 подано кілька ключових кроків для визначення ефективності інформаційної безпеки на підприємстві.

Рис. 3.2. Зміст заходів визначення ефективності інформаційної безпеки на підприємстві

Щоб оцінити ефективність заходів безпеки інформації, можна використати оновлений ISO/IEC 27004:2016. Цей стандарт надає вказівки щодо того, як оцінювати ефективність ISO/IEC 27001, як розробляти та керувати процесами вимірювання, а також як оцінювати та звітувати про результати набору показників інформаційної безпеки. Стандарт ISO/IEC 27004:2016 показує, як побудувати програму вимірювання інформаційної безпеки, як вибрати, що вимірювати, і як керувати необхідними процесами вимірювання. Він містить численні приклади різних типів заходів, а також те, як можна оцінити ефективність цих заходів.

Серед багатьох переваг для підприємств використання ISO/IEC 27004 можна виділити:

- підвищена підзвітність;
- підвищення продуктивності інформаційної безпеки та процесів СУІБ;
- докази відповідності вимогам стандарту ISO/IEC 27001, а також чинним законам, правилам і нормам.

Керівні органи інформаційної безпеки та загальне керівництво підприємством потребують регулярного звітування від співробітників служби безпеки, щоб оцінити плани та програми інформаційної безпеки і мати можливість повною мірою виконувати свої обов'язки. За відсутності чіткого бачення витрат, вигод, пріоритетів та ризиків керівники вищої ланки не можуть керувати програмою безпеки та наражати себе на ризик інцидентів, недотримання вимог та фінансових втрат. Звітність також слугує інструментом комунікації та зміцнює культуру безпеки серед усіх зацікавлених сторін. Кілька представлених високорівневих або стратегічних показників передають загальну інформацію про стан інформаційної безпеки з цією метою. Однак стратегічні показники повинні бути попередньо прийняті керівниками, адже індикатори стають важливою опорою в процесі управління.

Для того щоб оцінити ефективність пропонується застосувати метрики та критерії, які згруповані в табл. 3.1.

Таблиця 3.1.

Критерії і метрики оцінювання ефективності реалізації заходів інформаційної безпеки

Що оцінюється	Критерій	Метрика
Частота та обсяг інцидентів	Зниження кількості та обсягу інцидентів свідчить про ефективність заходів з проактивного та реактивного управління безпекою	Кількість та обсяг інцидентів за певний період часу
Реагування на інциденти	Швидке виявлення, реакція та відновлення після інциденту допомагає знизити потенційні втрати	Час реакції на інциденти та час відновлення після інциденту
Рівень виявлення загроз	Покращення систем виявлення загроз та відновлення вразливостей зменшує ризик втрат	Кількість та якість виявлених загроз та вразливостей
Рівень доступності	Підвищення рівня доступності та зниження невідповідностей управління доступом	рівень доступності інформаційних ресурсів, стабільність систем
Використання систем безпеки	Забезпечення ефективного використання систем безпеки сприяє управлінню ризиками та підвищує ефективність заходів	Частота та ефективність використання інструментів безпеки
Рівень свідомості персоналу	Підвищення рівня свідомості персоналу про загрози та відповідальність сприяє зменшенню людського фактору в ризиках безпеки	Результати тестів на свідомість з питань безпеки, кількість навчальних заходів
Витрати на інформаційну безпеку	Забезпечення адекватного рівня витрат, що зменшує загрози та ризики	Витрати на заходи інформаційної безпеки у порівнянні із збитками від можливих інцидентів

Ці метрики та критерії допомагають підприємствам оцінювати ефективність своїх заходів інформаційної безпеки та вчасно реагувати на можливі проблеми. Однак вони можуть бути адаптовані відповідно до конкретних потреб та характеристик кожного підприємства.

3.3 Формулювання конкретних рекомендацій для підприємств щодо вибору та впровадження підходів до планування і реалізації заходів інформаційної безпеки

Розглянуті у розділах 1,2 підходи до планування і реалізації заходів інформаційної безпеки підприємства дають можливість відпрацювати рекомендації та пропозиції щодо формування плану інформаційної безпеки та політики інформаційної безпеки підприємства.

За методикою, розробленою в п. 2.2. (рис. 2.4) сформовані пропозиції керівництву підприємства для забезпечення ефективності системи інформаційної безпеки, які включають організаційні, технічні та нормативно-правові заходи.

1. Створіть команду для планування з фахівців кібербезпеки, які обізнані з правилами інформаційної безпеки, мають відповідний досвід роботи, склали іспити або мають відповідні сертифікати інформаційної безпеки.

2. Розпочніть з оцінки потреб інформаційної безпеки вашого підприємства. Розгляньте основні активи, ризики, вразливості та загрози.

3. Визначте стандарти безпеки, які відповідають вашій галузі діяльності, а також вимоги регуляторів (якщо такі є). Наприклад, ISO/IEC 27001 може слугувати основою для створення системи управління інформаційною безпекою.

4. Визначте та класифікуйте критичні інформаційні активи, а також оцініть ризики, пов'язані з їх втратою чи пошкодженням.

5. Розробіть політики та процедури безпеки, які охоплюють всі аспекти інформаційної безпеки в організації.

6. Виберіть відповідні технічні та організаційні заходи для захисту інформації та впровадження їх в організації.

7. Забезпечте навчання та підвищення обізнаності персоналу щодо сучасних загроз та відповідних заходів безпеки.

8. Розгорніть системи моніторингу та системи аудиту для постійного контролю за ефективністю заходів безпеки та виявлення можливих відхилень.

9. Розробіть план відповіді на інциденти та відновлення, щоб бути готовим до швидкого та ефективного відновлення після кібератак чи інших інцидентів.

10. Встановіть механізми постійного вдосконалення системи інформаційної безпеки. Враховуйте результати аудитів, зміни в організації та нові технології.

11. Забезпечте співпрацю та взаємодію з іншими відділами організації, стейкхолдерами та іншими організаціями для підтримання інформаційної безпеки.

В результаті проведеного дослідження напрацьовані кілька рекомендацій технічного напрямку.

Безпека пристроїв і додатків повинна поширюватися на всі комп'ютери, планшети, корпоративні телефони, інтелектуальні пристрої, програми, програмне забезпечення користувача, комп'ютерні програми та облікові записи в Інтернеті. При цьому запобіжні заходи включають:

- підтримку всіх програм і програмного забезпечення в актуальному стані та їх подальша безпека;
- унікальні паролі та облікові дані для входу для кожного користувача, які регулярно змінюються;
- впровадження регулярних планових вікон для технічного обслуговування пристроїв та систем протягом місяця;
- ведення ретельних і актуальних записів про всі дії на пристроях і в додатках, включно з можливими, виявленими або окремими загрозами;
- надання кожному користувачеві пристрою та обліковому запису системи виявлення вторгнень на хост;
- видалення непотрібних програм, програмного забезпечення, облікових записів користувачів і пристроїв із ротації;
- впровадження керування патчами, щоб підтримувати все в актуальному стані та автоматично виправлятися при випуску нових патчів.

Незалежно від того, яким бізнесом чи галуззю займається підприємство, є ймовірність, що в якийсь момент часу воно може стати мішенню для хакерів і кіберзлочинців. Згідно з нещодавньою статистикою Accenture, щороку

відбувається понад 130 великих цілеспрямованих порушень кібербезпеки корпоративного масштабу. І це число зростає швидкими темпами – 27 відсотків на рік.

Середня вартість атаки шкідливого програмного забезпечення для компаній становить 2,4 мільйона доларів, а ефективна боротьба з компаніями коштує в середньому 50 днів. Уникнення кібератак, а також пов'язаних з ними збитків і витрат є причиною того, чому компаніям доцільно зосередити значну частину своїх IT-бюджетів і ресурсів на розробці (і впровадженні) корпоративної політики інформаційної безпеки (EISP).

Оскільки загрози корпоративній кібербезпеці зростають такими швидкими темпами, компанії зараз розробляють політику корпоративної програми інформаційної безпеки, яка служить як для мінімізації ризиків, так і для досягнення ключових бізнес-цілей і завдань.

Незалежно від того, чи вирішили на підприємстві вперше впровадити корпоративну політику в галузі кібербезпеки чи оновити ту, яка уже є, необхідно для створення корпоративної політики безпеки підприємства сформувати її елементи для покращення інформаційної та кібербезпеки, які наведені нижче з рекомендаціями.

Мережева безпека. Перш за все, політика безпеки підприємства повинна охоплювати всі критично важливі елементи, необхідні для забезпечення захисту ваших IT-мереж і систем. Елемент мережевої безпеки політики має бути зосереджений на визначенні, аналізі та моніторингу безпеки інформаційної мережі. Він повинен служити для забезпечення надійної позиції кібербезпеки, а також намагатися усунути потенційні прогалини, якими потенційні хакери можуть прагнути скористатися.

Архітектура та політика мережевої безпеки повинні охоплювати всі основні сфери:

- сканування вразливостей;
- керування патчами;

- оновлені програми безпеки (брандмауери, проксі-сервери, антивірусне програмне забезпечення тощо);
- проектування мережевої архітектури (і огляд);
- керування та аналіз кінцевих точок.

У політиці має бути відображено, що мережева безпека є спільною відповідальністю, починаючи від виконавчого керівництва та IT-команди і закінчуючи рядовими співробітниками. Доручіть своїй команді безпеки та IT визначити технічну політику та процедури, яких слід дотримуватися щодо мережевої безпеки, і обов'язково попрацюйте з управлінським та виконавчим персоналом, щоб забезпечити правильну бізнес-практику, щоб мінімізувати ризик порушення мережевої безпеки.

Безпека додатків. Елемент безпеки додатків, як правило, призначений для запобігання ризикам, які виникають через вразливості додатків. Це може бути що завгодно від сторонніх хмарних додатків до внутрішньо розроблених і виконуваних. У політиці мають бути визначені стратегії для усунення ризиків, пов'язаних із будь-якими програмами, які потенційно можуть бути використані, при цьому всі програми на підприємстві мають бути належним чином класифіковані залежно від того, наскільки вони критичні (і наскільки конфіденційними є дані, які вони містять). Ці класифікації допомагають командам з кібербезпеки та IT-відділам приймати обґрунтовані рішення про те, які типи контролю та захисту потрібні для кожної програми, а потім описані в політиці. Елемент безпеки програми повинен включати деякі (якщо не всі) з наведених нижче елементів:

- перегляд структури заявки;
- життєвий цикл розробки системи;
- тестування на проникнення;
- огляд вихідного коду;
- керування патчами.

Як правило, команда з інформаційної безпеки буде головною, яка зосереджується на частині безпеки додатків у політиці. Обов'язково залучіть усіх

відповідних технічних співробітників з кібербезпеки з *самого початку* будь-якого життєвого циклу проектування, розробки або впровадження програми. Це допомагає їм зрозуміти потенційні слабкі місця в будь-якій програмі, яка може стати мішенню, і розмістити відповідні найкращі практики у політиці, щоб закрити будь-які прогалини.

Управління ризиками. Цей третій елемент складається з набору заходів, спрямованих на зниження рівня ризику кібератак до рівня, який підприємство буде вважати «прийнятним рівнем». Що це таке, залежатиме від характеру бізнесу, систем і даних, і найкраще співпрацювати з надійним партнером з кібербезпеки, щоб зрозуміти основи управління кіберризиками, щоб визначити, який «прийнятний ризик в унікальних обставинах підприємства».

Розділ EISP з управління ризиками вплине на багато інших областей політики і зазвичай виконується в наступні чотири кроки (зазвичай спільно з партнером з кібербезпеки):

- *оцінка ризиків***:** усі ризики, що входять до сфери дії вашого EISP, визначаються з урахуванням культури та технічних систем вашої організації. Саме тут партнер зазвичай допомагає вам провести аналіз розриву;
- *аналіз ризиків***:** далі ризики у вашій політиці визначаються за пріоритетами на основі впливу, ймовірності та потенційних витрат. Це може бути зроблено на якісній, кількісній або гібридній основі з метою проведення аналізу витрат і вигоди для потенційних заходів безпеки;
- *лікування ризиків***:** ґрунтуючись на результатах попередніх двох кроків, ви окреслите конкретні кроки щодо того, як лікувати (і мінімізувати) ці ризики. У вашій політиці має бути зазначено, як кожен ризик буде пом'якшено, передано або прийнято на основі вашого аналізу;
- *моніторинг ризиків*: на цьому останньому етапі контроль постійно відстежується на предмет змін рівнів ризику або нових недоліків чи слабких місць, які можуть з часом вийти на поверхню. Майте звітність за показниками, на додаток до періодичного аудиту, щоб ваш рівень ризику постійно коригувався до відповідного рівня.

Управління дотриманням нормативних вимог. Кожне підприємство має набір вимог до відповідності, яким вони повинні відповідати залежно від галузі, в якій вони працюють. Це можуть бути такі фреймворки, як HIPAA для охорони здоров'я, PCI-DSS для фінансової індустрії або GDPR для тих, хто працює в Європі. Ці вимоги зазвичай включають юридичні, нормативні та сертифікаційні вимоги, які необхідно враховувати у EISP. До вимог законодавства належать і договірні вимоги. У політиці мають бути визначені всі законодавчі вимоги та окреслено програму, яка відповідає всім цим потребам. Комплаєнс, по суті, слід розглядати як ще одну форму ризику у вашій політиці. Керування дотриманням нормативних вимог зазвичай здійснюється вашою юридичною командою, якій потрібно зв'язатися з відділами IT та безпеки, щоб переконатися, що всі політики, пов'язані з дотриманням нормативних вимог, відповідають вимогам законодавства.

Недотримання належного законодавства у EISP може мати серйозні наслідки, включаючи судові розгляди та/або розслідування з боку регуляторних органів. Недоліки також можуть призвести до жорстких штрафів, судових зборів, не кажучи вже про шкоду репутації як підприємству, яке прагне визнання на ринку.

Аварійне відновлення. Аварійне відновлення, яке також іноді називають плануванням безперервності бізнесу (BCP), стосується того, як служба інформаційної безпеки потенційно впорається з успішним зламом або атакою. Для цього потрібно буде попрацювати зі своїми партнерами з кібербезпеки, щоб визначити, як має відбуватися оцінка впливу на бізнес після інциденту безпеки, вимірюючи такі речі, як час простою та втрата даних після (і під час) сценарію катастрофи.

У політиці повинні бути прописані конкретні показники та цілі щодо того, скільки часу має знадобитися для відновлення системи, а також визначено, яка єдина точка відмови дозволила здійснити атаку. Після того, як вони будуть визначені, у політиці будуть викладені стратегії та тактики відновлення, які відповідатимуть цим цілям. Повинні бути включені такі речі, як процедури

відновлення, дерева викликів, критерії ініціювання дій і обсяг дій для кожної ролі співробітника, щоб гарантувати, що системи та/або дані будуть відновлені якомога швидше після порушення.

Ці дії часто виконуються командою, яка підпорядковується головному технічному директору, директору з управління ризиками або безпосередньо генеральному директору організації. Однак команда з інформаційної безпеки також підтримуватиме діяльність, оскільки вона є критично важливою зацікавленою стороною в будь-якому EISP.

Фізична охорона. Елемент фізичної та екологічної безпеки EISP має вирішальне значення для захисту активів організації від *фізичних* загроз. Сюди входять такі речі, як комп'ютери, приміщення, медіа, люди та паперові/фізичні дані. У зв'язку з цим зазвичай виділяються такі обов’язкові засоби контролю:

- відеоспостереження;
- вогнегасники;
- водяні спринклери;
- детектори диму;
- системи управління будівлею (BMS);
- фізичні замки;
- охоронці;
- достатнє освітлення;
- картки контролю доступу, що видаються співробітникам.

Усі фізичні простори підприємства *мають* бути класифіковані на основі інформації, якою вони володіють, а засоби контролю мають бути розгорнуті на основі критичності та чутливості кожної області. Наприклад, у політиці може бути зазначено, що відвідувачам дозволено відвідувати лише спеціально відведені місця або що адміністратори не мають ключів до картотек із дуже конфіденційною інформацією, пов'язаною з кібербезпекою.

Області, що містять найважливіші дані, повинні вимагати кількох форм автентифікації відповідно до EISP. Це може бути що завгодно: від визначеного особистого PIN-коду до біометричних даних. Незалежно від того, які заходи

фізичної безпеки будуть вважатися доцільними, необхідно переконайтеся, що ці засоби контролю постійно вимірюються та перевіряються, щоб перевірити відповідність і готовність співробітників.

Керування ідентифікацією та доступом. Ще одним важливим елементом політики має бути спосіб ідентифікації працівників, які мають доступ до певних критично важливих систем і даних у вашій організації (наприклад, керування ідентифікацією та доступом). Це може бути комбінація будь-якої кількості речей, включаючи ім'я, вік, ідентифікаційний номер працівника, біометричні дані або будь-які інші форми особистої інформації, які вважаються доречними під час розробки політики. Це може бути доповнення до імен користувачів і паролів, які зазвичай потрібні персоналу для доступу до систем і даних.

Крім того, потрібно з'ясувати, які ролі співробітників матимуть доступ до яких типів інформації. Це може ґрунтуватися на таких ключових принципах, як найменші привілеї, необхідність знати та критично важливі бізнес-функції. Доступ до кожної ролі має бути чітко окреслений у політиці, а також запроваджено найкращий можливий рівень безпеки, щоб неправильні люди випадково (або навмисно) не потрапили в системи, які їм не слід використовувати.

Спеціалісти служби інформаційної безпеки підприємства повинні прописати у своїх процесах EISP щорічні перевірки, а також процедури на випадок, якщо неправильні люди отримають доступ до систем або даних, які вони не повинні. Як правило, про випадки несанкціонованого доступу слід негайно повідомляти ключовим зацікавленим сторонам у команді з інформаційної безпеки, при цьому в політиці прописані наслідки для користувачів, які навмисно це роблять.

Управління інцидентами. Звичайно, жоден EISC не обходиться без документації про те, як необхідно негайно реагувати на кіберзлам або інцидент. Потрібно визначити, які ключові співробітники входитимуть до команди з управління інцидентами, яка оцінюватиме технічні та бізнес-наслідки порушення, а також вживатиме заходів для локалізації та усунення.

Ще одне розширення управління безпекою ризиків, політика управління інцидентами, зосереджена на обмеженні шкоди від порушень, а також на зниженні ризику подібних порушень у майбутньому. Для більшості організацій політика управління інцидентами та реагування на них EISC включатиме наступні шість кроків:

- виявлення та ідентифікація інцидентів;
- сортування та аналіз інцидентів;
- стримування загрози;
- вирішення інцидентів;
- аналіз першопричин;
- повідомлення про інциденти.

Політика реагування на інциденти має слугувати для розробки засобів контролю безпеки, людей, процесів і технологій, які полегшують цей шестиетапний процес якомога швидше та ефективніше. Окрім внутрішнього персоналу, план реагування на інциденти може включати інші вимоги стекхолдерів, експертів з кіберкриміналістики, віртуальні команди та будь-яких інших, кого вважають за потрібне. Наприклад, бюджет підприємства може диктувати, що економічно вигідніше передати певні кроки на аутсорсинг постачальникам або постачальникам послуг. У зв'язку з цим добре розроблена політика управління інцидентами не тільки допоможе швидко усунути загрозу, але й зробить це економічно ефективним способом.

Навчання та обізнаність. Нарешті, постійне навчання та обізнаність, можливо, є найважливішим елементом EISP. Часто найслабшою ланкою виявляються не системи чи технології, а самі люди. Ось чому політика повинна ретельно окреслювати поточну програму навчання та програму та структуру обізнаності про безпеку , адаптовану до кожної окремої ролі та профілю співробітника підприємства. Саме тут важливо зі всіма, щоб розробити режими навчання, які найкраще підходять персоналу. Навчальна політика може складатися з аудиторних занять, вікторин, онлайн-тренінгів, семінарів, імітації «протипожежних тренувань» та багатьох інших тактик, які можна

використовувати. Крім того, те, як адаптувати нових співробітників, оцінюючи їхню початкову обізнаність і заповнюючи будь-які прогалини, має бути у EISP. Навчання та обізнаність є частиною політики та стандартів оцінювання співробітників підприємства, щоб у людей був стимул виконувати те, чому вони були навчені. Члени команди безпеки повинні мати цілі, пов'язані з проходженням навчання та/або сертифікацією, при цьому показники всебічної обізнаності про безпеку постійно оцінюються.

Корпоративна кібербезпека – це архітектура, протоколи та інструменти, які використовуються для захисту корпоративних активів, як внутрішніх, так і в Інтернеті, від кібератак всередині підприємства та за його межами.

Корпоративна кібербезпека відрізняється від загальної кібербезпеки тим, що сучасні підприємства мають складну інфраструктуру, яка вимагає сильної політики безпеки, постійних оцінок та ефективного управління для уникнення інцидентів безпеки.

Архітектура безпеки інформаційної системи визначає структуру, протоколи, моделі та методи, необхідні для захисту даних, які система збирає, зберігає та обробляє.

Архітектура безпеки є основою корпоративної архітектури, оскільки вона оцінює та покращує безпеку та конфіденційність. Без належних заходів безпеки вся інфраструктура підприємства, а отже, і весь бізнес, опиняється під загрозою.

Майже на кожному підприємстві, яке піклується про захист інформації відпрацьовуються *Положення про комерційну таємницю* (далі "Положення") - внутрішній документ компанії, створений для організації роботи з конфіденційною інформацією серед працівників компанії та її контрагентів, а також для запровадження заходів захисту такої інформації від несанкціонованого доступу третіх осіб (Додаток А).

Комерційна таємниця - це режим конфіденційності інформації, що дозволяє компанії при існуючих чи можливих обставинах збільшити доходи, уникнути невиправданих витрат, зберегти положення на певному ринку товарів і послуг або отримати будь-яку іншу комерційну вигоду.

Це Положення є внутрішнім локальним нормативно-правовим актом, яким встановлюється:

1) сукупність організаційних заходів, спрямованих на створення режиму захисту такої інформації (наприклад, встановлення технічних засобів захисту комерційної таємниці);

2) перелік інформації, що визнається комерційною таємницею (такий перелік відображається безпосередньо у тексті Положення або в окремому додатку до нього);

3) порядок доступу і роботи працівників із такою інформацією та перелік їх обов'язків;

4) порядок надання доступу до комерційної таємниці державним органам та контрагентам або діловим партнерам; а також

5) порядок роботи і захисту комерційної таємниці, отриманою компанією від третіх осіб.

Компанія в обов'язковому порядку має затвердити перелік посад, які матимуть доступ до комерційної таємниці. Вказаний перелік визначається або у тексті цього Положення, або в окремому додатку до нього. За загальним правилом керівник компанії та головний бухгалтер мають вільний доступ до будь-якої конфіденційної інформації за посадою.

Ще одним важливим моментом є визначення щодо кожної окремої посади виду та типу відомостей, що становлять комерційну таємницю, до яких надаватиметься доступ. Перелік конфіденційної інформації, до якої матиме доступ окремий працівник, вказується у його посадовій інструкції, в трудовому договорі або в окремому договорі про нерозголошення комерційної таємниці, який укладається з працівником.

Працівник втрачає наданий йому доступ до комерційної таємниці у наступних ситуаціях:

1) припинення трудового договору (за ініціативою працівника, за ініціативою роботодавця або за згодою сторін);

2) відсторонення працівника від посади на підставі відповідного наказу;

3) видача керівником компанії наказу, яким працівник позбавляється доступу до комерційної таємниці;

4) видача керівником компанії наказу, яким посада виключається із переліку посад, яким надається доступ до комерційної таємниці;

5) переведення працівника на іншу посаду, яка не передбачає доступу до комерційної таємниці, на підставі окремого наказу тощо.

У випадку розголошення комерційної таємниці працівником, останній може бути притягнутий до дисциплінарної (звільнення, догана), матеріальної, кримінальної або адміністративної відповідальності. Кожен працівник, який отримує доступ до комерційної таємниці, має бути обов'язково ознайомлений із текстом цього Положення, що підтверджується особистим підписом працівника в спеціальному журналі.

Під час здійснення підприємницької діяльності компанія надає доступ до комерційної таємниці не лише своїм працівникам, але й контрагентам та діловим партнерам з якими веде спільний бізнес. Так, перед наданням партнерам фактичного доступу до конфіденційної інформації з такими особами мають бути укладені відповідні договори про нерозголошення комерційної таємниці.

Окрім цього, партнери і контрагенти мають бути повідомлені про режим захисту комерційної таємниці, встановлений компанією, шляхом їх ознайомлення під підпис із цим Положенням. У випадку допущення партнером чи контрагентом розголошення комерційної таємниці, винна сторона може бути притягнута до цивільно-правової, адміністративної та кримінальної відповідальності.

Положення затверджується компанією (юридичною особою або фізичною особою-підприємцем) та визначає порядок організації роботи з комерційною таємницею працівниками, а також контрагентами і державними органами, які отримують на законних підставах доступ до такої інформації.

Положення є внутрішнім локальними нормативно-правовим актом, а його дія розповсюджується на:

1) ВСІХ працівників компанії, які отримують доступ до комерційної таємниці у зв'язку із виконанням своїх посадових обов'язків за трудовими договорами;

2) а також на ВСІХ партнерів і контрагентів, з якими підприємство, організація чи компанія обмінюються комерційною таємницею для спільного ведення бізнесу, укладення договорів та угод.

Працівники, які отримали доступ до комерційної таємниці, керуються цим Положенням при роботі з отриманою конфіденційною інформацією (наприклад, використовують лише визначені Положенням спеціальні канали для передачі зв'язку, дотримуються обов'язку щодо зберігання секретних документів у сейфі тощо). Порядок надання доступу працівникам до комерційної таємниці описаний у секції "Порядок надання доступу працівникам до комерційної таємниці" вище. Порядок надання доступу контрагентам та діловим партнерам до комерційної таємниці підприємства описаний у секції "Порядок надання доступу партнерам/контрагентам до комерційної таємниці" вище.

Документ обов'язково затверджується відповідним наказом керівника компанії та набуває чинності від дати його затвердження. Положення діє впродовж необмеженого строку - тобто до моменту його скасування на підставі відповідного наказу.

Текст Положення має бути доступним для ознайомлення з ним всіма працівниками та партнерами компанії в будь-який момент. У зв'язку із чим компанія може роздати по одному примірнику такого Положення кожному працівнику та/або партнеру, або ж направити це Положення у вигляді електронного файлу на електронну адресу працівника/партнера.

Таким чином, корпоративна політика інформаційної безпеки підприємства є найважливішим внутрішнім документом, який повинен бути з точки зору інформаційної та кібербезпеки. Від безпеки мережі та додатків до управління інцидентами та постійного навчання, не потрібно забувати, що EISC є «живим документом», який слід постійно переглядати, переглядати та переглядати.

Також існують труднощі при створенні EISA. Розробка оптимальної

стратегії EISA може бути складною, особливо коли діють такі загальні фактори:

- відсутність комунікації та координації між різними відділами чи командами, коли йдеться про управління ризиками та підтримку IT-безпеки;
- нездатність чітко сформулювати цілі EISA;
- відсутність розуміння серед користувачів та зацікавлених сторін необхідності пріоритезації інформаційної безпеки;
- складність розрахунку вартості та рентабельності інвестицій програмних засобів захисту даних;
- брак фінансування для належного вирішення питань безпеки;
- невдоволення раніше розробленими заходами безпеки, як-от фільтрацією спаму, яка позначає дійсну та критичну кореспонденцію;
- попередні невиконання нормативних вимог або бізнес-цілей;
- занепокоєння з приводу неефективності попередніх інвестицій в IT-безпеку.

Наступні 5 кроків допоможуть розробити ефективну EISA:

1. Оцініть свою поточну ситуацію з безпекою. Визначте процеси та стандарти безпеки, за якими зараз працює ваша організація. Потім проаналізуйте, де не вистачає положень безпеки для різних систем і як їх можна покращити.

2. Проаналізуйте інсайти безпеки (стратегічні та технічні). Зв'яжіть статистику, отриману на кроці 1, зі своїми бізнес-цілями. Обов'язково включіть як технічні заходи, так і контекст стратегії, щоб визначити пріоритети ваших зусиль.

3. Розробити логічний рівень безпеки архітектури. Щоб створити логічну архітектуру для EISA на основі найкращих практик безпеки, використовуйте встановлену структуру для призначення елементів керування з високим пріоритетом.

4. Спроектуйте реалізацію EISA. Перетворіть логічний шар на дизайн, який можна реалізувати. Ґрунтуючись на вашому досвіді, ресурсах і стані ринку, вирішіть, які елементи розробляти власними силами, а якими речами повинен

керувати постачальник.

5. Ставтеся до архітектури як до безперервного процесу. Оскільки ландшафт загроз, ваше IT-середовище, ринок рішень і рекомендації щодо найкращих практик постійно змінюються, обов'язково періодично переглядайте та переглядайте свою архітектуру інформаційної безпеки.

При створенні EISA не потрібно починати з нуля. Замість цього покладіться на одну з декількох концепцій, розроблених за останнє десятиліття, щоб створити ефективну EISA. Налаштуйте його за потреби, щоб переконатися, що він працює для вашої унікальної організації.

Основні фреймворки EISA перераховані нижче.

Структура архітектури Open Group (TOGAF). TOGAF вперше надає набір інструментів для створення архітектури безпеки підприємства з нуля. Це допоможе вам визначити чіткі цілі та подолати розрив між різними рівнями EISA. Крім того, фреймворк можна адаптувати, щоб підтримати вас, коли потреби вашої організації в безпеці змінюються.

Шервудська прикладна архітектура безпеки бізнесу (SABSA). SABSA – це методологія для EA та EISA. Він часто використовується з іншими процесами, такими як COBIT 5.

COBIT 5, розроблений ISACA, є детальним фреймворком, який допомагає організаціям будь-якого розміру керувати та захищати IT-інфраструктуру. Він охоплює бізнес-логіку, ризики та вимоги до процесів.

Структура архітектури Міністерства оборони США (DoDAF). DoDAF призначений не лише для державних установ. Оскільки він пов'язує операції з інформаційною безпекою, він ідеально підходить для того, щоб допомогти багатопрофільним організаціям із незалежними IT-мережами вирішувати проблеми сумісності. Він зосереджений на візуалізації інфраструктури для різних зацікавлених сторін на підприємстві.

Федеральна структура архітектури підприємства (FEAF). FEAF є еталонною архітектурою підприємства для федерального уряду США. Вона була розроблена, щоб допомогти федеральним агентствам розпізнати пріоритетні

сфери та побудувати загальну ділову практику, незважаючи на їхні унікальні потреби, цілі, операції та діяльність. Він може допомогти як державним установам, так і приватним організаціям з EISA, а також EA.

Фреймворк Захмана (Zachman Framework) – це високорівневий фреймворк, який часто використовується для створення EA, але він також може бути перетворений на підхід EISA зверху вниз. Ґрунтуючись на шести фундаментальних питаннях – що, як, коли, хто, де і чому – він має шість рівнів: ідентифікація, визначення, представлення, специфікація, конфігурація та створення екземпляра.

Вибір найбільш підходящого фреймворка для організації інформаційної безпеки підприємства залежить від конкретних потреб, цілей та особливостей самої організації. Кожен з цих фреймворків має свої переваги та специфічні характеристики. Важливо враховувати особливості організації, галузі її діяльності та конкретні бізнес-вимоги при виборі фреймворка для організації інформаційної безпеки. Також може виявитися корисним комбінувати різні фреймворки для досягнення комплексного покращення інформаційної безпеки.

ВИСНОВКИ до третього розділу. За методикою, розробленою в п. 2.2. (рис. 2.4) сформовані пропозиції керівництву підприємства для забезпечення ефективності системи інформаційної безпеки, які включають організаційні, технічні та нормативно-правові заходи.

Комплексне застосування перерахованих фреймворків дозволяє активно планувати заходи інформаційної безпеки та якісно будувати систему захисту інформації на підприємстві.

Сформований комплекс критеріїв і метрик оцінювання ефективності реалізації заходів інформаційної безпеки та відпрацьований перелік заходів визначення ефективності інформаційної безпеки на підприємстві та їх зміст дозволяють якісно проводити аудит системи інформаційної безпеки на підприємстві, постійний моніторинг стану безпеки інформації.

Розроблені рекомендації керівниками підприємств та керівниками підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки та ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ з урахуванням особливостей функціонування підприємства дозволить підвищити ефективність системи інформаційної безпеки підприємства.

ВИСНОВКИ

Розглянуті аспекти впровадження заходів планування інформаційної безпеки, моніторингу їхньої ефективності та формулювання конкретних рекомендацій мають на меті створення ефективної системи захисту інформації. На основі проведеного аналізу основних понять, моделей і методів планування інформаційної безпеки підприємства, основних нормативно-правових документів з планування інформаційної безпеки, які розроблені вітчизняними та зарубіжними організаціями інформаційної безпеки, сформовані удосконалені підходи до планування та реалізації заходів інформаційної безпеки, які включають

Відпрацьований перелік заходів визначення ефективності інформаційної безпеки на підприємстві та їх зміст дозволяють керівникам структурних підрозділів інформаційної безпеки оцінювати стан системи інформаційної безпеки підприємства. Запропонований порядок впровадження заходів інформаційної безпеки на основі інтеграції обраної методики планування в організаційну структуру підприємства, ґрунтується на застосуванні передових технік та механізмів, розроблених міжнародними організаціями інформаційної безпеки.

На основі аналізу компонентів планування інформаційної безпеки визначена нова удосконалена методика планування інформаційної безпеки, розроблена на основі вивчених підходів, яка передбачає системний аналіз потреб, ризиків та ресурсів підприємства. Вона включає етапи формування стратегії, визначення метрик ефективності, розроблення плану заходів та систему моніторингу та оцінки. Методика, для забезпечення повноцінних інтегрованих заходів інформаційної безпеки, розглядає всі аспекти, від технічних аспектів до людського фактору. Вона покликана бути гнучкою та адаптивною, щоб враховувати зміни в кіберзагрозах, технологічних парадигмах та стратегічних цілях підприємства. Розроблена методика дозволить підприємствам ефективно і системно підходити до планування і реалізації заходів інформаційної безпеки, забезпечуючи високий рівень захисту та

враховуючи всі необхідні аспекти цього складного процесу.

Вперше сформований комплекс критеріїв і метрик оцінювання ефективності реалізації заходів інформаційної безпеки та ключові показники дозволяють якісно оцінювати та визначати успішність стратегій, вчасно виявляти можливі недоліки.

Розроблені рекомендації керівниками підприємств та керівникам структурних підрозділів інформаційної безпеки для відпрацювання Політики інформаційної безпеки та ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ з урахуванням особливостей функціонування підприємства, що значно підвищить ефективність запланованих заходів інформаційної безпеки на підприємстві та буде сприяти підвищенню культури безпеки серед персоналу і зменшенню внутрішніх загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. General Data Protection Regulation. https://gdpr-info.eu/ (дата звернення: 16.12.2023).

2. Talimonchik V. Legal Aspects of International Information Security. In book: Contemporary Issues in Digital Ethics. pp. 1-15. URL: https://doi.org/10.5772/intechopen.86119.

3. Mazhorina M. Network paradigm of private international law: concept contouring. Actual Problems of Law. № 57(2019). pp. 140-159. URL: https://doi.org/10.17803/1994-1471.2019.101.4.140-159.

4. Про інформацію: Закон України від 02.10.1992 р. 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text. (дата звернення 22.11.2023 р.)

5. Про Національну програму інформатизації: Закон України від 01.03.2023. №2807-IX, чинний, URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення 25.11.2023 р.).

6. Про захист інформації в інформаційно-комунікаційних системах: Закон України (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286) Редакція від 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 26.11.2023 р.).

7. Про основні засади забезпечення кібербезпеки України: Закон України. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 26.11.2023 р.).

8. Про захист персональних даних: Закон України. (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 27.11.2023 р.).

9. Василенко В. В. Підходи до планування і реалізації заходів інформаційної безпеки на підприємстві. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2023 року). Навчально-науковий інститут захисту інформації, Державний університет інформаційно-комунікаційних технологій . Київ, 2023. с. 51-53.

10. Чунарьова А., Чунарьов А. Система управління інформаційною

безпекою на базі міжнародних стандартів серії ISO. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. С. 48-52.

11. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. - 2010. - № 3. - С. 123-129. - Режим доступу: http://nbuv.gov.ua/UJRN/econpr_2010_3_20. (дата звернення 27.11.2023 р.).

12. Kozhedub Y.. Implementation of the process approach to managing risks of information security in the nist documents. *Information Technology and Security*. July-December 2017. Vol. 5. Iss. 2 (9). pp. 76-89. https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2%289%29_09.pdf (дата звернення 27.11.2023 р.).

13. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 27.11.2023 р.).

14. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс]– Режим доступу : URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2 010_2_2/032-035.pdf. (дата звернення 27.11.2023 р.).

15. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. Державна безпека України. – 2011. – № 21. – С. 92–95.

16. Chernysh Iryna. Управління інформаційною безпекою підприємства в умовах динамічного бізнес-середовища. Науковий журнал «Економіка і регіон». – Полтава: ПНТУ, 2020. – Т. 1(76). – С. 106-112. URL: https://doi.org/10.26906/EiR.2020.1(76).1924.

17. Rusina Yu. O., Ostriakova V. Yu. Udoskonalennia systemy upravlinnia informatsiinoiu bezpekoiu na pidpryiemstvi. Mizhnarodnyi naukovyi zhurnal "Internauka". – 2017. – №14. С. 135-139. URL: https://doi.org/10.25313/2520-2057-2017-14.

18. Тацюра М. Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства. Матеріали Другої наук.-практ. конф. "Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях" 23–24 вересня 2010 року, м. Бахчисарай, НДІ сталого розвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана . – Сімферополь : Фенікс, 2010. – С. 451–453.

19. Архипов О.Є, Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах. Інформаційна безпека людини, суспільства, держави: науково-практ.журнал. Національна академія Служби безпеки України. – 2010. – №2(4).– С.62-65.

20. Архипов О.Є., Муратов О.Є. Про зміст та взаємозв’язок понять "інформаційна безпека" та "безпека інформації". Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф., 17 березня 2010 р., м. Київ. – К.: Наук.-вид. Відділ НА СБ України, 2010. – С.185-187.

21. Миколюк О.А., Бобровник В.М Особливості інформаційного забезпечення управління підприємством. Економічні науки. Вісник Хмельницького національного університету 2021, № 3. С. 48-52 URL: https://doi.org/10.31891/2307-5740-2021-294-3-7

22. Петренко С.М. Інформаційне забезпечення внутрішнього контролю господарських систем: монографія / С.М. Петренко Донецьк: ДонНУЕТ, 2007. − 290 с.

23. Череп А.В., Панченко О.М., Птіцина Л.А. Інформаційне забезпечення в системі управління промисловим підприємством: монографія. Запоріжжя: Запорізький національний університет, 2014. − 266 с

24. Фостолович В.А. Інформаційно-аналітична база в інтегрованій системі управління підприємством. Проблеми економічного, облікового, контрольного і аналітичного забезпечення управління підприємством: матеріали II Всеукр. наук.-практич. конф. молод. учених, 8 грудня 2016 року − Вінниця. − «Едельвейс і К». С.179-181.

25. Бурик З.М., Огірко О.І. Інформаційні технології забезпечення сталого розвитку в контексті формування нової науково-технічної парадигми. Міжнародний науковий журнал «Інтернаука». 2017. № 1(2). С. 24–28. URL: http://nbuv.gov.ua/UJRN/mnj_2017_1%282%29__8 (дата звернення: 03.10.2023).

26. Правдюк А. Л., Прутська Т. Ю., Правдюк М. В. Інформаційне забезпечення управління підприємницькою діяльністю на засадах інституціоналізму: монографія.– Київ: «Центр учбової літератури». 2019. – 360с.

27. Sepideh Yeganegi, André O. Laplume, Parshotam Dass. The role of information availability: A longitudinal analysis of technology entrepreneurship, Technological Forecasting and Social Change, Vol. 170, 2021, 120910, URL: https://doi.org/10.1016/j.techfore.2021.120910.

28. Laplume A. O., Pathak S., Xavier-Oliveira E. The politics of intellectual property rights regimes: An empirical study of new technology use in entrepreneurship. Technovation. – 2014. – Т. 34. – №. 12. – С. 807-816. URL: https://doi.org/10.1016/j.technovation.2014.07.006

29. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological forecasting and social change. – 2020. – Vol.. 150. – p. 119791. URL: https://doi.org/10.1016/j.techfore.2019.119791

30. Marzieh Shariati, Faezeh Bahmani, Fereidoon Shams, Enterprise information security, a review of architectures and frameworks from interoperability perspective, Procedia Computer Science, Vol. 3, 2011, Pages 537-543. URL: https://doi.org/10.1016/j.procs.2010.12.089.

31. Menzel M., Thomas I., Meinel C. Security requirements specification in service-oriented business process management. 2009 International Conference on Availability, Reliability and Security. – IEEE, 2009. – pp. 41-48. URL: https://doi.org/10.1109/ARES.2009.90.

32. Stephenson P. S-TRAIS: A Method for Security Requirements Engineering Using a Standards Based Network Security Reference Model. Conference Proceedings from SREIS. – 2005. С. 44-51.

33. К. Волтер, М. Менцель, А. Шаад, Ф. Місельдін, К. Майнель. Специфікація вимог безпеки бізнес-процесів на основі моделі. Журнал системної архітектури 55, № 4. 2009. С. 211-223. URL: https://doi.org/10.1016/j.sysarc.2008.10.002.

34. Lakomaa E., Kallberg J. Open data as a foundation for innovation: The enabling effect of free public sector information for entrepreneurs. IEEE Access. – 2013. – Vol. 1. – pp. 558-563. URL: https://doi.org/10.1109/ACCESS.2013.2279164.

35. Kondakci S. Analysis of information security reliability: A tutorial, Reliability Engineering & System Safety, Volume 133, 2015, Pages 275-299, URL: https://doi.org/10.1016/j.ress.2014.09.021.

36. Waseem Ahmed, Yong Wei Wu, A survey on reliability in distributed systems, Journal of Computer and System Sciences, Volume 79, Issue 8, 2013, Pages 1243-1255, URL: https://doi.org/10.1016/j.jcss.2013.02.006.

37. Yaghlane A., Azaiez M. Systems under attack-survivability rather than reliability: Concept, results, and applications, European Journal of Operational Research, Volume 258, Issue 3, 2017, Pages 1156-1164, URL: https://doi.org/10.1016/j.ejor.2016.09.041.

38. Pooley J. Chapter 1 - Information Security in the Modern Enterprise, Editor(s): John R. Vacca, Computer and Information Security Handbook (Third Edition), Morgan Kaufmann, 2017, Pages 3-11, URL: https://doi.org/10.1016/B978-0-12-803843-7.00001-6.

39. Bieńkowska A., Tworek K., Zabłocka-Kluczka A. IT Reliability and Its Influence on the Results of Controlling: Comparative Analysis of Organizations Functioning in Poland and Switzerland. Information Systems Management 37:1, 2020. pages 33-51. URL: https://doi.org/10.1080/10580530.2020.1696545.

40. Tworek K.. IT Reliability for Ensuring Performance of IT Used in Organizations Operating under Covid-19 Epidemic Crisis. Central European Business Review 2021.10:1, pages 39-53. URL: https://doi.org/10.18267/j.cebr.255.

41. Bieńkowska A., Tworek K. Zabłocka-Kluczka A.. Moderating Role of User Experience and IT Reliability in Controlling Influence on Job Performance and

Organizational Performance. E+M Ekonomie a Management 24:1, pages 66-83. 2021. URL: https://doi.org/10.15240/tul/2021-1-005.

42. Tworek, K. User Experience Influence on Reliability of IT in Organization in the Context of Job Characteristics. Central European Business Review, 8(1), 33-49. 2019. URL: https://doi.org/10.18267/j.cebr.210

43. Iulian D. Toader, Permanence as a principle of practice, Historia Mathematica, Volume 54, 2021, Pages 77-94, URL: https://doi.org/10.1016/j.hm.2020.08.001.

44. Abbasi M., Khosravi M. R., Ramezani A. Intelligent resource management at the network edge using content delivery networks. Enterprise Information Systems 17:5. 2023. https://doi.org/10.1080/17517575.2022.2037159.

45. Gupta B., Dharma P. Agrawal. Security, privacy and forensics in the enterprise information systems, Enterprise Information Systems, 15:4, 445-447, 2021. URL: https://doi.org/10.1080/17517575.2020.1791364.

46. Dhillon, G., Torkzadeh, G., Chang, J. Strategic Planning for IS Security: Designing Objectives. In: Chatterjee, S., Dutta, K., Sundarraj, R. (eds) Designing for a Digital and Globalized World. DESRIST 2018. Lecture Notes in Computer Science 2018. vol 10844. Springer, Cham. URL: https://doi.org/10.1007/978-3-319-91800-6_19/

47. Vincent LeVeque, Introduction in Information Security: A Strategic Approach, IEEE, 2006, pp.1-7, URL: https://doi.org/10.1109/9780471784340.ch1.

48. James Pooley, Chapter 1 - Information Security in the Modern Enterprise, Editor(s): John R. Vacca, Computer and Information Security Handbook (Third Edition), Morgan Kaufmann, 2017, Pages 3-11, URL: https://doi.org/10.1016/B978-0-12-803843-7.00001-6.

49. Onyshchenko, S., Hlushko, A., Maslii, O., Skryl, V. Risks and Threats to Economic Security of Enterprises in the Construction Industry Under Pandemic Conditions. In: Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (eds) Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020.

Lecture Notes in Civil Engineering, vol 181. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-85043-2_66/.

50. Chen H, Chau M, Li S-H. Enterprise risk and security management: data, text and Web mining. Decis Support Syst 50(4):649–650. 2011. URL: https://doi.org/10.1016/j.dss.2010.08.026/.

51. Pooley J. Information security in the modern enterprise. Computer and information security handbook. Elsevier, pp 3–11. 2017. URL: https://doi.org/10.1016/B978-0-12-803843-7.00001-6/.

52. Chase R. Is enterprise risk management (ERM) leaving security behind?, chap 10. In: Security leader insights for risk management, lessons and strategies from leading security professionals, pp 41–46. 2015. URL: https://doi.org/10.1016/B978-0-12-800840-9.00010-1/.

53. Kim S, Kim S, Lee G. Structure design and test of enterprise security management system with advanced internal security. Futur Gener Comput Syst 25(3):358–363. 2009. URL: https://doi.org/10.1016/j.future.2006.04.019.

54. Onyshchenko S, Yehorycheva S, Furmanchuk O, Maslii O. Ukraine construction complex innovation-oriented development management. Proceedings of the 2nd international conference on building innovations, pp 687–700. 2020. URL: https://doi.org/10.1007/978-3-030-42939-3_68.

55. Garoui, M. Safe-Platoon: A Formal Model for Safety Evaluation. International Journal of Software Science and Computational Intelligence (IJSSCI) 11 (2): 26–37. 2019. URL: https://doi.org/10.4018/IJSSCI.2019040102.

56. Ma, H., L. Zhang, Z. Liu, and E. Dong. Secure Deduplication of Encrypted Data in Online and Offline Environments. International Journal of High Performance Computing and Networking 14 (3): 294–303. 2019. URL: https://doi.org/10.1504/IJHPCN.2019.102129.

57. Stergiou, Christos. Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems 19 (2018): 174-184. URL: https://doi.org/10.1016/j.suscom.2018.06.003.

58. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection Information security management systems Requirements. URL: https://www.iso.org/standard/27001.

59. NISTCybersecurity Framework 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework.

60. Haes, Steven, Grembergen, Wim Joshi, Anant Huygh, Tim. COBIT as a Framework for Enterprise Governance of IT. In: Enterprise Governance of Information Technology. Management for Professionals. Springer, Cham. 2020. pp. 125-162. URL: https://doi.org/10.1007/978-3-030-25918-1_5.

61. Tabatha Farney. Library technology: Innovating technologies, services, and practices, College & Undergraduate Libraries, 27:2-4, 2020. pp. 51-55, DOI: URL: https://doi.org/10.1080/10691316.2020.1952776.

62. Moskalenko N. Critical issues of economic security of organizations. Економіка розвитку, 2016, 1: 69-76. URL: http://www.repository.hneu.edu.ua/jspui/handle/123456789/11078.

63. Litvinchuk I., Korchomnyi R., Korshun N., Vorokhob M., APPROACH TO INFORMATION SECURITY RISK ASSESSMENT FOR A CLASS «1» AUTOMATED SYSTEM. Cybersecurity Education Science Technique. 2. 98-112. 2020. URL: https://doi.org/10.28925/2663-4023.2020.10.98112.

64. Fedorenko V., Lytvyn N., Luchenko D., Panova I., Tsybulnyk N. Legal aspects of information security management in the conditions of ukraine's european integration. Journal of Security and Sustainability Issues. 2020. Vol. 10(2). pp. 477-489. URL: https://doi.org/10.9770/jssi.2020.10.2(9) .

65. Діллон, Г., Торкзаде, Г., Чанг, Дж. Стратегічне планування безпеки ІБ: розробка цілей. В: Чаттерджі, С., Датта, К., Сундарраджа, Р. (ред.) Проектування для цифрового та глобалізованого світу. DESRIST 2018. Конспект лекцій з інформатики, том 10844. Шпрінгер, Чам. URL: https://doi.org/10.1007/978-3-319-91800-6_19

66 Volchkov A. Key Performance Indicators for Security Governance, Part 1. Isaca journal Vol. 6. 2020. pp. 49-56. URL: https://www.isaca.org/resources/isaca-

journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1. (дата звернення 17.12.2023 р.)

ДОДАТКИ

ДОДАТОК А

ЗАТВЕРДЖЕНО
Наказом ФОП XXXXX № 12 від 9 грудня 2023 року

ПОЛОЖЕННЯ ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ

СТРУКТУРА ДОКУМЕНТА

1. ВИЗНАЧЕННЯ ПОНЯТЬ

"**Власник**" означає особу, яка володіє на законних підставах Комерційною таємницею та обмежила до неї Доступ третіх осіб шляхом запровадження відповідного Режиму комерційної таємниці.

"**Партнер**" або "**Партнери**" означає осіб, які **(1)** є стороною будь-яких цивільно-правових договорів чи угод, укладених з Підприємцем; або **(2)** ведуть переговори, співпрацюють або взаємодіють з Підприємцем в будь-який інший спосіб, в результаті чого мають доступ до Комерційної таємниці один одного.

"**Підприємець**" означає наступну фізичну особу: XXXXX, РНОКПП: _____, яка зареєстрована приватним підприємцем в Єдиному державному реєстрі за № _____.

"**Положення**" означає це Положення про комерційну таємницю, що затверджене наказом Підприємця № 12 від 9 грудня 2023 року з усіма наступними доповненнями та змінами.

"**Працівник**" означає фізичну особу, яка працевлаштована у штат для виконання певної трудової функції на підставі укладеного трудового договору у зв'язку із чим отримує Доступ до Комерційної таємниці.

"**Режим комерційної таємниці**" означає сукупність адміністративних, правових, технічних та організаційних заходів, розроблених Власником для захисту Комерційної таємниці від несанкціонованого доступу до неї третіх осіб.

"**Розголошення**" означає умисну чи без такого умислу дію чи бездіяльність Працівників та/або Партнерів, які **(1)** отримали попередньо Доступ до Комерційної таємниці; та/або **(2)**

випадково отримали доступ до Комерційної таємниці, внаслідок чого Комерційну таємницю було розголошено іншим Працівникам та/або Партнерам, які не мають Доступу, та/або будь-яким іншим третім особам.

"**Службове розслідування**" означає комплекс заходів, що здійснюється відповідно до цього Положення з метою повного, всебічного та об'єктивного з'ясування обставин вчинення Працівником чи Партнером Розголошення, виявлення причин та умов, що сприяли вчиненню Розголошення, а також встановлення інших подій, які потребують з'ясування.

2. ПРЕДМЕТ РЕГУЛЮВАННЯ

2.1. Це Положення розроблено у відповідності до норм Цивільного кодексу, Господарського кодексу, Закону України "Про інформацію", Постанови Кабінету Міністрів України № 611 від 9 серпня 1993 року "Про перелік відомостей, що не становлять комерційної таємниці", а також інших нормативно-правових актів.

2.2. Цим Положенням визначається перелік інформації, яка належить до Комерційної таємниці, порядок надання Доступу до неї, визначення особливостей функціонування Режиму комерційної таємниці, а також встановлення заходів відповідальності за Розголошення.

2.3. Дія цього Положення поширюється на **(1)** Працівників, **(2)** Партнерів та **(3)** Державні органи і спрямована на запобігання несанкціонованому розповсюдженню (Розголошенню) Комерційної таємниці.

2.4. Положення набуває юридичної сили від дати його затвердження Наказом, що зазначена вище, та діє без обмеження строку.

3. ІНФОРМАЦІЯ, ЩО НАЛЕЖИТЬ ДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ

3.1. Загальні положення

3.1.1. Комерційна таємниця, яка знаходиться у розпорядженні Підприємця, належить йому виключено на законних підставах, і отримана **(1)** в результаті самостійного проведення розробок, досліджень та/або підприємницької діяльності; **(2)** від Партнера на підставі окремо укладених договорів (угод) про нерозголошення комерційної таємниці; **(3)** від будь-яких інших третіх осіб на підставі договору чи закону.

3.1.2. Віднесення відомостей до Комерційної таємниці здійснюється у відповідності до принципів обґрунтованості та своєчасності. Обґрунтованість полягає у встановленні доцільності віднесення певних відомостей до Комерційної таємниці. Своєчасність полягає у встановленні обмежень на Розголошення відомостей з моменту їх отримання (розробки) або завчасно до вказаного моменту.

3.2. Визначення комерційної таємниці

3.2.1. Відповідно до умов цього Положення до Комерційної таємниці належатиме наступна інформація:

(1) інформація, яка отримана від Партнерів на підставі відповідних договорів (угод) про нерозголошення комерційної таємниці; та

(2) наступна інформація, яка належить Підприємцю:

_____

3.2.2. Перелік відомостей, що відноситься до Комерційної таємниці Підприємця, може бути змінений чи доповнений на підставі окремого наказу Підприємця.

3.3. Інформація, що не може бути віднесена до комерційної таємниці

3.3.1. Не можуть бути віднесені до Комерційної таємниці наступні відомості:

(1) установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;

(2) інформація за всіма встановленими формами державної звітності;

(3) дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

(4) відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;

(5) документи про сплату податків і обов'язкових платежів;

(6) інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

(7) документи про платоспроможність;

(8) відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

(9) відомості, що відповідно до чинного законодавства підлягають оголошенню.

4. ЗАПРОВАДЖЕННЯ РЕЖИМУ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

4.1. Загальні положення

4.1.1. Для цілей захисту Комерційної таємниці запроваджується спеціальний Режим комерційної таємниці, що включає:

(1) визначення вичерпного переліку відомостей, що становлять Комерційну таємницю.

(2) встановлення переліку осіб, які отримують Доступ.

(3) обмеження Доступу третіх осіб до Комерційної таємниці шляхом запровадження певних технічних засобів захисту та контролю.

(4) регулювання відносин щодо порядку використання Комерційної таємниці Працівниками у відповідних трудових договорах та договорах про нерозголошення комерційної таємниці.

(5) регулювання відносин щодо порядку використання Комерційної таємниці Партнерами у відповідних цивільно-правових договорах та договорах (угодах) про нерозголошення комерційної таємниці.

4.1.2. Щодо Комерційної таємниці Власником якої є Підприємець, Підприємець має виключне право здійснювати наступні дії:

(1) встановлювати, змінювати та скасовувати у письмовому вигляді Режим комерційної таємниці.

(2) використовувати Комерційну таємницю для власних потреб та/або для досягнення будь-яких інших цілей.

(3) надавати Доступ або обмежувати його, визначати порядок та умови такого Доступу для третіх осіб, Працівників та Партнерів.

(4) вимагати від Партнерів, Державних органів та Працівників, що отримали Доступ на законних підставах, дотримання обов'язків конфіденційності.

(5) вимагати від третіх осіб, які отримали Доступ випадково або в результаті помилки, дотримання вимог повної конфіденційності.

(6) захищати у встановленому законом порядку свої права у випадку Розголошення, незаконного отримання або незаконного використання третіми особами Комерційної таємниці, у тому числі вимагати відшкодування збитків, втраченої вигоди, а також притягнення до інших видів юридичної відповідальності винних осіб.

4.1.3. Щодо Комерційної таємниці Власником якої є Партнер, Підприємець має право здійснити наступні дії:

(1) надати Доступ окремим Працівникам, за умови укладення з ними попередньо відповідних договорів про нерозголошення комерційної таємниці.

(2) використовувати отриману Комерційну таємницю виключно у тих цілях, які письмово погоджені з Партнером.

(3) надати Комерційній таємниці, отриманій від Партнерів, захист аналогічний захисту Підприємцем власної Комерційної таємниці.

(4) дотримуватися вимог нерозголошення Комерційної таємниці впродовж строку, погодженого з Партнерами.

(5) після завершення співпраці та/або досягнення цілей чи мети, для якої Підприємцю надавався доступ до Комерційної таємниці Партнера, повернути назад їм всі матеріальні

носії, на яких розміщена Комерційна таємниці.

4.1.4. Знищення матеріальних та/або електронних носіїв, на яких міститься Комерційна таємниця, допускається лише за умови отримання попереднього письмового погодження від Власника.

4.2. Зберігання та поширення комерційної таємниці

4.2.1. У випадку збереження Комерційної таємниці на матеріальному носії, включаючи, однак не обмежуючись, фотографії, флешки, диски, дискети, таблиці, схеми, ескізи, малюнки, на таких носіях повинен бути в обов'язковому порядку проставлений гриф "Конфіденційно" із зазначенням ідентифікаційних даних Власника.

4.2.2. У випадку збереження Комерційної таємниці на електронному носії (документи, таблиці, малюнки, презентації і т.п.) у колонтитулі документа повинен бути проставлений напис "Комерційна таємниця" або "Конфіденційно" із зазначенням ідентифікаційних даних Власника.

4.2.3. Якщо Комерційна таємниця пересилається за допомогою електронних повідомлень (Інтернет, електронна пошта, месенджери), такі повідомлення в обов'язковому порядку повинні містити текст наступного змісту: "Це повідомлення та всі додатки до нього є конфіденційними і призначені виключно для використання отримувачем (адресатом), вказаним вище. Якщо Ви не є отримувачем цього повідомлення - негайно видаліть його із системи. Використання інформації, що міститься у цьому повідомленні, допускається лише із дотриманням вимог законодавства України про захист комерційної таємниці та укладених угод щодо захисту комерційної таємниці." Електронні повідомлення направляються лише з використанням захищених каналів зв'язку.

4.2.4. Підприємцем запроваджуються наступні технічні заходи захисту Комерційної таємниці:

_____

5. ПОРЯДОК ДОСТУПУ ПРАЦІВНИКІВ ДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ

5.1. Загальні положення

5.1.1. Працівники, які займають наступні посади, отримують Доступ:

_____

Вид відомостей та тип інформації, що становлять Комерційну таємницю, а також обсяг Доступу до них визначається договорами (угодами) про нерозголошення комерційної таємниці або посадовою інструкцією Працівника або будь-якими іншими внутрішніми локальними нормативно-правовими актами.

5.1.2. Перелік посад, які мають Доступ, може бути змінений чи доповнений на підставі Наказу Підприємця.

5.1.3. Працівник отримує Доступ шляхом **(1)** ознайомлення такого Працівника із текстом цього Положення, що підтверджується особистим підписом Працівника у відповідному журналі, в якому фіксується факт ознайомлення працівників із Режимом комерційної таємниці; та **(2)** підписання відповідного договору про нерозголошення комерційної таємниці.

5.1.4. Працівник втрачає Доступ в одному з наступних випадків: **(1)** припинення трудового договору; або **(2)** переведення Працівника на іншу посаду/роботу, де Доступ не вимагається; або **(3)** притягнення Працівника до дисциплінарної відповідальності за факт порушення обов'язків з нерозголошення Комерційної таємниці, передбачених цим Положенням, договором про нерозголошення комерційної таємниці з Працівником або будь-якими іншими внутрішніми локальними нормативно-правовими актами; або **(4)** за окремою ініціативою Підприємця; або **(5)** у випадку виключення назви посади, яку займає Працівник, із переліку посад, які отримують Доступ; або **(6)** у випадку відсторонення Працівника від виконання його трудових обов'язків на підставі окремого наказу.

5.2. Обов'язки працівників

5.2.1. Працівник, який отримав доступ, зобов'язується дотримуватися наступних правил:

(1) не допускати Розголошення без попередньої письмової згоди, отриманої від Підприємця.

(2) дотримуватися норм, правил та приписів, що стосуються Режиму комерційної таємниці, встановлених внутрішніми локальними нормативно-правовими актами.
(3) використовувати Комерційну таємницю виключно для виконання трудових обов'язків та поставлених завдань.
(4) негайно повідомляти Підприємця про факт Розголошення та/або про спроби несанкціонованого доступу третіх осіб до Комерційної таємниці.
(5) у випадку припинення трудового договору негайно повернути безпосередньому керівнику всі без виключно носії, на яких розміщена Комерційна таємниця і які знаходяться у розпорядженні Працівника.
(6) впродовж всього строку дії трудових відносин і впродовж певного строку після припинення трудового договору, передбаченого окремими договорами про нерозголошення комерційної таємниці, не допускати Розголошення або використання Комерційної таємниці в особистих цілях або в інтересах третіх осіб, включаючи, проте не обмежуючись, у трудовий або підприємницькій діяльності, при написанні наукових або будь-яких публіцистичних робіт, під час публікацій у мережі Інтернет або ЗМІ.
(7) не виносити носії, на яких розміщена Комерційна таємниця, за межі робочого місця Працівника.
(8) не допускати інших Працівника або Партнерів, які не мають Доступ, до Комерційної таємниці.
(9) повертати безпосередньому керівнику будь-які матеріальні носії з Комерційною таємницею перед відпусткою, лікарняним, декретом та/або службовим відрядженням.
(10) дотримуватися встановленого порядку роботи та зберігання документів, які містять Комерційну таємницю.
(11) забезпечувати схоронність Комерційної таємниці.
(12) повідомляти негайно про втрату або недостачу документів, що містять Комерційну таємницю, посвідчень, перепусток, ключів від приміщень, сейфів, особистих печаток, печаток та штампів, а також про причини і умови можливої втрати таких відомостей.
(13) не проводити службові міжміські або міжнародні переговори, розмови або листування з використанням незахищених каналів зв'язку.

5.2.2. Власником Комерційної таємниці, створеної у результаті виконання Працівником своїх посадових обов'язків за трудовим договором, є Підприємець.
5.2.3. Працівник має право працювати лише з тим обсягом інформації, що становить Комерційну таємницю, до якої ним було отримано попередній Доступ.

5.3. Відповідальність працівників за розголошення

5.3.1. В разі встановлення факту Розголошення з вини Працівника, Працівник може бути притягнутий до дисциплінарної, матеріальної, кримінальної або адміністративно-правової відповідальності у порядку, встановленому чинним законодавством України, а також внутрішніми локальними нормативно-правовими актами.
5.3.2. Дисциплінарна відповідальність застосовується до Працівника у вигляді сурової догани або звільнення з відповідних підстав. Працівник має бути ознайомлений з наказом про притягнення його до дисциплінарної відповідальності під особистий підпис.
5.3.3. Матеріальна відповідальність застосовується до Працівника у вигляді відшкодування прямих збитків у повному обсязі, спричинених Підприємцю таким Розголошенням. Компенсація завданих збитків Працівником може бути проведена у добровільному порядку або на підставі рішення суду.

6. ПОРЯДОК ДОСТУПУ ПАРТНЕРІВ ДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ

6.1. Загальні положення

6.1.1. Партнер отримує Доступ до Комерційної таємниці Підприємця у результаті **(1)** укладення відповідного цивільно-правового договору з Підприємцем; або **(2)** у результаті початку перемовин про можливу/потенційну співпрацю або щодо укладення певного цивільно-правового договору.

6.1.2. Партнер отримує фактичний Доступ лише після **(1)** укладення відповідного договору (угоди) про нерозголошення комерційної таємниці з Підприємцем; та **(2)** його ознайомлення з текстом цього Положення, що підтверджується особистим підписом Партнера або його законного представника у відповідному журналі, в якому фіксується факт ознайомлення партнерів із Режимом комерційної таємниці.

6.1.3. Партнер, який отримав Доступ, зобов'язується:

(1) не допускати Розголошення без отримання попередньої письмової згоди від Власника.

(2) використовувати отриману Комерційну таємницю виключно для досягнення цілей та задач, для яких така інформація надається Партнеру.

(3) повідомити негайно внутрішніх працівників Партнера, які будуть мати Доступ, про конфіденційний статус такої інформації, про заборону її Розголошення, а також укласти з ними відповідні окремі договори (угоди) про нерозголошення комерційної таємниці.

(4) не проводити службові міжміські або міжнародні переговори, розмови або листування з використанням незахищених каналів зв'язку.

(5) повідомити негайно Підприємця про всі відомі Партнеру факти Розголошення та/або спробах третіх осіб отримати несанкціонований доступ до Комерційної таємниці.

6.1.4. Партнер, якому наданий Доступ, зобов'язується не допускати Розголошення та дотримуватися Режиму комерційної таємниці впродовж строку, встановленого відповідним договором (угодою) про нерозголошення комерційної таємниці, що укладена між Партнером та Підприємцем.

6.2. Відповідальність партнерів за розголошення

6.2.1. У випадку встановлення факту вчинення Партнером Розголошення, такий Партнер може бути притягнутий до цивільно-правової, адміністративної або кримінальної відповідальності у порядку, передбаченому чинним законодавством України.

6.2.2. Цивільно-правова відповідальність застосовується до Партнера у вигляді відшкодування ним прямих збитків та упущеної вигоди, заподіяних Підприємцю у добровільному порядку або на підставі відповідного судового рішення.

7. НАДАННЯ ДОСТУПУ ДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ ДЕРЖАВНИМ ОРГАНАМ

7.1. Підприємець зобов'язується на мотивовану вимогу Державного органу надати йому безкоштовно Доступ. Мотивована вимога повинна бути підписана повноважною посадовою особою, містити цілі та правові підстави витребування такого Доступу, перелік інформації, до якої потрібно надати Доступ, а також строк, на який має бути наданий Доступ.

7.2. Перед отриманням фактичного Доступу представник Державного органу має взяти на себе зобов'язання з недопущення Розголошення, що підтверджується підписом уповноваженого представника у відповідному журналі, в якому фіксується факт ознайомлення третіх осіб з Режимом комерційної таємниці.

7.3. У випадку відмови у наданні Доступу Державному органу, Державний орган має можливість отримати такий Доступ на підставі відповідного рішення суду.

8. СЛУЖБОВІ РОЗСЛІДУВАННЯ

8.1. Службове розслідування проводиться з наступних підстав:

(1) повідомлення про факт Розголошення, що отримано від Працівника, Партнера, посадових осіб.

(2) анонімне повідомлення, отримане від третіх осіб, що дає підстави вважати про настання обставин Розголошення.

(3) безпосереднє виявлення факту Розголошення Підприємцем.

8.2. Рішення щодо проведення службового розслідування приймається особисто Підприємцем і оформлюється відповідним наказом.

У тексті наказу також визначається **(1)** голова комісії з проведення Службового розслідування; **(2)** члени комісії з Службового розслідування; **(3)** предмет проведення Службового

розслідування, дата його початку та завершення.
8.3. Голова комісії з Службового розслідування здійснює загальне координування Службового розслідування, надає усні та письмові доручення членам комісії, які є обов'язковими до виконання. Комісія із Службового розслідування (далі "**Комісія**") підконтрольна безпосередньо Підприємцю.
8.4. До участі у проведенні Службового розслідування, а також до складу членів комісії не можуть бути залучені особи, які є підозрюваними у вчиненні Розголошення та/або якщо певні обставини свідчать про їх безпосередню заінтересованість у результатах Службового розслідування.
8.5. Організаційною формою діяльності Комісії є засідання.
8.6. Якщо Службове розслідування проводиться відносно Працівника, в такому випадку такий Працівник має бути в обов'язковому порядку відсторонений від роботи на підставі окремого наказу на весь період проведення такого Службового розслідування.
8.7. За результатами проведення Службового розслідування Комісією складається відповідний акт, який підписується всіма членами Комісії, і в якому зазначаються: **(1)** факти, що стали підставою для проведення Службового розслідування; **(2)** пояснення та зауваження осіб, щодо яких проводилося Службове розслідування; **(3)** висновки за результатами проведення Службового розслідування, а також можливі рекомендації щодо удосконалення Режиму комерційної таємниці.
8.8. Акт за результатами проведення Службового розслідування, що складений Комісією, подається на затвердження особисто Підприємцю. Зазначений акт носить лише рекомендаційний характер, а остаточне рішення приймається особисто Підприємцем.

ДОДАТКИ

Невід'ємною частиною цього Положення є наступні документи:

(1) Журнал, в якому фіксується факт ознайомлення осіб із змістом Положення про комерційну таємницю.