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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студентки Андрузької Анастасії Максимівни

академічної групи 125м–21–1

спеціальності 125 Кібербезпека

спеціалізацією

за освітньо–професійною програмою Кібербезпека

на тему Методи та засоби підвищення обізнаності персоналу з кібербезпеки на промисловому підприємстві

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.–м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст.викл. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.	94	відмінно	

Рецензент				

Нормоконтролер	ст.викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня магістра

студентки Андрузької А. М. **академічної групи** 125м–21–1
(прізвище та ініціали) (шифр)

спеціальності 125 Кібербезпека

спеціалізацією _____

за освітньо–професійною програмою Кібербезпека

на тему Методи та засоби підвищення обізнаності персоналу з кібербезпеки на промисловому підприємстві

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022 № 1200–С

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Дослідження антропогенних загроз на промисловому підприємстві, а також методи та засоби підвищення обізнаності персоналу з інформаційної та кібербезпеки	10.11.2022
Розділ 2	Розробка програми підвищення обізнаності персоналу та розробка засобів і методів підтримки поінформованості персоналу	01.12.2022
Розділ 3	Визначення економічної доцільності та ефекту від впровадження програми підвищення обізнаності персоналу	10.12.2022

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

Дата видачі завдання: 10.09.2022

Дата подання до екзаменаційної комісії: 16.12.2022

Прийнято до виконання _____ Андрузька А.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 102 стр., 18 рис., 2 табл., 4 додатка, 46 джерел.

Об’єкт дослідження: методи протидії антропогенним загрозам на промисловому підприємстві.

Предмет дослідження: методи та засоби підвищення обізнаності персоналу в питаннях, пов’язаних з інформаційною та кібербезпекою на промисловому підприємстві.

Мета кваліфікаційної роботи: забезпечення необхідного рівня захищеності інформації в ІКС промислового підприємства за рахунок підвищення обізнаності персоналу.

У першому розділі виконано аналіз антропогенних, внутрішніх та зовнішніх, загроз на промисловому підприємстві. Також були проаналізовані існуючі методи та засоби підвищення рівня обізнаності персоналу.

В другому розділі здійснено розробку та впровадження програми підвищення обізнаності персоналу з інформаційної та кібербезпеки. А також виконано розробку рекомендацій щодо організації підвищення обізнаності персоналу та розробка методів та засобів підтримки поінформованості персоналу з інформаційної та кіберебезпеки на промисловому підприємстві.

В економічному розділі визначено економічний ефект від впровадження програми підвищення обізнаності персоналу. Проведені розрахунки капітальних та експлуатаційних витрат.

Новизна роботи полягає в розробці програми підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки на промисловому підприємстві, а також методів та засобів підтримання поінформованості персоналу.

ПРОГРАМА ПІДВИЩЕННЯ ОБІЗНАНОСТІ, ІНФОРМАЦІЙНА БЕЗПЕКА, АНТРОПОГЕННІ ЗАГРОЗИ, ПРОМИСЛОВЕ ПІДПРИЄМСТВО, САЙТ, ПІДТРИМКА ПОІНФОРМОВАНОСТІ ПЕРСОНАЛУ

ABSTRACT

Explanatory note: 102 pages, 18 pictures, 2 tables, 4 appendices, 46 sources.

Object of research: methods of combating anthropogenic threats at industrial enterprise.

The subject of the study: methods and means of raising staff awareness of issues related to information and cyber security at industrial enterprise.

The purpose of the qualification work: ensuring the necessary level of information security in the ICS of industrial enterprise due to increasing the awareness of the personnel.

In the first chapter, an analysis of anthropogenic, internal and external threats at industrial enterprises is carried out. Existing methods and means of raising the level of staff awareness were also analyzed.

In the second section, the development and implementation of the program for raising staff awareness of information and cyber security was carried out. And also the development of recommendations on the organization of raising staff awareness and the development of methods and means of supporting staff awareness of information and cyber security at the industrial enterprise was carried out.

In the economic section, the economic effect of the implementation of the personnel awareness program is determined. Calculations of capital and operational costs were carried out.

The scientific novelty of the work consists in the development of a program to increase staff awareness of information and cyber security issues at industrial enterprise, as well as methods and means of maintaining staff awareness.

AWARENESS PROGRAM, INFORMATION SECURITY, ANTHROPOGENIC THREATS, INDUSTRIAL ENTERPRISE, WEBSITE, STAFF AWARENESS SUPPORT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO – international organization for standardization;

NIST– national institute of standards and technology;

АС – автоматизована система;

ДСТУ – державні стандарти України;

ІБ – інформаційна безпека;

ІКС – інформаційно-телекомунікаційна система;

ІМ – інформаційна мережа;

ІМП – інформаційні матеріали програми;

ІС – інформаційна система;

ІТ– інформаційні технології;

КМ – комп'ютерна мережа;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер.

ЗМІСТ

ВСТУП

Щоденний розвиток інформаційних технологій призводить до підвищення кількості ризиків для ІБ промислових підприємств. Автоматизованість, в наш час, будь–якого процесу на промисловому підприємстві дає велику можливість кіберзлочинцям здійснити атаку на ці процеси, що в свою чергу несе катастрофічні наслідки.

Люди – це найслабкіша ланка в інформаційній безпеці промислового підприємства. Людський фактор є найбільшим ризиком для інформаційних систем підприємств. Брак знань з інформаційної та кібербезпеки та нехтування простими правилами для захисту інформації – все це є головними чинниками для створення програми підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою на промисловому підприємстві.

Мета кваліфікаційної роботи – забезпечення необхідного рівня захищеності інформації в ІКС промислового підприємства за рахунок підвищення обізнаності персоналу.

Задачі кваліфікаційної роботи:

- аналіз антропогенних загроз на промисловому підприємстві;
- аналіз методів та засобів підвищення обізнаності персоналу;
- розробка програми підвищення обізнаності персоналу;
- розробка методів та засобів підтримки поінформованості персоналу.

Об'єкт дослідження – методи протидії антропогенним загрозам на промисловому підприємстві.

Предмет дослідження – методи та засоби підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою на промисловому підприємстві.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз внутрішніх та зовнішніх джерел загроз на промисловому підприємстві

Розвиток глобального процесу інформатизації суспільства, що спостерігається останні десятиліття, породило нові глобальні проблеми ІБ. Багато ключових доходів компанії сильно залежать від стану її інформаційного середовища. Будь–який навмисний чи ненавмисний вплив на інформаційне охоплення зовнішніх або внутрішніх джерел може завдати серйозної шкоди цим інтересам та створити загрози та ризики безпеки. Тому ІБ за сучасних умов одна із необхідних умов успішного функціонування підприємства.

Все більш очевидним стає той факт, що загальний рівень фінансової безпеки компанії залежить від її інформаційної складової. Практика показує, що недружня поведінка проти інтересів суб'єктів господарювання починається зі збору інформації. Зазвичай з кримінальними думками про можливу протиправну діяльність і без належного інформаційного супроводу навіть дрібні крадіжки не є руйнівною ознакою, наприклад: підприємницьке або рейдерське захоплення пенсійних активів. Не випадково питання ІБ вже давно є одними з головних пріоритетів майже всіх великих компаній. Останнім часом багато власників малого бізнесу в країні почали усвідомлювати реальні ризики для внутрішньої інформації, систем обробки та працівників, залучених до її обробки [1].

Правову основу ІБ становлять Конституція України, Закон України «Про національну безпеку України» [2], та інші закони України, міжнародні договори, а також у Стратегії національної безпеки України, яка затверджена Указом Президента [3]. У Законі «Про національну безпеку України» надано офіційну оцінку значущості й системної сутності ІБ як невід'ємної складової національної безпеки України.

У «Стратегії національної безпеки», присвяченій стану ІБ в нашій державі, зазначено:

1. Посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;

2. Недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;

3. Наближається до критичного стан безпеки інформаційно–комп'ютерних систем у фінансовій і банківській сфері, сфері державного управління, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо [3].

В інформаційному праві ІБ є одним із аспектів, що розглядають інформаційні відносини в рамках інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства та держави, загроз цим інтересам.

Інформація стала фактором, здатним призвести до серйозних техногенних аварій, військово–політичних конфліктів, порушень адміністративної та фінансової системи. Чим вищий рівень інтелектуалізації та інформатизації суспільства, чим більша реалізація інтересів, людей та націй за допомогою інформатизації, тим більше воно потребує надійної ІБ [1].

Останні кілька років були далеко не звичайними як для кібербезпеки, так і для бізнесу в цілому. Пандемія COVID–19 остаточно змінила спосіб ведення бізнесу, і кіберзлочинці адаптувалися до цих змін, пристосовуючи свою тактику до нової реальності. Суб’єкти кіберзагроз випробували нові тактики та методи, визнали їх успішними та додали їх до свого основного арсеналу [4].

Щоб здійснити складну атаку, як зараження програмами–вимагачами або шпигунство, суб’єкти загрози повинні спочатку закріпитися в системі. Саме тут і з’являються фішинг і вразливості програмного забезпечення. За даними IBM, 75% атак у 2021 році використовували фішинг (41%) і використання вразливостей (34%) як вектори початкового злому. На додаток до цього, невеликий відсоток вторгнень передбачав використання вкрадених облікових

даних (9%), грубу силу (6%), віддалений робочий стіл (4%), знімний носій (4%) і розпилення пароля (1%).

Фішинг і вразливості програмного забезпечення це лише початковий крок у ширшій схемі речей. За даними IBM, кінцеві цілі зловмисників варіювалися від програми–вимагача, доступу до сервера, компрометації бізнес–електронної пошти, крадіжки даних, збору облікових даних, інструменту віддаленого доступу, неправильної конфігурації, зловмисних інсайдерів тощо. Цікаво, що більше половини (53%) кібератак використовували найслабшу ланку – користувачів. За даними IBM, 21% програм–вимагачів і 8% шахрайства BEC покладалися на фішинг; доступ до сервера (14%) включав відомі вразливості, про які в ідеалі повинні були знати групи безпеки. Подібне спостереження щодо участі людської помилки також було зроблено у звіті Verizon DBIR за 2022 рік [5].

Відповідно до звіту IBM Security X–Force Threat Intelligence Index 2022 вектор атак змістився з економічної сфери на промисловість у 2021 році. Цільовими галузями операційних технологій у 2021 році були: виробництво (61%), нафта і газ (11%), транспортна (10%), комунальні послуги (10%), видобуток корисних копалин (7%),важка і цивільна інженерія (1%). [6]

Близько 80% зловмисників, які намагаються зробити протиправні дії, належать до інсайдерів.

Промислове підприємство – це складна система, яка складається з комплексам більш простих систем, які характеризуються певними особливостями, змістом та організацій функціонування виробничого об’єкту.

Промислові підприємства характеризуються довговічністю, повторюваністю виробничих процесів, великим масштабом діяльності з відповідним розподілом праці, з використанням машин і технічних пристроїв.

Промислове підприємство переслідує свої цілі та повинно мати певні ресурси, включаючи сировину, матеріали, технічне обладнання, людські ресурси, інформацію, структуру тощо. Крім того, здійснюючи певну діяльність,

підприємство повинно співпрацювати з іншими учасниками ринку, від яких він отримує ресурси, необхідні для виробництва матеріалів.

Основні види діяльності промислового підприємства включають:

- внутрішню логістику, пов'язану з процесами отримання, зберігання, складування та розподілу сировини та матеріалів, необхідних у виробничих процесах;
- операційну діяльність, пов'язану з основною діяльністю підприємства, яка включає перетворення виробничих факторів у готовий продукт. Ця діяльність включає в себе обробку, формування, пакування, оновлення, обслуговування тощо;
- зовнішню логістику, пов'язану з перевозкою та зберіганням готової продукції;
- маркетинг і продажі, тобто діяльність із переконання потенційного покупця придбати товар. Ця діяльність може використовувати низку інструментів, таких як: реклама, прямі продажі, ярмарки та виставки тощо;
- сервіси, завданнями якого є підтримка функціювання компанії на високому рівні та забезпечення відповідної якості продукту [6].

В соціальному відношенні підприємство – це соціальна система суспільства, в якій здійснюється взаємодії колективних та особистих інтересів на принципах взаємної зацікавленості.

В інформаційному відношенні підприємство – складна динамічна система, що постійно розвивається та яка характеризується великою кількістю різних зв'язків між всіма підрозділами всередині та із зовнішнім середовищем.

Промислові підприємства зараз стикаються з найбільшою кількістю потенційних ризиків ніж будь–коли в історії. Більш складне обладнання, швидкий ріст та потреба в отриманні конкурентної переваги означає, що виробництво і логістика повинні працювати безупинно.

На даний час не існує ще жодного підприємства, яке не має в своїх рядах людини, і тому найслабшою ланкою в ланцюжку безпеки становить людський

фактором, що викликає великий інтерес для кіберзлочинців. Страх, необережність, брак обізнаності та інформації в таких ситуаціях роблять людей більш сприйнятливими до шахраїв. Кіберзлочинці використовують людський фактор для отримання несанкціонованого доступу, викрадення облікових даних і зараження систем шкідливим програмним забезпеченням. Кількість кібератак зростає. Вони не такі дорогі, як фізичні атаки, не обмежуються відстанями та географією, їх неможливо легко відстежити та ідентифікувати. Таким чином, ці напади є більш привабливими та небезпечними, ніж фізичні. Крім того, шкідливі програми можуть повторно використовуватися для атаки на інші системи [8].

Важливість ІБ на промислових та інших підприємствах в даний час є найбільшою. Це є наслідком високого рівня інформатизації економічної діяльності та суспільства в цілому, в тому числі в глобальній перспективі, та повсюдного впровадження інформаційних ресурсів у всі сфери людської діяльності, які часто витісняють інші види ресурсів. Боротьба з різноманітними загрозами та викликами, що виникли внаслідок становлення та зростання глобальної інформаційної економіки, стала серйозною проблемою, яка впливає на питання забезпечення загального сталого функціонування та розвитку як сучасного світу, так і окремих об’єктів. в теперішньому і майбутньому [9].

Погіршення таких параметрів інформації, як конфіденційність, цілісність, доступність та надійність на підприємстві може призвести до вкрай негативних наслідків: порушення функціонування систем керування технологічними процесами та інших відповідальних систем; розголошення інформації, що становить комерційну та інші види конфіденційності; порушення достовірності фінансових документів; несанкціонований доступ до персональних даних фізичних осіб та ін. Наслідками вищевикладеного можуть бути: погіршення ділових відносин із партнерами; зрив переговорів; втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність додаткових досліджень ринку; втрата можливості патентувати чи продавати ліцензії на результати

науково–технічної діяльності; зниження ціни чи обсягу продажів; втрата ділової репутації [1].

Тріада КЦД (цілісність даних; конфіденційність інформації; доступність інформації) – це модель, яку компанії використовують для оцінки своїх можливостей безпеки та ризиків. Звернення до безпеки разом із цими трьома основними компонентами забезпечує чіткі вказівки для компаній щодо розробки ефективніших і ефективніших методів безпеки та політики.

Цілісність даних. Заходи цілісності захищають інформацію від несанкціонованої зміни. Ці заходи забезпечують впевненість у точності та повноті даних. Необхідність захисту інформації включає як дані, які зберігаються в системах, так і дані, які передаються між системами, наприклад електронна пошта. Підтримуючи цілісність, необхідно не лише контролювати доступ на системному рівні, але й додатково гарантувати, що користувачі системи можуть змінювати лише ту інформацію, на яку вони мають законне право.

Як і захист конфіденційності, захист цілісності даних виходить за рамки навмисних порушень. Ефективні засоби протидії цілісності також повинні захищати від ненавмисних змін, таких як помилки користувача або втрата даних у результаті несправності системи.

Існує багато контрзаходів, які можна вжити для захисту цілісності. Контроль доступу та сувора автентифікація можуть допомогти запобігти внесенню авторизованими користувачами несанкціонованих змін. Перевірка хешу та цифрові підписи можуть допомогти переконатися, що транзакції є автентичними, а файли не змінено чи пошкоджено. Не менш важливими для захисту цілісності даних є засоби адміністративного контролю, такі як розподіл обов'язків і навчання [10].

Конфіденційність інформації. Заходи конфіденційності захищають інформацію від несанкціонованого доступу та зловживання. Більшість інформаційних систем містять інформацію, яка має певний ступінь

конфіденційності. Це може бути конфіденційна бізнес–інформація, яку конкуренти можуть використати у своїх інтересах, або особиста інформація про працівників, клієнтів або клієнтів організації.

Конфіденційна інформація часто має цінність, тому системи часто піддаються атакам, оскільки злочинці шукають уразливості, щоб використати їх. Серед векторів загрози – прямі атаки, такі як викрадення паролів і перехоплення мережевого трафіку, а також більш багатошарові атаки, такі як соціальна інженерія та фішинг. Не всі порушення конфіденційності є навмисними. Кілька типів поширених випадкових порушень включають надсилання конфіденційної інформації електронною поштою не тому одержувачу, публікацію особистих даних на загальнодоступних вебсерверах і залишення конфіденційної інформації на моніторі комп'ютера без нагляду.

Для забезпечення конфіденційності підприємства вживають багато контрзаходів. Паролі, списки контролю доступу та процедури автентифікації використовують ПЗ для контролю доступу до ресурсів. Ці методи контролю доступу доповнюються використанням шифрування для захисту інформації, до якої можна отримати доступ, незважаючи на елементи керування, наприклад електронних листів, що передаються. Додаткові контрзаходи конфіденційності включають адміністративні рішення, такі як політики та навчання, а також фізичні засоби контролю, які перешкоджають людям отримати доступ до об'єктів і обладнання [10].

Доступність інформації. Для того, щоб ІС була корисною, вона повинна бути доступною авторизованим користувачам. Заходи доступності захищають своєчасний і безперебійний доступ до системи. Деякі з найбільш фундаментальних загроз доступності не є зловмисними за своєю природою та включають апаратні збої, незаплановані простої програмного забезпечення та проблеми з пропускною здатністю мережі. Зловмисні атаки включають різні форми саботажу, спрямовані на заподіяння шкоди організації шляхом відмови користувачам у доступі до інформаційної системи.

Доступність і оперативність вебсайту є пріоритетом для багатьох компаній. Порушення доступності вебсайту навіть на короткий час може призвести до втрати доходу, незадоволеності клієнтів і шкоди репутації. Атака «Відмова в обслуговуванні» (DoS) – це метод, який часто використовують хакери для порушення роботи вебсервісу. Під час DoS–атаки хакери заповнюють сервер зайвими запитами, перевантажуючи сервер і погіршуючи якість обслуговування законних користувачів. З роками постачальники послуг розробили складні контрзаходи для виявлення та захисту від DoS–атак, але хакери також продовжують набувати витонченості, і такі атаки залишаються проблемою.

Контрзаходи доступності для захисту доступності системи такі ж широкі, як і загрози доступності. Системи, які мають високі вимоги до безперервної безперебійної роботи, повинні мати значну надлишковість апаратного забезпечення з резервними серверами та сховищем даних, доступними негайно. Для великих корпоративних систем зазвичай мають резервні системи в окремих фізичних місцях. Повинні бути встановлені програмні засоби для моніторингу продуктивності системи та мережевого трафіку. Контрзаходи для захисту від атак DoS включають брандмауери та маршрутизатори [10].

ІБ означає збереження цілісності та таємності під час зберігання або передачі інформації. Коли до інформації звертаються неавторизовані сторони або особи, трапляються порушення ІБ. Інциденти порушення можуть бути спричинені злодіями, суперниками, працівниками, хакерами, спецслужбами чи іншими сторонами. Крім того, особи, які цінують і бажають зберегти свою конфіденційність, зацікавлені в інформаційній безпеці [11].

Порушення одного з елементів може призвести до погіршення нормальної роботи підприємства. І як внутрішні, так і зовнішні небезпеки можуть спричинити зрив. Оскільки інформаційне суспільство швидко розширюється, ми можемо припустити, що існує дедалі більше потенційних джерел загроз інформаційній безпеці організації.

Під інформаційною загрозою промислового підприємства розуміють потенційну небезпеку випадкової (ненавмисної) або навмисної компрометації якості інформації, спричинену особливостями зберігання, обробки та використання інформації. Оскільки інформація зберігається і обробляється переважно за допомогою автоматизованих інформаційних систем, результати діяльності промислового підприємства залежить від функціональної стабільності цих систем і їх захищеності від дій зловмисників і конкурентів [12].

Усі джерела загроз інформаційній безпеці можна розділити на три основні групи: антропогенні (обумовлені діями суб'єкта), техногенні (обумовлені технічними засобами) та стихійні (обумовлені природними явищами). Антропогенні джерела загроз стосуються людської поведінки та є навмисним (отримання, видалення чи пошкодження неавторизованої інформації, фінансове шахрайство), спричиненим недбалістю користувача або випадковою ймовірністю. Техногенні загрози пов'язані з обладнанням. Наприклад, вихід з ладу накопичувача інформації або збій процесора чи жорсткого диска під час передачі чи обробки інформації. Природні явища спричинені дією різних природних явищ, таких як повені, урагани, землетруси та блискавки. Всі джерела загроз поділяються на :

1 Антропогенні джерела:
   1.1 Зовнішні джерела:
      1.1.1 Кримінальні структури;
      1.1.2 Потенційні зловмисники та хакери;
      1.1.3 Недобросовісні партнери;
      1.1.4 Технічний персонал постачальників телекомунікаційних послуг;
      1.1.5 Представники аварійних служб;
      1.1.6 Представники силових структур.
   1.2 Внутрішні загрози:
      1.2.1 Основний персонал (користувачі, розробники тощо);

1.2.2 Представники служби захисту інформації;

1.2.3 Допоміжний персонал (прибиральники, охоронці тощо);

1.2.4 Технічний персонал (життєзабезпечення та експлуатація) .

2 Техногенні джерела:

2.1 Зовнішні джерела:

2.1.1 Засоби зв'язку;

2.1.2 Мережі інженерних комунікацій (каналізація, водопостачання);

2.1.3 Транспорт.

2.2 Внутрішні джерела:

2.2.1 Неякісні технічні засоби обробки інформації;

2.2.2 Неякісні засоби обробки інформації;

2.2.3 Допоміжні засоби (сигналізація, телефонія);

2.2.4 Інші технічні засоби.

3 Стихійні джерела

3.1 Пожежі;

3.2 Землетруси;

3.3 Інші природні явища;

3.4 Різні непередбачувані обставини;

3.5 Незрозумілі явища;

3.6 Інші форс–мажорні обставини.

Внутрішні загрози.

Внутрішні загрози – це загрози, створені особами, які походять із самої організації. Ними можуть бути нинішні працівники, колишні працівники, зовнішні підрядники чи постачальники. По суті, будь–хто, хто має доступ до пристроїв або даних компанії. Ця форма витоку даних передбачає доступ внутрішнього зловмисника до конфіденційної інформації компанії зі зловмисними намірами. Серед зловмисників можуть бути як діючі, так і колишні співробітники [13].

Цілі осіб, які становлять загрозу для організації, можуть зовсім відрізнятися від цілей зовнішніх кіберзлочинців. Основними мотивами внутрішніх загроз є:

1. Шахрайство: крадіжка, зміна або знищення даних компанії з метою обману.

2. Шпигунство: викрадення інформації для іншої організації (як правило, конкурента).

3. Саботаж: використання законного доступу до мережі/активів компанії для пошкодження або знищення функціональності компанії.

4. Крадіжка інтелектуальної власності: крадіжка інтелектуальної власності компанії з наміром продати або використати власність.

5. Помста: Співробітники, яких компанія звільнила або іншим чином звільнила з роботи, можуть спробувати завдати шкоди репутації компанії, отримавши доступ до конфіденційної інформації [13].

Людський фактор часто найважче контролювати та передбачити, коли йдеться про захист даних. Більшість співробітників підприємств завжди усвідомлює фінансові та репутаційні наслідки витоку даних, тому буде достатньо, щоб люди підвищили пильність і запобігали поганим методам безпеки. Однак, в багатьох випадках підприємства знаходяться лише в одному недбалому співробітнику від шкідливого інциденту безпеки. Також завжди існує потенційна небезпека зловмисних інсайдерів і незадоволених співробітників, які хочуть завдати шкоди репутації компанії або викрасти дані, покидаючи організацію.

Найпоширеними внутрішніми загрозами є саботаж співробітників і викрадення даних і/або фізичного обладнання; несанкціонований доступ співробітників до охоронюваних зон і адміністративних функцій; слабкі заходи кібербезпеки та небезпечні практики; випадкова втрата або розголошення даних [14].

Саботаж співробітників і викрадення даних і/або фізичного обладнання. Саботаж і крадіжки співробітників часто виникають через погані переживання, які пов'язані з роботою. Можливо, співробітника не підвищили по службі; вони відчувають, що їм недоплачують або їхній авторитет підірвано новим керівником. Також може статися, що їх звільнили з причин, які вони вважають несправедливими.

Опортуністичні крадіжки також можуть бути проблемою на робочому місці. Відсутність політики, нагляду або, звісно, неадекватні заходи безпеки можуть створити спокусу перед людьми, деякі з яких просто не можуть не скористатися перевагами відкриття, особливо якщо вони обурені з будь–якої причини або якщо вони зіткнулися з фінансовими труднощами [15].

Методи які допомагають боротися з крадіжками та саботажем персоналу:

1. Відеоспостереження працює як стримуючий фактор, хоча, він ще працює, щоб попередити роботодавців про нечесну поведінку, а записаний матеріал може бути використаний як доказ для звільнення та/або кримінального переслідування.

2. Контроль доступу до певних частин підприємства потрібен для відстежування, кому куди дозволено заходити.

3. Сейфи та часові замки: зберігання готівки та цінностей у сейфах чи сховищах або під захистом часових замків, потрібно якщо є підозри на внутрішні крадіжки [15].

Несанкціонований доступ співробітників до охоронюваних зон і адміністративних функцій. Запобігання несанкціонованому доступу до території підприємства має важливе значення для не тільки ІБ, а й ще для безпеки здоров'я всіх співробітників . Відсутність належного захисту приміщень призводить до крадіжок та нещасних випадків, які завдадуть шкоди працівникам підприємства.

Щоб запобігти несанкціонованому доступу, усі заборонені зони в межах підприємства мають бути чітко визначені відповідними покажчиками; особливо в місцях, де часто присутні клієнти або неавторизований персонал. Залежно від

контексту, у якому відбувається несанкціонований доступ, відповідного і до того будуть наслідки від того доступу. Якщо уповноваженій стороні вдається отримати доступ до заборонених зон підприємства, це може призвести до травм, крадіжок або конфіденційної комерційної інформації [16].

Заходи щодо запобігання несанкціонованому доступу поділяють на 2 групи:

1. Проведення навчання персоналу по розпізнаванню ризиків та своєчасне повідомлення про підозрілу поведінку. Також треба мати чітку політику доступу до всіх будівель підприємства та переконатися, що всі співробітники прочитали та зрозуміли цю політику.

2. Контроль доступу на основі ролей (RBAC) відноситься до систем контролю доступу, які працюють шляхом надання або заборони доступу на основі ролі або посади особи на підприємстві. Певні зони в межах ділових приміщень можуть бути визначені як доступні лише для певних команд або співробітників, які перебувають вище певного рівня в ієрархії компанії.

Компанії повинні вживати заходів для запобігання несанкціонованому доступу до того, як він стався. Неможливо усунути наслідки злому після того, як воно сталося, тому зараз необхідно вжити комплексних заходів, щоб запобігти крадіжці, витоку даних і травмам на місці в майбутньому [16].

Слабкі заходи кібербезпеки та небезпечні практики. Не маючи відповідної цифрової та фізичної безпеки, підприємство з нерозвиненою інформаційною системою безпеки або взагалі не маючи дане, збільшує ймовірність використання вразливості, особливо через проблеми, які виникали раніше, як крадіжка.

Слабкі заходи безпеки накладають певні загрози, наприклад, якщо сервер для мережі компанії залишити в незачиненій кімнаті, будь–хто може зайти туди та пошкодити/викрасти майно. Незадоволений працівник чи відвідувач, який заходить у компанію, яка не пройшла належної перевірки безпеки.

Крім того, цими вразливими місцями безпеки може випадково скористатися звичайний працівник, зробивши щось просте, наприклад,

переглянувши ненадійний вебсайт – може бути ненавмисно завантажено вірус, який може вплинути на всю мережу [14].

Випадкова втрата або розголошення даних. Втрата даних є серйозною проблемою для підприємств. Втрата файлів означає втрату часу та грошей на відновлення інформації, яка є важливою для вашого бізнесу. Втрата даних відбувається, коли дані випадково видаляються або щось спричиняє їх пошкодження. Віруси, фізичні пошкодження чи помилки форматування можуть зробити дані нечитабельними як для людей, так і для програмного забезпечення.

Одним із важливих заходів для запобігання людським помилкам під час обробки даних є належне навчання. Головне, щоб співробітники розуміли, як працює обробка даних на підприємстві та як функціонують системи резервного копіювання на локальних комп'ютерах.

Помилки, спричинені помилками людини, також можна мінімізувати за допомогою кількох програмних засобів. Автоматизація мінімізує кількість взаємодії людини з даними, що знижує ризик видалення або перезапису. Оптимізований робочий процес також залишає мало місця для людських помилок, заощаджуючи час співробітників і полегшуючи виявлення помилок. Також треба використовувати системи резервного копіювання для збереження попереднього стану даних.

Відновлення випадково видалених або перезаписаних даних іноді можливо зробити так само просто, як пошук у кошику комп'ютера. В інших випадках можно отримати доступ до попередньо збережених версій документа. Коли втрачені дані не так легко відновити, тоді допоможе ПЗ для відновлення файлів. ПЗ для відновлення файлів сканує жорсткий диск вашого комп'ютера, щоб визначити та відновити втрачені дані [17].

Внутрішні загрози може бути важче виявити або запобігти, ніж зовнішні атаки, і вони невидимі для традиційних рішень безпеки, таких як брандмауери та системи виявлення вторгнень, які зосереджені на зовнішніх загрозах. Якщо зловмисник використовує авторизований вхід, наявні механізми безпеки можуть

не визначити аномальну поведінку. Крім того, зловмисникам легше уникнути виявлення, якщо вони знайомі із заходами безпеки організації [18].

Зовнішні загрози.

Зовнішня загроза означає ризик того, що хтось ззовні компанії намагається використати вразливі місця системи за допомогою шкідливого програмного забезпечення, злому, саботажу або соціальної інженерії [19].

Шкідливе ПЗ, шкідлива реклама, фішинг, DDoS–атаки, програми–вимагачі; це лише деякі з вірусів і методів, які хакери використовують ззовні, щоб отримати доступ до вашого програмного забезпечення або мережі.

Отримавши доступ, кіберзлочинці залишаються всередині системи, іноді місяцями, непоміченими та витягуючи інформацію. Більшість з них так і не знайдено, а ще більше – виявлено пізніше. Ви зіткнетеся з набагато більшою кількістю зовнішніх атак, ніж внутрішніх, і ідея полягає в тому, щоб посилити периметр, щоб не допустити хакерів. Периметри можна правильно побудувати за допомогою відповідного тестування на проникнення, яке проводить досвідчена фірма з кібербезпеки [20].

Основні зовнішні антропогені загрози, які можуть впливати на інформаційну систему підприємства поділяють на:

Шкідливе ПЗ (malware).

Зловмисне ПЗ – це файл або код, який зазвичай доставляється через мережу, який заражає, досліджує, викрадає або виконує практично будь–яку поведінку, яку хоче зловмисник. А оскільки зловмисне ПЗ існує в багатьох варіантах, існує безліч методів зараження комп'ютерних систем.

Хоча зловмисне ПЗ різне за типом і можливостями, зазвичай має одну з таких цілей:

- забезпечити дистанційне керування зловмисником для використання зараженої машини;
- надсилання спаму із зараженої машини нічого не підозрюючим цілям;

- дослідити мережу зараженого користувача або підприємства;
- викрасти конфіденційні дані.

Зловмисне ПЗ доставляє своє корисне навантаження кількома різними способами. Від вимоги викупу до викрадення конфіденційних особистих даних кіберзлочинці стають усе більш витонченими у своїх методах. Нижче наведено деякі найпоширеніші типи шкідливих програм.

Ботнети – скорочення від «мережі роботів», це мережі заражених комп'ютерів під контролем однієї атакуючої сторони за допомогою командно–контрольних серверів. Ботнети є надзвичайно універсальними та адаптованими, здатними підтримувати стійкість через резервні сервери та використання заражених комп'ютерів для ретрансляції трафіку. Ботнети часто є арміями сучасних розподілених атак типу «відмова в обслуговуванні» (DDoS).

Криптоджекінг (cryptojacking) – це зловмисний криптомайнінг (процес використання обчислювальної потужності для перевірки транзакцій у мережі блокчейн і отримання криптовалюти за надання цієї послуги), який відбувається, коли кіберзлочинці зламують корпоративні та персональні комп'ютери, ноутбуки та мобільні пристрої для встановлення програмного забезпечення.

Шкідлива реклама (malvertising) – це поєднання «зловмисне ПЗ + реклама», що описує практику онлайн–реклами з метою поширення шкідливого програмного забезпечення. Зазвичай це включає введення зловмисного коду або рекламних оголошень із зловмисним програмним забезпеченням у законні рекламні мережі та вебсторінки.

Поліморфне зловмисне ПЗ – будь–який із зазначених вище типів зловмисного програмного забезпечення зі здатністю регулярно «перетворюватися», змінюючи зовнішній вигляд коду, зберігаючи внутрішній алгоритм. Зміна зовнішнього вигляду програмного забезпечення руйнує виявлення за допомогою традиційних сигнатур вірусів [20].

Програми–вимагачі (ransomware) – злочинна бізнес–модель, яка використовує зловмисне ПЗ для зберігання цінних файлів, даних або інформації

з метою отримання викупу. Жертви атаки програм–вимагачів можуть суттєво погіршити роботу або повністю припинити роботу.

Засоби віддаленого адміністрування (RAT) – ПЗ, яке дозволяє віддаленому оператору контролювати систему. Спочатку ці інструменти створювалися для законного використання, але зараз ними користуються зловмисники. RAT забезпечують адміністративний контроль, дозволяючи зловмиснику робити майже все на зараженому комп'ютері. Їх важко виявити, оскільки вони зазвичай не відображаються в списках запущених програм або завдань, і їх дії часто приймають за дії законних програм.

Руткіти – програми, які надають привілейований (на кореневому рівні) доступ до комп'ютера. Руткіти відрізняються та ховаються в операційній системі.

Шпигунське ПЗ (spyware) – шкідливе ПЗ, яке збирає інформацію про використання зараженого комп'ютера та передає її зловмиснику. Термін включає ботнети, рекламне ПЗ, бекдор, кейлоггери, крадіжки даних і мережевих хробаків [21].

Троянське вірусне ПЗ (trojans malware) – шкідливе ПЗ, замасковане в тому, що здається легальним програмним забезпеченням. Після активації шкідливі трояни виконуватимуть будь–які дії, на які вони були запрограмовані. На відміну від вірусів і хробаків, трояни не розмножуються через зараження.

Вірусне ПЗ (virus malware) – програми, які копіюють себе на комп'ютері чи в мережі. Шкідливе ПЗ–віруси створюють існуючі програми та можуть бути активовані лише тоді, коли користувач відкриває програму. У гіршому випадку віруси можуть пошкодити або видалити дані, використовувати електронну пошту користувача для поширення або стерти все на жорсткому диску.

Зловмисне ПЗ–черв'як (worm malware) – віруси, що саморозмножуються, які використовують вразливі місця системи безпеки для автоматичного поширення між комп'ютерами та мережами. На відміну від багатьох вірусів, шкідливі черв'яки не прикріплюються до існуючих програм і не змінюють

файли. Зазвичай вони залишаються непоміченими, доки реплікація не досягне масштабу, який споживає значні системні ресурси або пропускну здатність мережі [21].

Зловмисне ПЗ також використовує різноманітні методи, щоб поширюватися на інші комп'ютерні системи поза початковим вектором атаки. Визначення атак шкідливих програм можуть включати:

- вкладення електронної пошти, що містять зловмисний код, можуть бути відкриті й, отже, виконані користувачами, які нічого не підозрюють. Якщо ці листи пересилаються, зловмисне ПЗ може поширитися ще глибше в організацію, ще більше скомпрометувавши мережу;
- файлові сервери, наприклад ті, що базуються на загальній файловій системі Інтернету (SMB/CIFS) і мережевій файловій системі (NFS), можуть сприяти швидкому поширенню зловмисного програмного забезпечення, коли користувачі отримують доступ до заражених файлів і завантажують їх;
- ПЗ для обміну файлами може дозволити шкідливому програмному забезпеченню відтворюватися на знімних носіях, а потім у комп'ютерних системах і мережах;
- одноранговий (P2P) обмін файлами може запровадити зловмисне ПЗ, обмінюючись файлами, здавалося б, нешкідливими, як музика чи зображення;
- уразливості, які можна віддалено використовувати, можуть надати хакеру доступ до інформаційної системи незалежно від географічного розташування з невеликою потребою або взагалі без участі користувача комп'ютера [21].

Хакерство з боку окремих осіб, груп людей або компаній.

Загальноприйняте визначення хакерства – це акт компрометації цифрових пристроїв і мереж через несанкціонований доступ до облікового запису чи комп'ютерної системи. Хакерство не завжди є зловмисною дією, але найчастіше воно пов'язане з незаконною діяльністю та крадіжкою даних кіберзлочинцями.

Хакерство стосується неналежного використання таких пристроїв, як комп'ютери, смартфони, планшети та мережі, щоб завдати шкоди або пошкодити системи, зібрати інформацію про користувачів, викрасти дані та документи або порушити діяльність, пов'язану з даними. Метод атаки відомий як «вектор атаки» і часто передбачає використання вразливостей у таких аспектах, як Wi–Fi, Bluetooth, підключення до Інтернету або через отримання доступу до внутрішньої мережі.

Існує широкий спектр можливих мотивацій, залежно від того, чи виконує це окрема особа, група чи компанія.

Якщо це робить окрема особа, дуже важко розпізнати її мотивацію, оскільки це може бути що завгодно: від прибутку до протесту до відпочинку. Багато хакерських груп стверджують, що здійснюють свої дії заради політичних або соціальних цілей, так звані хактивісти. Однак набагато більше зроблять це просто для того, щоб завдати шкоди [19].

Тим часом компанії набагато чіткіше розуміють, чого вони хочуть: оцінити власні слабкі сторони, отримати прибуток чи зібрати інформацію.

Компанії можуть використовувати хакерство з метою корпоративного шпигунства, щоб дізнатися про плани, продукти та фінанси своїх конкурентів.

Стратегії злому поділяються на одну з двох категорій, незалежно від того, який відтінок хакера.

Категорія 1: Нульовий день – це вразливості, які раніше не бачили, також відомі як уразливості нульового дня. Служби безпеки не знають, як захиститися від них, і часто навіть не усвідомлюють, що систему зламано.

Категорія 2: Більшість сучасних хакерів використовують код, який був написаний кимось іншим і випущений у дику природу. Такого роду хакерів часто називають script kiddie –вони використовують уже існуюче ПЗ для здійснення атак і не мають особливого досвіду програмування [22].

Організації безпеки дуже добре просувають оновлення системи безпеки після виявлення зломів і оприлюднення коду.

Хакерство є хронічною проблемою, яка ставить під загрозу інформаційну безпеку підприємства та його робітників. Це може призвести до непідрахованих економічних втрат, навіть до знищення всеєї фінансової системи підприємства. На організаційному рівні це може призвести до крадіжки даних, що призведе до значних довгострокових наслідків.

Методи соціальної інженерії, які використовуються для обману з метою надання інформації.

Атаки соціальної інженерії не тільки стають все більш поширеними проти підприємств, але й стають все більш витонченими. Оскільки хакери розробляють все більш хитрі методи, щоб обдурити співробітників і окремих осіб, щоб вони передали цінні дані компанії, підприємства повинні проявляти належну обачність, щоб бути на два кроки попереду кіберзлочинців.

Методи соціальної інженерії, які використовуються для обману зазвичай передбачають певну форму психологічної маніпуляції, обманюючи користувачів або співробітників, які нічого не підозрюють, щоб вони передали конфіденційні чи чутливі дані. Як правило, соціальна інженерія включає електронну пошту чи інше спілкування, яке викликає у жертви терміновість, страх або подібні емоції, спонукаючи жертву негайно розкрити конфіденційну інформацію, натиснути шкідливе посилання або відкрити шкідливий файл. Оскільки соціальна інженерія включає людський елемент, запобігання цим атакам може бути складним для підприємств [23].

Нижче приведені найпоширеніші кіберзагрози, які використовують тактику соціальної інженерії для отримання доступу до конфіденційної інформації.

Фішинг. Найбільш поширеним способом впровадження соціальної інженерії є використання оманливих фішингових електронних листів, вебсайтів і текстових повідомлень, щоб викрасти конфіденційну організаційну інформацію від нічого не підозрюючих жертв. Незважаючи на те, наскільки

добре відомі методи фішингової електронної пошти, 1 з 5 співробітників все одно натискає на ці підозрілі посилання.

Цільовий фішинг. Це шахрайство електронною поштою використовується для цілеспрямованих атак на окремих осіб або компанії. Цільовий фішинг є більш складним, ніж звичайна масова фішингова електронна пошта, оскільки вимагає поглибленого дослідження потенційних цілей та їхніх організацій.

Приманка (baiting). Цей тип атаки може бути здійснений онлайн або у фізичному середовищі. Кіберзлочинець зазвичай обіцяє жертві винагороду в обмін на конфіденційну інформацію [24].

Шкідливе ПЗ (malware). Категорія атак, яка включає програми–вимагачі, жертвам яких надсилається термінове повідомлення та обманом змушують установити зловмисне ПЗ на їхні пристрої. За іронією долі, популярна тактика полягає в тому, щоб повідомити жертві, що зловмисне ПЗ вже встановлено на її комп'ютері, і що відправник видалить ПЗ, якщо він сплатить комісію.

Претекстинг (pretexting). Ця атака полягає в тому, що зловмисник видає себе за фальшиву особу, щоб обманом змусити жертв надати інформацію. Перетекстування часто використовується проти організацій, які мають велику кількість клієнтських даних, як–от банки, великі підприємства чи компанії [24].

Тейлгетинг (tailgating). Ця атака спрямована на особу, яка може надати злочинцю фізичний доступ до будівлі чи території підприємства. Це шахрайства часто стають успішними завдяки помилковій ввічливості жертви, наприклад, якщо вона затримує двері для незнайомого «співробітника».

Атака водопою (water–holing). Ця атака використовує передові методи соціальної інженерії для зараження вебсайту та його відвідувачів шкідливим програмним забезпеченням. Зазвичай інфекція поширюється через вебсайт, який стосується індустрії жертв, наприклад популярний вебсайт, який регулярно відвідують [24].

Зовнішні та внутрішні антропогенні загрози однаково руйнівні, але це залежить від галузі промисловості, в якій працює підприємство, та інформації,

яка береться. Якщо працівник продає секрети конкуренту та вирішує зіпсувати дані компанії, тоді шкода репутації та прибуткам може бути довгостроковою та руйнівною, що робить внутрішні зломи потенційно більш загрозливими, ніж зовнішні. Зовнішні хакери зазвичай шукають інформацію, яку вони можуть продати або використати для отримання прибутку, тож якщо хакер проникає у вашу мережу чи ПЗ, а потім приховує цінну інформацію та вимагає грошовий викуп за передачу інформації назад вам – тоді зовнішні хакери можуть бути грошово шкідливішим [20].

1.2 Аналіз методів та засобів підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою

Обізнаність з ІБ можна визначити як процес інформування працівників про інформаційну безпеку. Іншими словами, інформування співробітників підприємства про правила та положення, пов’язані з інформаційною безпекою [25]. Накопичення таких знань серед співробітників і їх ставлення до ІБ зміцнить захист організації від фізичних інцидентів або інцидентів ІБ [26].

Головною метою обізнаності з ІБ є навчання людей методам безпеки в Інтернеті та забезпечити надійний захист від кіберзлочинності. Сучасні технології забезпечують зараз великий захист. ПЗ відстежує електронні листи та сеанси вебсерфінгу, фільтруючи велику кількість непотрібної та загрожуючої інформації. Мережеві та комп’ютерні брандмауери добре справляються зі своєю роботою, не даючи стороннім стати внутрішніми. Контроль доступу допомагає гарантувати, що лише авторизовані користувачі можуть використовувати мережеві ресурси. Але жодна технологія захисту не є ідеальною [27].

Зловмисники постійно винаходять нові способи обійти, існуючи на підприємстві, системи ІБ. Крім того, зловмисне ПЗ розвивається швидко, а фішинг з кожним місяцем стає все складнішим. Лише розуміючи загрози для комп’ютерів і даних під час серфінгу в Інтернеті (або перевірки електронної

пошти, обміну миттєвими повідомленнями чи текстовими повідомленнями), можно навчитися не стати жертвами зловмисників.

Поінформованість про безпеку є важливою протидією кіберзлочинам, і це ключ до уникнення цих злочинів майже в кожному випадку. Навчання з питань безпеки є важливою частиною стратегії поглибленого захисту співробітників та концентраційної інформації [28].

Цілі щодо обізнаності про безпеку можуть бути досягнуті, коли поведінка співробітників базується на передовій практиці, якої їм рекомендується дотримуватися під час розповсюдження політики ІБ та програм підвищення обізнаності, які проводить підприємство [29]. Зрозуміло, що підприємства, як правило, більше зосереджуються на технічних рішеннях, коли мова йде про інформаційну безпеку, а не на те, щоб їхні знання постійно оновлювалися, щоб досягти стабільної обізнаності про безпеку.

Широке зростання залежності від інформаційних технологій у повсякденній роботі співробітників багатьох підприємств робить збереження цих технологій ще більш складним завданням. Якщо розглядаєти співробітників як найслабшу ланку в ланцюжку ІБ, інформаційні кампанії є першою лінією захисту. Крім того, збільшення використання Інтернет–сервісів призводить до загроз безпеці інформації та багатьох проблем з інформаційною безпекою [30].

Існує підвищена потреба в обізнаності про інформаційну безпеку серед кінцевих користувачів, щоб переконатися, що культура безпеки є частиною їхньої щоденної роботи. Тому дуже важливо, щоб співробітники на всіх рівнях усвідомлювали свою відповідальність щодо ІБ. Це означає заохочувати користувачів усвідомлювати пов’язані з цим ризики та мотивувати їх уникати цих ризиків. Отже, знання безпеки навчає кінцевих користувачів, як захищати інформацію організації та як вживати розумних заходів для запобігання порушенням безпеки.

Таким чином, знання ІБ діє як профілактичний захід, і багато міжнародних стандартів, таких як ISO 27005, посилаються на це як на обов’язкову умову. Для

отримання підприємством сертифікації за цим стандартом спочатку необхідно впровадити плани підвищення обізнаності щодо ІБ. Основну роль обізнаності про інформаційну безпеку можна підсумувати такими пунктами:

- зменшити кількість інцидентів безпеки;
- відповідати міжнародним стандартам або передовій практиці ІБ;
- охопити всі проблеми керівництва щодо безпеки інформації та систем;
- відповідати нормативним вимогам.

Вищезазначені пункти чітко пояснюють величезні переваги підвищення обізнаності про інформаційну безпеку в організаціях. Крім того, загальновідомо, що в інформуванні кінцевих користувачів про інформаційну безпеку та потенційних загроз, зменшиться кількість ризиків безпеки [31].

Незважаючи на стрімкий розвиток технологій ІБ та інструментів захисту, таких як антивіруси, брандмауери та інструменти аудиту, працівники все ще ведуть ризиковану поведінку. Таким чином, не дивно, що працівники є однією з основних причин порушень ІБ.

Нинішній розвиток інформаційних технологій привів до того, що підприємства стали більш усвідомлювати важливість інформування своїх співробітників про інформаційну безпеку, і тому витрачається багато часу, зусиль і грошей саме на цю сферу. Створення та впровадження політики ІБ робиться для того, щоб спрямувати поведінку працівників на правильні практики. Однак наявність політики не означає, що підприємства повністю захищене від небажаної поведінки. Крім того, «хоча наявність політики є важливою для визначення цілей організації в галузі інформаційної та кібербезпеки, є очевидні переваги в тому, щоб переконатися, що вона розуміється та впроваджується відповідним чином» [32].

Тому підвищення рівня знань співробітників про політику безпеки підприємства відіграє дуже важливу роль в успішній реалізації такої політики. На перший погляд, підвищення обізнаності, освіта та навчання можуть здатися подібними концепціями, які слід використовувати для підвищення рівня знань

працівників, однак існує тонка різниця між цими трьома термінами [33]. Вивчення ІБ є безперервним процесом, який починається з інформованості, яке потім переходить у навчання і, нарешті, розвивається в освіту.

У цієї моделі є три етапи безперервного навчання інформаційній безпеці: обізнаність, навчання та освіта.

Перший етап – «обізнаність про безпеку». Він розташований у нижній частині сукупності навчання безпеки та є основним типом навчання, з якого повинні починати всі співробітники. Рівень «основ безпеки та грамотності» є перехідним етапом між етапом обізнаності та етапом навчання, і він гарантує, що всі співробітники мають базові знання ІБ.

Другий етап, навчання, представлений двома рівнями: «основи безпеки та грамотність» і «функціональні ролі та обов'язки». На цьому етапі співробітники потребують навчання основам безпеки та розвитку спеціальних знань про загрози безпеці, вразливості та заходи протидії.

Останній етап, освіта, представлений рівнем «освіта та досвід», який орієнтований на працівників, які працюють у сфері інформаційній безпеки. Основною метою цього етапу є розвиток здатності співробітників виконувати складні завдання. Фахівці з ІБ повинні бути в курсі розвитку технологій і мінливих загроз [27].

Обізнаність. Поінформованість про безпеку включає дії, які були розроблені, щоб змінити поведінку співробітника таким чином, щоб вона була в межах ІБ підприємства. Основною метою інформування про безпеку є привернення уваги користувачів до ІБ. Завдяки підвищенню обізнаності співробітники зможуть розпізнавати загрози інформаційній безпеці та визначати найкращі кроки для вирішення таких проблем. Обізнаність про безпеку має на меті покращити поведінку працівників і ставлення до безпечних методів у всіх системах підприємства. Іншими словами, обізнаність зосереджується на знаннях співробітників конкретних питань безпеки або ряду проблем [33]. Основні методи підвищення обізнаності співробітників:

1. Повідомлення на засобах підвищення обізнаності, наприклад, ручках, брелоках, листівки, блокноти;
2. Плакати, «списки дій і заборон» або чек–листи;
3. Заставки та попереджувальні банери/повідомлення;
4. Інформаційні бюлетені;
5. Сповіщення від столу до столу (наприклад, друкована копія, яскравого кольору);
6. Повідомлення електронної пошти в межах підприємства;
7. Відеокасети;
8. Зустрічі (через Інтернет; телеконференції; особисто, під керівництвом інструктора);
9. Дні IT-безпеки або подібні заходи;
10. Спливаючий календар із нагадуванням щодо оновлень в інформаційній безпеці, щомісячні поради щодо безпеки тощо;
11. Кросворди;
12. Програма нагородження, наприклад, за гарне пройдений курс з ІБ.

Навчання. Навчання в основному має на меті надати співробітникам необхідні навички безпеки щодо конкретних або обраних тем безпеки. Програми навчання повинні бути обрані та реалізовані відповідно до цілей навчання, встановлених підприємством. Наприклад, процес навчання співробітника, як користуватися антивірусним програмним забезпеченням, вважається навчанням інформаційній безпеці. Важливо розуміти різницю між навчанням і підвищенням обізнаності [34]. Навчання має на меті навчити співробітників навичкам, які допоможуть їм у виконанні конкретного завдання, тоді як підвищення обізнаності має на меті привернути увагу співробітників до проблеми безпеки або набору проблем [27]. Головними методами навчання, які допомагають в підвищенні рівня знання ІБ є:

1. Інтерактивний відеотренінг (IVT);
2. Вебнавчання;

3. Без доступу до Інтернета, комп'ютерне навчання;
4. Навчання на місці, під керівництвом інструктора.

Освіта. Освіта вважається найвищим рівнем розвитку знань, і вона є більш спеціалізованою з точки зору методу навчання, що передбачає більш поглиблене шкільне навчання. Наприклад, курс або програма отримання ступеня в певній галузі, що надається університетом або інститутом, вважається освітою. «Освіта об'єднує всі навички безпеки та компетенції різних функціональних спеціальностей у загальну сукупність знань і прагне створити спеціалістів з IT–безпеки та професіоналів, здатних до бачення та проактивного реагування» [34]. Методи підвищення знань в цьому пункті не різняться великою кількістю: проходження курсів, семінарів з підвищення кваліфікації, відвідування конференцій.

Всі три пункти формують сукупність, яка починається з обізнаності, розвивається до навчання та може перерости в освіту. Обізнаність означає знання ситуації або факту. Освіта з питань безпеки призначена для тих, хто хоче зробити кар'єру з безпеки. Навчання надає співробітникам необхідні навички безпеки щодо конкретних або обраних тем безпеки.

Національний інститут стандартів і технологій (NIST) розділив методології для програм інформування про інформаційну безпеку на: навчання з ІБ, комп'ютерне інформування про інформаційну безпеку та послуги з інформування та інструменти нагадування.

Навчання з питань ІБ: це вважається найефективнішим методом привернення уваги користувачів (NIST 2005). Зазвичай аудиторія, яка знає про безпеку, поділяється на три категорії: керівництво, кінцеві користувачі та технічний персонал [27].

Поінформованість про інформаційну безпеку на основі комп'ютера: це підхід до самонавчання; комп'ютерна програма розроблена та доступна в мережі в будь–який час, щоб кінцеві користувачі могли отримати до неї легкий доступ, а потім самостійно вивчати теми, які їх цікавлять, у вільний час.

Інструменти інформування та нагадування: Інструменти нагадування використовуються для того, щоб інформувати кінцевих користувачів про обізнаність щодо ІБ, час від часу нагадуючи їм. Прикладами інструментів нагадування є: мультимедійні презентації, буклети безпеки, плакати безпеки, екранні заставки комп'ютера, електронні листи, рекламні матеріали з питань безпеки та інформаційні бюлетені безпеки [27].

Незважаючи на наявність найкращих програм інформування про інформаційну безпеку, існують перешкоди, які ускладнюють успішне впровадження заходів інформування:

Впровадження нової технології: прийняття нової технології вимагає нового рівня розуміння користувачем або зміни в поведінці користувача для того, щоб користувач міг використовувати цю технологію. Програми підвищення обізнаності зазвичай застаріли та не оновлюються через швидкий розвиток інформаційних технологій. Крім того, на рівні фахівців команда з підвищення обізнаності може не бути в курсі останніх новин або навіть не мати відповідних знань щодо нових технологій і того, як зробити співробітників більш обізнаними про політику безпеки організації.

Розмір підходить усім: деякі програми підвищення обізнаності про безпеку розроблені таким чином, щоб відповідати всім працівникам. Це може призвести до того, що працівники нехтують усім, чого вони дізналися, через перевантаження інформацією. Тому співробітники повинні бути розділені на класи, щоб донести до кожного класу цілеспрямовані повідомлення. Крім того, програми інформування повинні бути розроблені спеціально для кожної групи користувачів, при цьому кожен сегмент зосереджується на конкретній програмі інформування.

Забагато інформації: це поширена проблема під час організації програм підвищення обізнаності, навіть після сегментування користувачів на групи та надсилання цільових повідомлень. Програми підвищення обізнаності щодо

безпеки прагнуть надати якомога більше інформації. Як наслідок, працівники можуть нудьгувати, а їхній ентузіазм до навчання зменшується.

Відсутність організації: більшість процесів надання обізнаності про безпеку непослідовні.

Відсутність подальших дій: часто спостерігається великий ентузіазм на початку будь–якої нової інформаційної кампанії з безпеки, однак через деякий час цей ентузіазм може зменшитися або навіть зникнути. Для задоволення потреб співробітників потрібно прислухатися до них і збирати їх відгуки.

Відсутність підтримки керівництва: якщо не має належної та активної підтримки зі сторони керівництва, то будь–яке навчання не матиме сенсу [33].

Хоча багато методів використовуються для підвищення обізнаності співробітників щодо ІБ, вкрай важливо, щоб підприємства забезпечували їх ефективність [25]. Розглянемо дані методи:

- отримання інформації одразу: якщо інформація буде короткою, розуміння персоналом цієї інформації буде набагато легшим;
- цікава інформація: привернення уваги співробітників і мотивування їх бути зацікавленими. Наприклад, використання гумору ефективно сприяє заохоченню співробітників читати більше;
- використання реальних прикладів: використання теоретичних прикладів інцидентів безпеки не є доцільним, ефективне надання співробітникам реальних прикладів інцидентів безпеки є кращим варіантом;
- повсякденне нагадування та практикування заходів безпеки: співробітники повинні усвідомлювати свою щоденну діяльність за допомогою різноманітних методів інформування, таких як плакати чи електронні листи;
- використання правильних методів доставки: рівень освіти працівників явно різниться, і важливо використовувати метод інформування, який підходить працівникам [27].

ІБ – це безперервний процес, а не проєкт; тому плани з ІБ потрібно вивчати на безперервній основі, а професійні команди мають запровадити політики та

процедури, які підтримуються достатньою кількістю програм підвищення обізнаності щодо безпеки. Той факт, що більшість працівників не приділяють достатньої уваги інформаційній безпеці, призводить до того, що організація стає вразливою до значних загроз безпеці [35].

Забезпечення навчання персоналу з різних питань ІБ та як найкраще їх вирішення є ключем до гарантування потрібних відповідностей вимогам політиці безпеки. Отже, під час уроків підвищення обізнаності про інформаційну безпеку слід пропагувати політику безпеки, щоб забезпечити більшу відповідність. Щоб гарантувати більшу ефективність, програма інформування про інформаційну безпеку повинна будуватися на основі добре продуманої стратегії. Під час інформаційних програм співробітники повинні знати про таке:

- наявність політики безпеки;
- способи доступу персоналу до політики безпеки підприємства;
- практики, які слід використовувати для дотримання політики безпеки підприємства;
- важливість захисту інформаційних активів;
- які наслідки невиконання політики безпеки підприємства [36].

Багато стратегій використовуються для впливу, заохочення, мотивації та навчання працівників у зв’язку з підвищенням їх обізнаності щодо важливих питань ІБ. Переконливі технологічні стратегії включають: спрощення, тунелювання, персоналізацію, моніторинг, кондиціонування та пропозиції:

Спрощення: спрощення процесу та зведення його до мінімальної кількості дій. Спрощення обов'язків користувачів щодо безпеки допоможе їм зрозуміти необхідні завдання безпеки інформації. Тому завдання безпеки потрібно полегшити, скоротивши їх до якомога меншої кількості кроків.

Тунелювання: надання вказівок та підтримка користувачів, мотивування їх на цьому шляху. Використання послідовність завдань, для переконання того, що користувачі виконують кожен крок процесу втручання.

Персоналізація: персоналізація інформації для кожного користувача. Більш особистий підхід із індивідуальною інформацією є більш переконливим, ніж загальна інформація.

Моніторинг: статус або продуктивність користувача виконувати через повідомлення безпосередньо самому користувачеві.

Обумовлення: посилення цільової поведінки. Як правило, користувачі недооцінюють потенційні загрози чи ризики у своєму кіберпросторі й тому не вірять у важливість безпечної поведінки. Застосування різних методів підкріплення може допомогти сформувати бажану поведінку або змінити поточну поведінку на більш безпечні звички [27].

Співробітники повинні мати достатній рівень усвідомлення важливості ІБ та того, як захистити себе від зростаючих загроз. Лише технологічні рішення не можуть забезпечити повний захист. Тому обізнаність працівників щодо вимог безпеки відіграє додаткову роль у процесі захисту.

Застосування ефективних програм обізнаності про інформаційну безпеку є складним завданням. Людський фактор все ще залишається найслабшою ланкою в ланцюжку ІБ, в той час як спостерігається рух і збільшення кількості загроз безпеці.

Використання новітніх методів та засобів навчання та освіти дозволить покращити вже існуючі програми підвищення обізнаності персоналу на підприємстві, а також створити більш доскональні програми, які націлені на кожного співробітника підприємства.

1.3 Постановка задачі

Згідно з проаналізованими теоретичними матеріалами, відносно всіх антропогенних загроз, які можуть впливати на підприємство, з подальшим детальним розглядом внутрішніх та зовнішніх загроз, які можуть бути викликані людиною, був зроблений висновок о доцільності розробки програми підвищення обізнаності персоналу. Швидкий розвиток інформаційних загроз, приводить до

того, що важко за всім слідкувати, особливо, якщо ІБ не є основною спеціалізацією співробітника. Проведений аналіз матеріалів, на рахунок підвищення обізнаності персоналу на підприємстві показав, що методи якими користується персонал під час програми підвищення обізнаності в інформаційній безпеці не є доцільним для нашого часу. Багато з тих методів, що є, вже застаріли, а інформація, яка надається не актуальна.

На основі отриманих даних, були поставлені задачі на необхідність розробки програми підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою, а також розробка рекомендацій щодо організації підвищення обізнаності персоналу та засобів підтримки поінформованості персоналу на промисловому підприємстві.

1.4 Висновки до першого розділу

У першому розділі було проаналізовано внутрішні та зовнішні антропогенні загрози, які можуть впливати як на локального користувача мережі так і на мережу підприємства взагалі. Було виявлено, що головну загрозу інформаційній безпеці підприємства становить людина: як співробітник компанії (інсайдер), так і людина з зовні(хакер). Вони можуть мати однакові цілі, але діяти зовсім по–різному, через доступність до тих чи інших засобів, які допомагають їм досягти своєї мети. Також було досліджено якими видами зовнішніх і внутрішніх загроз людина може нанести шкоду на діяльність підприємства.

Далі було розглянуто методи та засоби підвищення рівня обізнаності персоналу на підприємстві, які з цих методів є більш ефективним. Обізнаність в інформаційній безпеці, в головному, залежить від людини. Знаючи як працюють зловмисники і які методи використовують, знижуються шанси на те, що підприємство чи сам співробітник зазнають атаки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка програми підвищення обізнаності персоналу

Розробка програми підвищення обізнаності співробітників потрібна для покращення інформування користувачів про ризики ІБ. Це потрібно для того, щоб мати можливість вплинути на поведінку користувачів і допомагати користувачам у прийнятті правильних рішень під час роботи з комп'ютерами та Інтернетом для виконання повсякденних обов'язків. Співробітники повинні знати про поширені схеми шахрайства та фішингу, про основні методи, які використовують зловмисники, щоб обманом змусити нічого не підозрюючих користувачів виконати ненавмисну дію. Добре розроблена програма підвищення обізнаності щодо кібербезпеки має сприяти організаційному навчанню та підтримувати загальну місію організації з точки зору безпеки інформації на підприємстві. Без організаційного навчання користувачам не вистачатиме досвіду чи навичок, щоб визначити загальні загрози для інформаційних систем, над якими вони працюють.

Документ NIST SP 800–50 «Створення програми підвищення кваліфікації та навчання безпеки інформаційних технологій» описує три компоненти успішних програм підвищення обізнаності щодо кібербезпеки.

1. Створення політики безпеки інформаційних технологій, яка відображає потреби бізнесу та спрямована на відомі ризики;
2. Інформування користувачів про їхні обов'язки ;
3. Визначення повторюваних процесів для моніторингу та перегляду програми.

Крім того, виділяють наступні компоненти розробки програми обізнаності персоналу:

- Залучення керівництва: вище керівництво повинно підтримувати програму інформування; користувачі будуть знати про участь вищого керівництва та реагуватимуть відповідно;

- Наполегливість: для програми підвищення обізнаності найкращою практикою є складання річного плану з конкретними віхами навчання протягом року;
- Актуальність: програми інформування про кібербезпеку мають відповідати користувачам, для яких саме розробляється дана програма та їхнім повсякденним завданням;
- Миттєвий зворотний зв'язок: Проведення практичного навчання підсилює заходи з підвищення обізнаності, охоплені кампанією чи програмою;
- Оцінювання: щоб визначити будь–які необхідні коригування, потрібно зрозуміти, з чого розпочинається програма та як вона просувається.

Беручи все це до уваги, програма підвищення обізнаності про кібербезпеку повинна бути застосована до всіх співробітників підприємства, при цьому керівництво має брати на себе провідну роль і подавати приклад для всіх користувачів. Програма підвищення обізнаності про кібербезпеку функціонує як засіб розповсюдження інформації всередині організації та підтримується в актуальному стані, вносячи корективи відповідно до поточних загроз і змін у тому, як організація реагує на загрози. Ефективна програма підвищення обізнаності щодо кібербезпеки повинна інформувати та навчати персонал щодо політики безпеки та оновлень політик і процедур ІБ з метою відповідності. Зрештою, користувачі повинні знати, що від них очікується, і будь–яке невідповідність виправдовуватиме відповідальність. Програма підвищення обізнаності з питань кібербезпеки формує добре поінформовану робочу силу, яка чітко усвідомлює очікування, ризики та загрози, що призведе до підвищення безпеки для підприємства в цілому [36].

Перед початком розробки програми підвищення обізнаності персоналу треба спочатку мати чітке розуміння середовища, для якого буде розробляться дана програма. Слід враховувати наступні пункти:

- ролі та обов'язки;
- зовнішні або допоміжні зацікавлені сторони;

- існуючу політику безпеки, положення та законодавство;
- культуру кібербезпеки;
- бюджет.

Усі ці фактори необхідно враховувати під час проєктування та реалізації ефективної програми з підвищення обізнаності. Це допоможе визначитись з тим, в якому напрямку рухатися під час розробки програми, хто повинен нести відповідальність за розробку та реалізацію програми та як це на вже існуючі устої на підприємстві. Це також допоможе визначити аудиторію, цілі та завдання програми [37].

Ролі та обов'язки. Функціонування команд, на які поділені співробітники, та їх координування потрібно для загального розуміння ролей та обов'язків кожного співробітника в рамках організаційної або командної архітектури. Часто люди не розуміють, як виконувати ці ролі та обов'язки так, щоб досягти значних результатів. Важливими при запуску програми підвищення обізнаності з ІБ є розуміння конкретних політик безпеки для подальшого розуміння відповідальних сторін під час проєктування, розробки та впровадження програми підвищення обізнаності з кібербезпеки.

Додаткові зацікавлені сторони. При розробці програм підвищення обізнаності щодо кібербезпеки можуть бути створенні додаткові групи для залучення протягом всіх етапів розробки та впровадження програми. Таблиця 2.1 визначає додаткові групи [38].

Таблиця 2.1 – Додаткові групи зацікавлених сторін для розробки та впровадження програми обізнаності персоналу

Зацікавлена сторона (стейкхолдер)	Будь–яка організація, яка має інтерес або яка має проблему, що пов'язана з вашим підприємством. Не може безпосередньо обслуговуватися організацією/командою, але може отримати значні переваги. Організації можуть надавати вхідні дані, такі як фінансування, персонал, політика, поради та

Продовження таблиці 2.1

	вказівки.
Додаткова складова	Підмножина зацікавлених сторін. Організації або установи, які будуть обслуговуватися організацією/командою.
Спільнота	Більш широкий набір дотичних і пов'язаних організацій, які мають певні стосунки з вашою організацією/командою.

Регламент або законодавство. Обізнаність про кібербезпеку має на меті формувати поведінку користувачів для підтримки ІБ. Це включає в себе знання організаційних правил, політики безпеки та інших вимог. Ці вимоги часто визначаються та повідомляються в політиці ІБ. Нормативні вимоги, такі як описання поведінки користувача щодо захисту інформації та використання комп'ютера, можуть надаватися організації на національному, державному, місцевому та/або організаційному рівні. Користувач, який не вживає відповідних дій або поводиться неприйнятно з огляду на встановлені заходи, не тільки не відповідає вимогам, але й призводить до того, що організація не відповідає вимогам. Як правило, відповідність нормативним вимогам стосується певних галузей або секторів. При розробці та впровадженні програми підвищення обізнаності з кібербезпеки важливо враховувати та включати існуючі та застосовні нормативні акти. Ось кілька прикладів нормативних актів, які можуть стосуватися певних країн, регіонів і секторів [37].

Культура кібербезпеки. Програми підвищення обізнаності персоналу, в питаннях пов'язаних з інформаційною та кібербезпекою знайомлять користувачів із безпечними онлайн–практиками та допомагають їм розвивати навички, які вони використовуватимуть як на роботі, так і в особистому житті. Успішні програми підвищення обізнаності об'єднують керівників організацій навколо спільної мети підвищення обізнаності –захисту активів і ресурсів підприємства, пов'язаних з інформаційними технологіями. «Підтримуючи» цілі

безпеки підприємства(і будуючи організаційну культуру з усіма співробітниками та користувачами), керівники підвищують обізнаність щодо кібербезпеки та створюють міцну культуру безпеки. Культуру кібербезпеки організації можна охарактеризувати як аспект ширшої організаційної культури, яка заохочує співробітників і користувачів виконувати свої обов'язки відповідно до політики безпеки організації [37].

Бюджет. Важливо розуміти фінансування та ресурси з самого початку програми. Це дає змогу адекватно охопити програму та визначити, скільки заходів (і якого рівня) буде запропоновано. Розуміння та управління бюджетом може бути складним, але це важливо для забезпечення масштабу та успіху програми з підвищення обізнаності співробітників щодо кібербезпеки.

Розробляючи програму або кампанію з підвищення обізнаності, важливо, щоб програма підтримувала бізнес–потреби організації та доповнювала вже існуючу організаційну культуру, а також не шкодила вже існуючим та усталеним правилам. Ці програми мають бути розроблені з метою підтримки місії організації у відповідності з потребами безпеки організації чи групи. Крім того, користувачі повинні знайти програму, що відповідає їх повсякденній діяльності. Програма підвищення обізнаності з кібербезпеки розробляється, для того, щоб доповнювати обізнаність, потреби та цілі організації чи групи.

Розробка програми починається з визначення основних компонентів даної програми:

1. Розуміння політики безпеки підприємства.
2. Визначення ролей та відповідних їм обов'язки.
3. Визначення моделі.
4. Проведення оцінки потреб.
5. Розробка стратегії.
6. Розробка плану програми.
7. Інформаційні матеріали для програми.
8. Впровадження програми.

9. Проведення програми підвищення обізнаності персоналу.
10. Проведення заходів після впровадження даної програми.

Політика безпеки промислового підприємства має на меті захист інформаційних ресурсів від можливого нанесення їм матеріальних, фізичних, моральних та інших шкод, за допомогою випадкового чи навмисного впливу на інформацію, її носії, процеси обробки та передачі, а також мінімізація ризиків ІБ. Зазначена мета досягається шляхом забезпечення властивостей об'єктів захисту, таких як доступність, цілісність та конфіденційність. Дія політики безпеки розповсюджується на все підприємство в цілому та використовується для всіх бізнес–процесів підприємства, які можуть негативно вплинути на підприємство. Забезпечення необхідного рівня функціонування підприємства відбувається за рахунок: всіх автоматизованих систем підприємства (апаратні та програмні засоби); приміщень, в яких розташовані елементи автоматизованої системи підприємства; інформації, яка обробляється і зберігається в автоматизованій системі підприємства. Підприємство керується такими принципами, як законність; залучення вищого керівництва; економічна доцільність; комплексність та системність; персональна відповідальність; врахування вимог ІБ у проєктній діяльності. В свою чергу керівництво зобов'язане забезпечити підтримку та вдосконалення систем управління інформаційною безпекою підприємства відповідно стандарту ISO 27001, доведення всіх вимог політики безпеки підприємства до кожного співробітника, а також забезпечити всі системи управління інформаційною безпекою підприємства потрібними ресурсами для досягнення відповідних поставлених цілей [39].

Відповідно до NIST SP 800–50 [38] потрібно розглянути ролі на промисловому підприємстві та відповідні ролям обов'язки персоналу, який буде розробляти програму. Дані ролі наведено в Таблиці 2.2.

Таблиця 2.2 – Ролі та обов'язки персоналу, який буде розробляти програму на підприємстві

Голова організації чи підприємства	Призначення відповідальності для відділів інформаційних технологій та ІБ. Переконання в тому, що програма реалізована.
Голова відділу інформаційних технологій або відділу ІБ	Створення загальної обізнаності щодо даної програми та створення відповідних стратегії. Переконання в тому, що всі керівники розуміють розроблену програму, а також поінформовані про хід і виконання цієї програми.
Менеджер програми з підвищення обізнаності персоналу	Забезпечення в ознайомлені та розроблених навчальних матеріалів, які є доречними та своєчасними для цільової аудиторії.
Інші менеджери	Обговорення з керівниками відділів для роз'яснення їх відповідальності в програмі. Переконання в тому, що всі користувачі пройшли належну та відповідну підготовку для виконання обов'язків щодо кібербезпеки для систем, до яких вони мають доступ.
Користувачі	Дотримання політик безпеки та процедур кібербезпеки на підприємстві. Проходження належного навчання, правил поведінки та вивчення матеріалів, до яких вони мають доступ.
Інші зацікавлені сторони	Приймання участі в розробці та впровадженні програми з підвищення обізнаності персоналу в відповідній ролі.

Далі треба визначити модель програми підвищення обізнаності. Відповідальність за адміністрування різних аспектів програми інформування про кібербезпеку може бути централізованою або розподіленою залежно від організаційної структури та наявних ресурсів. NIST SP 800–50 визначає три загальні підходи до проєктування, розробки та впровадження програми інформування про кібербезпеку:

Модель 1: Централізована політика, стратегія та реалізація

Модель 2: Централізована політика та стратегія, розподілена реалізація

Модель 3: Централізована політика, розподілена стратегія та реалізація

Усі три моделі показують централізовану політику.[36] Використання будь–якої з них потребує первинного аналізу підприємства, тому що в залежності від розміру підприємства; IT–інфраструктури; обов'язків співробітників які є на кожному рівні підприємства; функцій, які виконуються кожним учасником підприємства; наявність автономних відділів з окремими завданнями; можна обрати лише одну, підходящу до підприємства модель. Кожна з моделей має свої плюси та недоліки.

Для більшості промислових підприємств притаманна 1 модель – централізована політика, стратегія та реалізація. У централізованій моделі управління програма обізнаності про кібербезпеку, стратегія та плани реалізації централізовані та керовані центральною владою. Це означає, що всі директиви щодо розробка стратегії поінформованості, планування моделі, реалізація і будь–яка координація здійснюється центральним органом.

Плюси даної моделі:

1. Центральний орган керує всіма аспектами програми підвищення обізнаності з кібербезпеки;
2. Він добре працює зі структурованим та централізованим керуванням IT–функціями;
3. Організаційні підрозділи допомагають у міру необхідності.

Мінуси даної моделі:

1. Можливо, бракує даних організаційного підрозділу;
2. Зміни до матеріалів програми інформування можуть бути відкладені через обмеження центральної влади;
3. Зміни до матеріалів програми інформування проводяться центральним органом і можуть не відображати точний стан, пріоритети або проблеми в організаційному підрозділі [37].

Незалежно від обраної моделі, необхідно провести оцінку потреб, щоб визначити з чого треба починати програму обізнаності персоналу. Оцінка потреб – це процес, який може допомогти визначити стан вашої організації щодо обізнаності з кібербезпеки, виявити прогалини в навчанні та розумінні, і, як результат, визначити потреби вашої організації в обізнаності з кібербезпеки.

На підприємствах є багато джерел, які можна використовувати, щоб допомогти визначити потреби в обізнаності з ІБ. Крім того, NIST SP 800–50 надає різні методи, які можна використовувати для збору цієї інформації, включаючи:

- інтерв'ю з ключовими групами на підприємстві;
- опитування;
- огляд планів ІБ для загальних систем підтримки;
- аналіз результатів будь–яких керівних і наглядових органів;
- аналіз інцидентів і подій ІБ;
- огляд будь–яких технічних та інфраструктурних змін;
- дослідження поточних подій і тенденцій, виявлених у сфері ІБ;
- будь–які показники отримані в результаті попередніх заходів з підвищення обізнаності щодо кібербезпеки [37].

Перед тим як розробляти саму програму підвищення обізнаності треба розробити стратегію та план даної програми.

Стратегія програми стосується основних питань, які передбачені NIST 800–50:

- будь–яка національна, регулятивна чи місцева політика, яка вимагає проведення заходів з підвищення обізнаності з кібербезпеки;
- обсяг програми підвищення обізнаності з кібербезпеки;
- ролі та обов'язки тих, хто розробляє та впроваджує програму підвищення обізнаності з кібербезпеки;
- цілі, яких потрібно досягти для кожного аспекту програми: навчальні цілі; теми, які потрібно розглянути;

- цільова аудиторія та застосовність програми до конкретної аудиторії [38].

Стратегія програми це спосіб досягти цілей та показників програми. Тобто, стратегія програми підвищення обізнаності персоналу щодо кібербезпеки відповідає головній меті створення даної програми – підвищення рівня обізнаності персоналу на промисловому підприємстві в інформаційній та кібербезпеці. Без стратегування всі цілі та бажані наслідки, у вигляді забезпечення більш безпечного інформаційного середовища, не будуть досягнені, тому що буде велике розмаїття всього та фокус зміститься на якусь іншу ціль, яка не є головною.

Коли стратегія інформування про кібербезпеку завершена та узгоджена, далі відбувається створення плану програми та графік її впровадження на підприємстві. Впровадження програми може робитися поетапно, якщо існують обмеження щодо бюджету чи ресурсів [37].

Розробка плану програми обізнаності персоналу в питаннях інформаційної та кібербезпеки розробляється відповідно до стратегії і стає головним компонентом для створення плану, так як стратегія формується на основі головної цілі даної програми. Але окрім стратегії потрібно розуміти всі вище перелічені аспекти: розуміння політики безпеки підприємства; визначення ролей та відповідних їм обов'язки; визначення моделі; проведення оцінки потреб. Все це формує план програми і якщо не буде враховано один з цих пунктів, то сам план не буде доцільним.

Оскільки всі пункти були враховані, то план програми підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою на промисловому підприємстві виглядає наступним чином:

1 Ландшафт загроз:

1.1 Онлайн, нова лінія фронту:

1.1.1 Орієнтування;

1.1.2 Розмови про інформаційну безпеку на промисловому підприємстві: основи;

1.1.3 Порушення в кібербезпеці;

1.1.4 Кібератаки на промисловому підприємстві;

1.1.5 Опис порушень кібербезпеки;

1.1.6 Інвентаризація інформаційних ресурсів підприємства;

1.1.7 Тестування.

1.2 Розуміння поточних загроз:

1.2.1 Розуміння поточних загроз на промисловому підприємстві;

1.2.2 Виявлення вразливих інформаційних систем на промисловому підприємстві;

1.2.3 Знання своїх ворогів;

1.2.4 Тестування.

1.3 Захист особистої цифрової інформації:

1.3.1 Захист особистої цифрової інформації;

1.3.2 Загрози особистим активам;

1.3.3 Тестування;

1.3.4 Підсумок пройдених тем.

2 Автентифікація:

2.1 Ким хакери вважають інших людей?:

2.1.1 Паролі – ключі;

2.1.2 Паролі – для чого вони потрібні?;

2.1.3 Що відбувається, коли ви вводите пароль?;

2.1.4 Тестування.

2.2 Покращення безпеки пароля:

2.2.1 Покращення безпеки пароля;

2.2.2 Як обрати належний пароль, який підходить для корпоративної мережі підприємства?;

3.2.7 Роль шкідливого програмного забезпечення в клікфорді (скликування рекламних оголошень);

3.2.8 Ботнети;

3.2.9 Тестування.

3.3 Тримання шкідливого програмного забезпечення на відстані:

3.3.1 Захист всіх даних підприємства за допомогою Антивірусного ПЗ;

3.3.2 Антивірусне ПЗ;

3.3.3 Бути у курсі подій;

3.3.4 Кінець життєвого циклу ПЗ;

3.3.5 Пісочниці (середа безпечного тестування) та підписані програми;

3.3.6 Тестування;

3.3.7 Підсумок пройдених тем.

4 Загальне тестування за всіма темами.

Модуль “Ландшафт загроз” включає в себе лекції та обговорення, а також статті та відео–матеріали на відповідну тему. Цей модуль дозволяє: дослідити ландшафт загроз інформаційній безпеці; вивчити основні прийоми захисту корпоративного та особистого комп'ютерів; дізнатися про різні види загроз, уразливості якими загрози користуються; вивчити контрзаходи, які можна вжити для захисту від загроз; зрозуміти, як захистити особисту цифрову інформацію. Після вивчення кожної теми проводиться тестування. Мета тестування – встановлення рівня засвоєного матеріалу та аналіз помилок, для детального розбору неправильних відповідей та роботи над помилками.

В модулі “Автентифікація” вивчається: основний спосіб автентифікації користувача; способи покращення безпеки паролів; які стратегії використовуються під час вибору паролів; як працює двофакторна автентифікація; як запровадити двофакторну автентифікацію в облікових засобах. Модуль висвітлює важливість захисту корпоративних даних за рахунок

створення пароля, який не можливо легко взламати. За рахунок лекцій та презентацій з відповідної теми, вданому модулі використовують відео–матеріали.

Модуль “Шкідливе ПЗ” повинен навчити користувачів:

- які є типи зловмисного програмного забезпечення, як вони розвивалися та яку шкоду можуть завдати;
- як захиститися від зловмисного програмного забезпечення;
- які бувають види антивірусного програмного забезпечення та поради щодо виявлення фішингових електронних листів.

Цей модуль включає в себе інформування за рахунок презентації та паралельно проводження лекції. Окрім того, в даному модулі виступає запрошена людина з органів правопорядку, яка розповість саме про фішингові атаки на підприємствах та як їх запобігти.

ІМП – це різні матеріали та предмети споживання, які використовуються для виконання завдань проєкту. Використання різносторонніх інформаційних матеріалів – один з головних ключей ефективності та результативності програми. Джерела матеріалів повинні мати відповідне підтвердження, для того щоб не поширювати недостовірну інформацію на велику аудиторію співробітників підприємства. В випадку програми підвищення обізнаності персоналу, всі інформаційні матеріали беруться у статтях, книгах та в інших засобів, які доступні в Інтернеті. Під іншими засобами розуміється відео матеріали, рольові ігри, комп'ютерні ігри, різноманітні тести для перевірки знань, які пов'язані безпосередньо з темами програми та мають на меті змінити метод отримання інформації для більш успішного засвоєння інформації.

Програма підвищення обізнаності персоналу розробляє наступні види інформаційних матеріалів для навчання та подальшого забезпечення важливою інформацією після закінчення програми, як:

- залучення запрошеного спікера з правоохоронних органів для розмови про фішинг та як захиститися від нього;

- випуск веселого мікровідео з місцевими працівниками в ролі акторів з актуальної теми, яка стосується ІБ на підприємстві;
- проведення онлайн–сесії з керівництвом для обговорення важливих питань щодо кібербезпеки;
- публікація щомісячного подкаст від відділу ІБ або відділу інформаційних технологій;
- розсилання інфографіки про те, як створити безпечний середовище навколо себе та свого робочого місця;
- інформування через пошту на рахунок нових видів загроз інформаційній безпеці;
- створення сайту для програми підвищення обізнаності з метою покращити доступність викладеної інформації.

Етап впровадження програми – це те, де програма оживає. Підприємство та голова проєкту вирішують, чи проводитиметься навчання власними силами чи координуватиметься ззовні. Реалізація програми повинна враховувати залученість співробітників і цілі програми, а також ретельне планування розкладу навчальних заходів і будь–яких пов'язаних ресурсів (приміщення, обладнання, процес створення, анкети тощо). Потім програма навчання офіційно запускається, рекламується та проводиться. Під час навчання відстежується прогрес учасників, щоб переконатися в ефективності програми [39].

Програма підвищення обізнаності персоналу в питаннях пов'язаних з інформаційною та кібербезпекою на промисловому підприємстві проводиться в 3 етапи: кожний етап займає 1 тиждень. Тобто, вся програма займає лише 3 тижня. Це доволі середній термін для програми. Впровадження програми може займати як 1 тиждень, так і декілька місяців, але чим довше проходить навчання, тим складніше засвоюється матеріал, і на виході отримаємо незадовільний результат від самої програми, а якщо впровадити програму протягом 1 тижня – отримаємо той самий результат, що із декількома місяцями навчання: багато інформації потрібно вивчити за маленький проміжок часу, що в свою чергу

призводить до не запам'ятовування чи переплутування вивчених матеріалів. А оскільки, дана програма впроваджується протягом робочого дня, то співробітникам ще потрібно виконувати свої прямі обов'язки, тобто 3 тижня це “золота середина” для програми підвищення рівня обізнаності персоналу.

Проведення програми підвищення обізнаності персоналу здійснюється співробітника підприємства зі знаннями та досвідом у галузі інформаційної та кібербезпеки. Немає нічого гіршого, ніж бути в класі з учителем, який не знає, чого навчати. Найкращий варіант – використання внутрішнього співробітника або зовнішнього джерела професійного навчання (лектор з університету чи з курсів). Ефективна навчальна програма дозволяє співробітникам брати участь у навчальному процесі та розвивати свої навички та знання. Співробітників слід заохочувати брати участь у процесі навчання, беручи участь в обговореннях, ставлячи запитання, вносячи свої знання та досвід, навчаючись через практичний досвід.

Після впровадження програми одним із способів переконатися, що програма досягає своїх цілей, є оцінка студентами та викладачами навчання. Оцінки допомагають визначити рівень навчання та те, чи покращились знання співробітника та як це впливає на інформаційну систему підприємства в цілому. Оцінити успішність програми можна за допомогою:

1. Кінцевий відгук: написання чесного та змістовного відгуку кожного учасника програми після завершення цієї програми для подальшого аналізу та оцінювання даної програми.

2. Додатковий (заключний) семінар: отримання змістовних відповідей наживо допомагає більш краще зрозуміти переваги та недоліки програми.

3. Тестування: проведення кінцевого (загального) тестування за програмою допомагає зрозуміти які теми не були достатньо вивчені, що треба додати та покращити в програмі.

4. Атаки: відправлення провокаційних повідомлень через електрону пошту для перевірки персоналу щодо їх нових знань.

5. Результат: успішність програми буде доведена, коли знизиться кількість ризиків для ІБ зі сторони співробітників.

Результати опитування після проходження програми підвищення обізнаності показали наступне:

- розпізнавання масованої фішингової атаки зросло з 23% до 68%;
- розпізнавання цільових електронних листів зросло з 27% до 63%;
- розпізнавання вебшахрайства зросло з 24% до 57%;
- показник співробітників, які можуть загрожувати інформаційній безпеці підприємства знизився від 38% до 12%;
- показник обізнаності персоналу, який пройшов програму зріс від початку програми на 74%.

Результати розробки програми підвищення обізнаності персоналу з інформаційної та кібербезпеки показують, що відсоток співробітників, які впровадили вивчені матеріали в свою діяльність значно виріс, що говорить про правильність створення даної програми.

2.2 Розробка рекомендацій щодо організації підвищення обізнаності персоналу

Співробітники підприємства є слабкою ланкою для інформаційної системи даного підприємства, особливо коли мова йде про створення та посилення заходів кібербезпеки на підприємстві. Рівень ІБ підприємства зводиться до того, наскільки добре персонал вивчив те, як боротися та запобігати кібератакам, незважаючи навіть на впровадження, удосконалення, постійне оновлення та підтримку всім заходів кібербезпеки. Співробітники це головна лінія захисту інформації на підприємстві, тож для того щоб вони змогли чітко та кваліфіковано надати відповідь кіберзлочинцям для цього і розробляються рекомендації щодо організації підвищення обізнаності персоналу на промисловому підприємстві. В даному випадку, рекомендація щодо організації програми підвищення обізнаності співробітників це лише поради про, те як та що потрібно робити в

різних ситуаціях пов'язаних з кібербезпекою. А тепер, розглянемо кожну розроблену рекомендацію.

1. Надання пріоритету кібербезпеці на підприємстві.

Успіх програми підвищення обізнаності персоналу, в питаннях пов'язаних з інформаційною та кібербезпекою, залежить від впровадження та подальшої її реалізації на підприємстві.

Потрібно чітко розуміти, які групи співробітників є слабкими, для того щоб негайно отримати вигоду від навчання з кібербезпеки. Слабкі групи співробітників – це категорія людей, які зневажають будь–якими правилами ІБ або просто їх не знають. Ця група є головною загрозою інформаційній безпеці промислового підприємства. Аналіз всього персоналу підприємства та виявлення таких співробітників, формування їх в групу та подальше навчання робиться для зменшення основних ризиків для ІБ. Тому важливо розробляти програму підвищення рівня обізнаності спираючись на те, що знання співробітників з інформаційної та кібербезпеки є різними, тому важливо першочергово знайти та розділити персонал по рівню знань, а пріоритетом навчання програмі зробити тих людей, які мають слабкий рівень обізнаності з кібербезпеки або не мають його взагалі.

Розробка програми підвищення обізнаності персоналу окупиться в довгостроковій перспективі через усунення прогалин в інформаційній та кібербезпеці.

2. Залучення керівництва до участі в програмі.

Участь вищого керівництва в програмі підвищення обізнаності з кібербезпеки показує високий пріоритет, який має ця програма, наскільки вона важлива не тільки для захисту особистих даних співробітників від кібератак, а й для правильного функціонування інформаційної системи підприємства в цілому.

Проходження програми вищим керівництвом звертає увагу всіх співробітників. Завдяки такої участі в програмі підвищення обізнаності з кібербезпеки співробітники розуміють, що навчання потрібно і важливе не

тільки для простих співробітників, а ще й для керівників відділів та головного керівництва підприємства.

Все це робиться для формування спільного розуміння розвитку підприємства в питаннях, пов'язаних з інформаційною безпекою та, застосовування вивчених на програмі знань та практик для безпечного функціонування інформаційних систем підприємства, реалізація поєднання теорії та практики для підвищення не тільки власної цінності персоналу, але й для того, щоб забезпечити більшу життєздатність підприємства, у той же час, надихнути потенціал персоналу.

3. Пропагування найкращих методів та засобів кібербезпеки, підкріплені політиками безпеки та стандартами.

Використання найкращих методів та засобів під час навчання програмі підвищення обізнаності персоналу та після закінчення програми, для підтримки вже існуючого рівня знань та вивчення нових матеріалів з кібербезпеки має на меті захист співробітників, їх особистих даних, а також захист всіх інформаційних автоматизованих систем від кібератак.

Навчання за допомогою таких методів та засобів несе тільки позитивний характер. Кожний метод чи засіб, який використовується для вивчення інформаційної та кібербезпеки повинен бути зорієнтован на відповідні групи співробітників, кожна з яких має певний рівень знань з кібербезпеки.

Засоби, через які відбувається вивчення програми дуже різняться. В залежності від виду доставки потрібної інформації, засоби ділять на паперові та електронні. Паперові методи та засоби не мають необхідної залученості співробітників в надану, через паперові носії, інформацію. Але деякі паперові засоби, наприклад, плакати має непоганий відгук серед персоналу. Електронні методи та засоби зараз головне джерело через яке проходить вивчення програми. Це мультимедійні види інформування (презентації, відео, інфографіки) та інші види, наприклад, запобігання фішингових атак через розсилку співробітникам

листів, що повинно навчити персонал відрізняти фішинговий лист від спам–листа.

Розробка надійних політик безпеки лежить в основі програми підвищення обізнаності персоналу. Створення ефективної політики ІБ підприємства, яка відповідає всім вимогам відповідності, є критично важливим кроком у запобіганні інцидентам безпеки. Політики ІБ мають такі переваги для ІБ підприємства:

- Сприяє цілісності, доступності та конфіденційності даних. Ефективні політики безпеки інформації стандартизують правила та процеси, які захищають цілісність, доступність та конфіденційність даних;
- Захищає конфіденційні дані. Політика ІБ надає пріоритет захисту інтелектуальної власності та конфіденційних даних, таких як особиста інформація чи інформація підприємства;
- Мінімізує ризик інцидентів безпеки. Політика ІБ допомагає підприємствам визначити процедури для виявлення та пом'якшення вразливостей і ризиків;
- Допомагає відповідати нормативним вимогам. Створення політики ІБ може допомогти організаціям виявити прогалини в безпеці, пов'язані з нормативними вимогами, і усунути їх [41].

Стандарти з інформаційної та кібербезпеки також лежать в основі не тільки програми підвищення рівня обізнаності персоналу, а й в основі будь–яких документів та політик безпеки, які використовуються для інформаційних систем підприємства. Прикладами таких стандартів є: ISO 27000, ISO 27001, ISO 27002, ISO 27005, NIST SP 800.

Пропаганда різних методів та засобів, на основі політики безпеки підприємства та міжнародних стандартів є наріжним каменем для розробки програми підвищення обізнаності співробітників та вивчення інших питань, пов'язаних з кібербезпекою, які запроваджені цими документами.

4. Запровадження кібербезпеки з першого дня

Найефективнішим способом підвищення обізнаності з інформаційної та кібербезпеки – це почати з першого дня. Під час створення, ще на початку, підприємства вже необхідно запровадити не тільки політики безпеки, які будуть використовуватись для безпеки всіх інформаційних систем на підприємстві, а ще створити інструктажі з кібербезпеки та певну програму з питань інформаційної та кібербезпеки, тобто співробітник одразу проходить навчання, шо в свою чергу одразу зменшує кількість ризиків безпеки, а ніж запровадження програми підвищення обізнаності персоналу вже в давно усталену систему зі своїми порядками.

Окрім основних питань з кібербезпеки, кожен співробітник, з першого дня, розуміє всі свої обов'язки перед безпекою інформаційного систем та конфіденційних даних.

5. Проведення регулярних навчань з програми підвищення обізнаності персоналу з кібербезпеки.

Регулярність – основний ключ для вивчення нових та повторення старих матеріалів. Чим частіше проводиться навчання, тим більш безпечними становляться ІС підприємства. Навчання може бути не тільки під час програми, а й, наприклад, між двома програмами, якщо є необхідність або ж зацікавленість зі сторони персоналу. Додаткове навчання, окрім регулярних 4 програм підвищення обізнаності персоналу на рік, може відбуватися через безкоштовні курси в Інтернеті.

Занадто часте проводження програми є недоцільним. Звісно, кіберзлочинці кожен день вигадують нові способи заволодіння інформацією, але види атак дуже схожі, тому часте проведення програми підвищення обізнаності персоналу буде впливати лише на роботу співробітників в погану сторону. А занадто рідкісне навчання з програми призведе до збільшення ризиків інформаційній безпеці підприємства через забування вивченого матеріалу.

6. Здійснення навчання з програми підвищення обізнаності персоналу обов'язковим для всіх.

Незалежно від посади працівника в компанії, кожен повинен знати про всі можливі загрози інформаційній безпеці підприємства. Безпека інформаційних систем потребує проходження програми для кожного співробітника підприємства, незважаючи на його посаду.

Рівень знань з кібербезпеки не сильно відрізняється в керівника відділу від працівника відділу, теж саме стосується і вищого керівництва. Тому помилки, в не залежності від посади, допущені через незнання основних правил та вимог з кібербезпеки підвищують кількість ризиків інформаційній безпеці підприємства.

Примусове навчання не принесе користі ні співробітнику, ні інформаційній безпеці, тому треба заохочувати співробітників або мати точки тиску, якщо це необхідно. Програма повинна бути цікавою та корисною для всіх, щоб кожен співробітник знайшов для себе потрібну інформацію.

7. Запровадження тренувань та різних вправ з кібербезпеки.

Виконання регулярних вправ підчас та після програми підвищення обізнаності персоналу є цікавим метод навчання. Наочні приклади повинні навчити знаходити загрози особистим даним та інформаційним системам. Це дуже популярний метод навчання через його інтерактивність та залучення до процесу всіх учасників групи програми. Інформація засвоєна на особистих прикладах або через певні ситуації краще запам'ятовується, а ніж проста лекція. Розглянемо конкретну вправу.

Вправа: Шкідливе ПЗ

Сценарій: співробітник підприємства використовував цифрову камеру підприємства для службових цілей. Під час цього було зроблено мальовничу фотографію, яка потім була завантажена на персональний комп'ютер співробітника, вставивши SD–карту. Карта SD була заражена шкідливим програмним забезпеченням під час підключення до персонального комп'ютера працівника. Коли його повторно вставили в комп'ютер компанії, він заразив систему організації тим самим шкідливим програмним забезпеченням.

Яка ваша відповідь?

Питання для обговорення:

1. Кому на підприємстві вам потрібно буде повідомити про це?

2. Як би підприємство виявляло та реагувало на зараження зловмисним програмним забезпеченням системи через цей вектор?

3. Який процес ідентифікації переносника інфекції?

1.1 Які інші пристрої можуть становити подібну загрозу?

1.2 Що має робити керівництво?

1.3 Як ви можете запобігти повторенню цього?

Перевірені процеси: здатність до виявлення/обізнаність користувача.

Загрозливий діяч: випадковий інсайдер.

Постраждалий ресурс: цілісність мережі.

Сценарії вправ можуть мати різні теми, але націлені вони на одне – щоб співробітник правильно використовував наданий йому матеріал у випадках кіберзагроз та міг розуміти як себе поводити при цьому [42].

8. Підтримання ліній зв'язку відкритими

Відгуки підчас та після закінчення програми підвищення обізнаності персоналу, відповіді на наявні питання поштою, особисто або через месенджери – все це допомагає розвивати та доповнювати програму новою необхідною інформацією. За наявністю питань під час семінарів або лекцій можна також зрозуміти чи була зрозуміла викладена тема.

Кількість загроз інформаційній безпеці промислових підприємств безперервно зростає. Підприємства повинні усвідомити небезпеку, яку створює ця загроза, і вжити необхідних заходів із залученням усіх зацікавлених сторін. Значна частка атак виникає через недбалість співробітників, що призводить до збитків. Зважаючи на поширеність загроз безпеці, підприємствам необхідно зосередитися на підвищення обізнаності співробітників, проводячи регулярно програми підвищення обізнаності персоналу з інформаційної та кібербезпеки.

2.3 Розробка засобів підтримки поінформованості персоналу

Програма підвищення обізнаності персоналу впроваджується, щоб поінформувати користувачів про проблеми та концепції ІБ на промисловому підприємстві. Успіх програми підвищення обізнаності про кібербезпеку залежить від того, як вона доводиться до користувача. Існують різноманітні методики доставки інформації до користувачів під час навчання. Використання всіх методів в програмі не є обов'язковим, але методи повинні бути орієнтовані відповідно до кількості співробітників, які приймають участь в програмі, в залежності від цілей програми, наявності відповідного забезпечення, яке присутнє на підприємстві. Все методи навчання та доставки корисної інформації до кінцевого користувача повинні спонукати до участі в програмі, заохочувати ефективне навчання.

В програмі підвищення обізнаності персоналу та подальшого підтримання поінформованості співробітників використовуються наступні методи та засоби:

Звичайні методи: електроні або паперові матеріали.

До електронних матеріалів слід відносити: електронні листи, які ознайомлюють з новою та важливою інформацією щодо кібербезпеки; електронні бюлетені; розробка та розповсюдження інфографіки, яка стосується тем інформаційної та кібербезпеки.

Інформування через електронні листи не є дуже практичним, тому що співробітник може просто не мати часу прочитати лист відразу, а потім співробітник отримає нові листи і лист з новою інформацією просто загубиться.

Електронні бюлетені, як і паперові випускаються періодично та використовуються для посилення програми інформування про кібербезпеку; Головна перевага бюлетенів – це те, що вони можуть передавати кілька повідомлень одночасно. Однак, незважаючи на те, що інформаційні бюлетені можуть зацікавити певну групу, немає гарантії, що користувач прочитав та зрозумів весь матеріал написаний в інформаційному бюлетені.

Інфографіка – це добірка зображень або діаграм і мінімального обсягу тексту, що роблять огляд теми легкозрозумілою. Інфографіка є більш новим засобом ознайомлення з новою інформацією, тому що мінімальна кількість тексту не дає загубитися в інформації, а ще й представлена у вигляді картинки, яку можна завантажити та встановити на робочій стіл, чи роздрукувати та повісити біля робочого місця. Інфографіка, що представлена на рисунку 2.1, інформує співробітників про ризик втрати корпоративних даних через не усвідомлення співробітниками самих ризиків та їх щоденної поведінки.

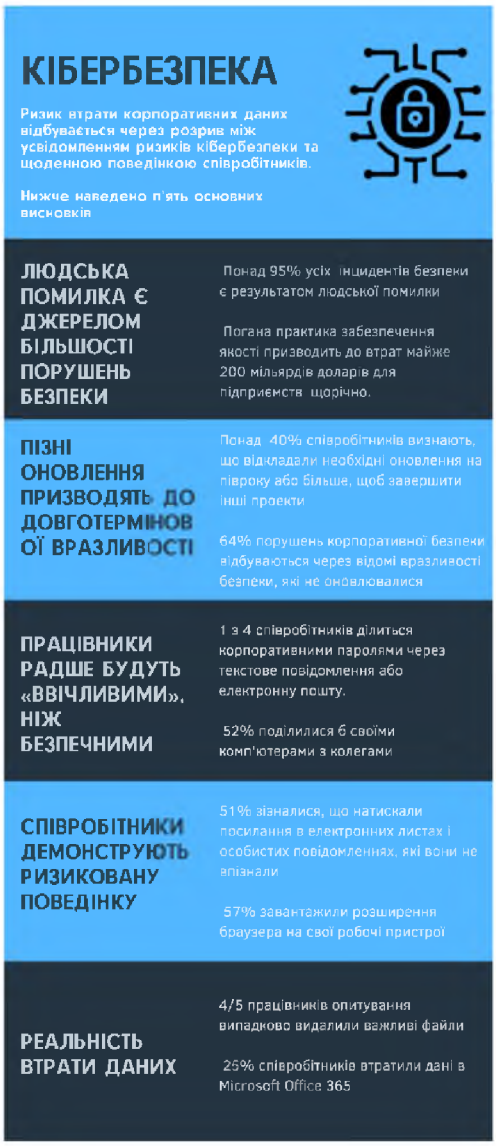

Рисунок 2.1 – Інфографіка з кібербезпеки

До паперових матеріалів відносяться: роздаткові матеріали та листівки з порадами та підказками щодо кібербезпеки; плакати на теми пов'язані з інформаційною безпекою; паперові бюлетені.

Роздаткові матеріли використовуються як додаткове джерело інформації під час навчання та при подальшій самостійній роботі. В розрізі програми підвищення обізнаності персоналу роздатковими матеріалами виступають роздрукована версія змісту та тем програми. Ці матеріали надаються кожному учаснику програми.

Плакати є вагомим засобом для підвищення поінформованості персоналу через їх постійну доступність для кожного співробітника підприємства. Плакати потрібно розташовувати в місцях великого скупчення співробітників, проходячи повз яке будуть кожний раз звертати на плакат увагу. Плакати використовуються для нагадування користувачам про важливі питання, такі як кібербезпека на підприємстві або більш конкретизовані теми, які мають попит серед співробітників. Однак, користувачі можуть проходити повз і не помічати повідомлення або втрачати чутливість до цього методу, тому потрібно час від часу змінювати місця розташування плакатів та їх теми. На малюнках зображені плакати для підтримки поінформованості персоналу. На плакаті, в якому йдеться мова про пароль (малюнок) є тільки текст, але він привертає до себе увагу контрастним дизайном та веселим змістом. Інформація краще засвоюється через смішні написи та картинки на плакатах. Теми, які підіймаються на плакатах повинні мати віддзеркалення в подальших діях співробітників. Плакат про пароль (рисунок 2.2) має на меті нагадати користувачам про важливість створення гарного пароля і , в жодному разі, не використання особистих даних. Плакат про фішінг (рисунок 2.3) підкупає свою картинкою. Він був створений, як нагадування всім співробітникам підприємства, що не треба вестися на вудочку, яку тобі закидають шахраї.

Рисунок 2.2 – Плакат «Надійний пароль»

Рисунок 2.3 – Плакат «Фішинг»

Паперові бюлетені мають той самий відгук що і електронні: багато інформації, яка надається в паперових бюлетенях може бути просто пропущена. Бюлетені потрібні лише для того сегменту співробітників підприємства, які не хочуть або не можуть сприймати туж саму інформацію через інші засоби розповсюдження інформації.

Методи онлайн доставки інформації.

Цей спосіб добре підходить для взаємодії з інформацією, коли користувачам, по різним причинам, не може бути присутнім під час проведення програми на самому підприємстві. Даний метод включає в себе: проходження програми підвищення рівня обізнаності персоналу на підприємстві на сайті програми, а також може включати і онлайн–присутність під час проведення навчання програми, яка базується на підприємстві; асинхронне навчання; використання різних блогів, відео та інших мультимедійних засобів.

Сайт програми підвищення рівня обізнаності персоналу на промисловому підприємстві був створений за допомогою системи управління контентом WordPress. За допомогою даної системи можна створювати сайти різноманітного характеру та керувати їм без знань та додаткових навичок. Вона містить велику кількість шаблонів, має зручний інтерфейс, що має велику перевагу серед інших подібних систем. Адреса сайту програми: cybsa.wordpress.com

Структура сайту – логічна побудова всіх сторінок та розділів вебресурса. Структурування сайту є дуже важливим етапом , тому що від цього залежить чи буде зручно користувачу використовувати сайт. Структура сайту програми підвищення обізнаності персоналу представлена на рисунку 2.4. Основні вимоги до структури сайту:

- наявність навігації на сторінках;
- глибина URL–адреси не повинна перевищувати чотирьох папок (тобто щоб потрапити на потрібну сторінку, потрібно зробити не більше трьох кліків з головної сторінки);

- при збільшенні або зменшенні кількості категорій і підкатегорій структура сайту повинна залишатися незмінною.

Рисунок 2.4 – Структура сайту “Cybersecurity Awareness Training”

Головна сторінка сайту програми підвищення рівня обізнаності персоналу на промисловому підприємстві складається з 6 блоків: обкладинка сайту; тем програми, які розбиті за тижнями; навчання; переваги та особливості програми; інформація про розробника сайту.

Перший блок – обкладинка (рисунок 2.5). Даний блок лише має назву програми “Cybersecurity Awareness Training” та навігацію, за якою можно одразу перейти до потрібного блоку сайту.

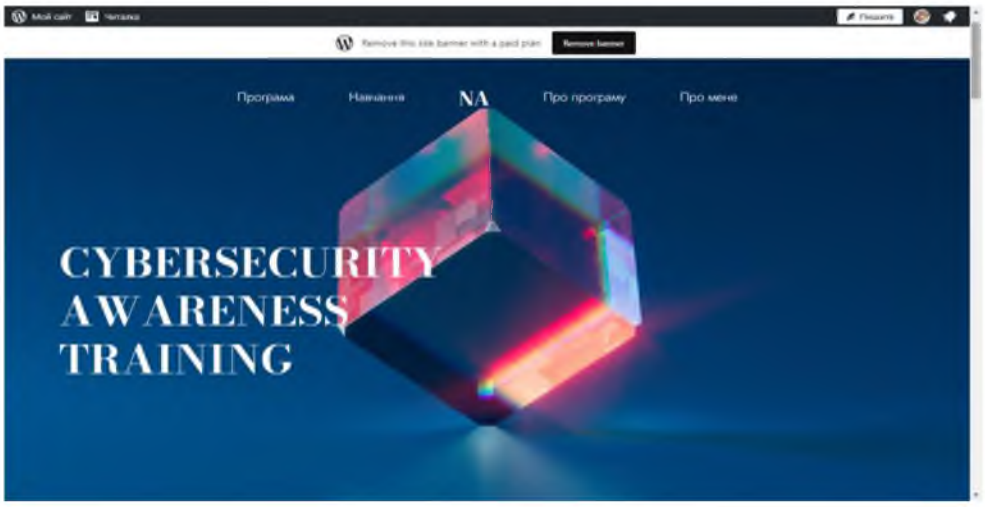

Рисунок 2.5 – Обкладинка сайту

Другий блок – програма навчання та теми, за якими буде здійснюватися навчання (рисунок 2.6). Визначення чітких термінів та потрібних співробітникам тем є одними з головних показників успішності програми підвищення обізнаності персоналу. Програма розрахована на 3 тижні та включає в себе такі теми, як ландшафт загроз, автентифікація та шкідливе ПЗ. Кожна з цих тем має свої підтеми, які має ще свої підтеми, тобто навчання враховує необхідні та критично важливі тем, в яких співробітники не мають знань, і тому має таку розгалуженість. Це робиться для того, щоб не пропустити нічого важливого.

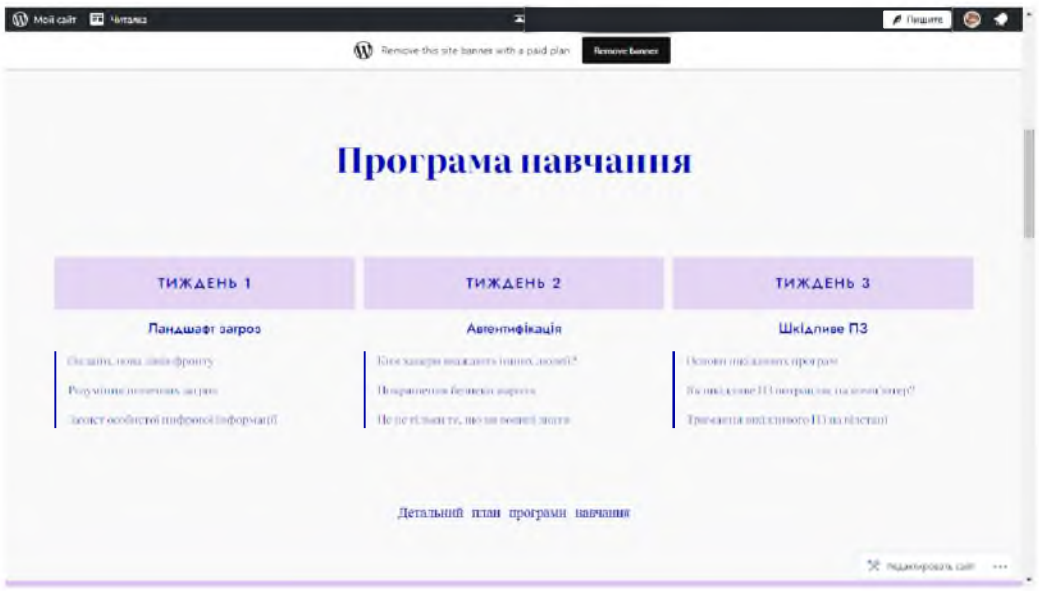

Рисунок 2.6 – Блок сайту «Програма навчання та теми програми»

Другий блок також включає посилання «Детальний план програми навчання», яке переводить на сторінку з повним описом всіх тем, за якими проводиться навчання (рисунок 2.7).

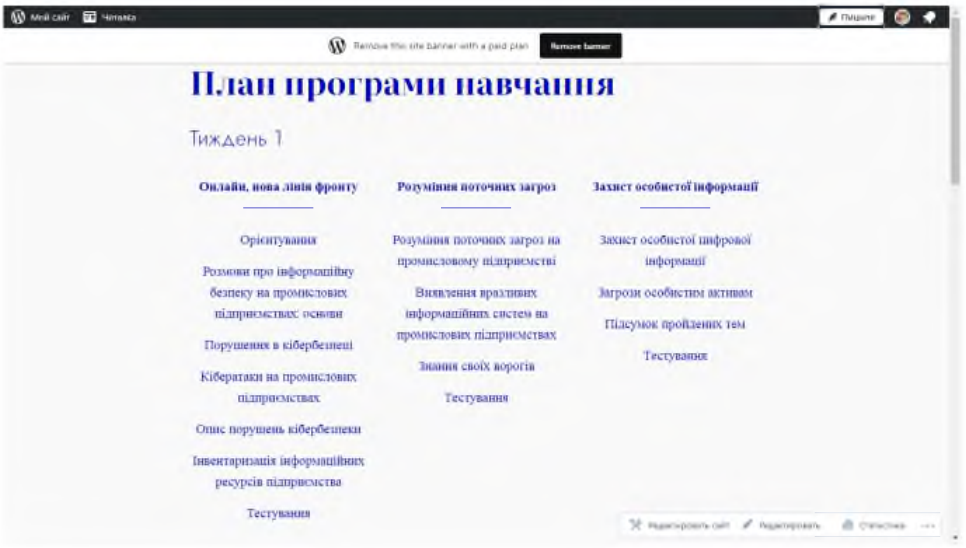

Рисунок 2.7 – Блок сайту «План програми навчання»

Третій блок – навчання (рисунок 2.8). Даний блок потрібен для проходження навчання за програмою підвищення обізнаності персоналу. Блок “Навчання” має 3 кнопки: “Підготовка”, “Тестування”, “Отримати сертифікат”, кожна з яких посилається на окрему відповідну сторінку. Цей блок є навігацією серед програми.

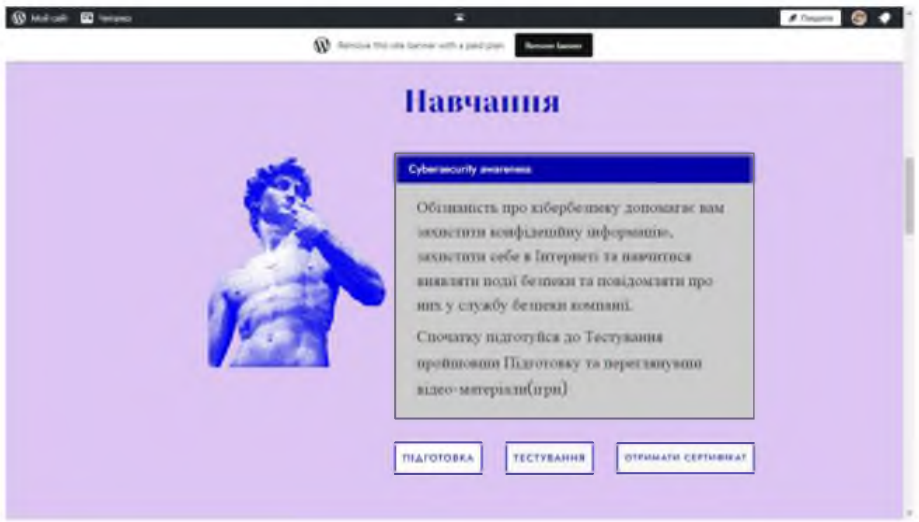

Рисунок 2.8 – Блок сайту «Навчання»

Сторінка “Підготовка” (рисунок 2.9). На даній сторінці проходить навчання за такими темами програми: Розпізнавання фішингових програм; Зменшення фізичних ризиків безпеки; Використання ресурсів компанії; Захист інформації та даних; Використання сторонніх програм або сервісів; Передача даних; Підтримання безпеки пристроїв; Конфіденційність даних; Звички безпечного спілкування; Розпізнавання загроз соціальної інженерії.

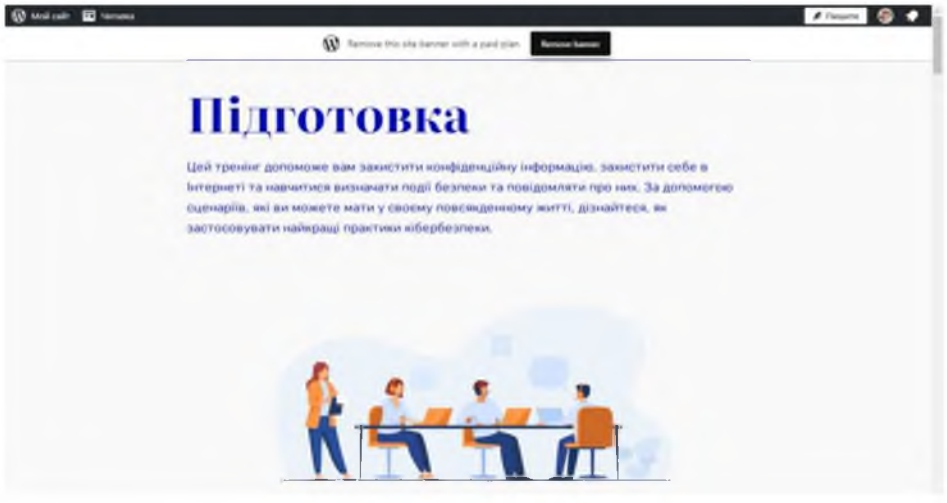

Рисунок 2.9 – Сторінка «Підготовка»

Кожна з тем знаходиться на окремій карточці та описує ситуацію відповідно темі та поради безпеки, яких слідує дотримуватись в описаній ситуації (рисунок 2.10, рисунок 2.11). Тобто вивчення програми не має на меті просто подати суху інформацію з великою кількістю даних. Навпаки, реальні ситуації краще розуміються персоналом. Так інформація краще запам'ятовується. Окрім загальної інформації до кожної теми є також додаткові матеріали – відео, статті чи ігри. Додаткова інформація [43] потрібна для більш поглибленого вивчення теми, якщо це потрібно.

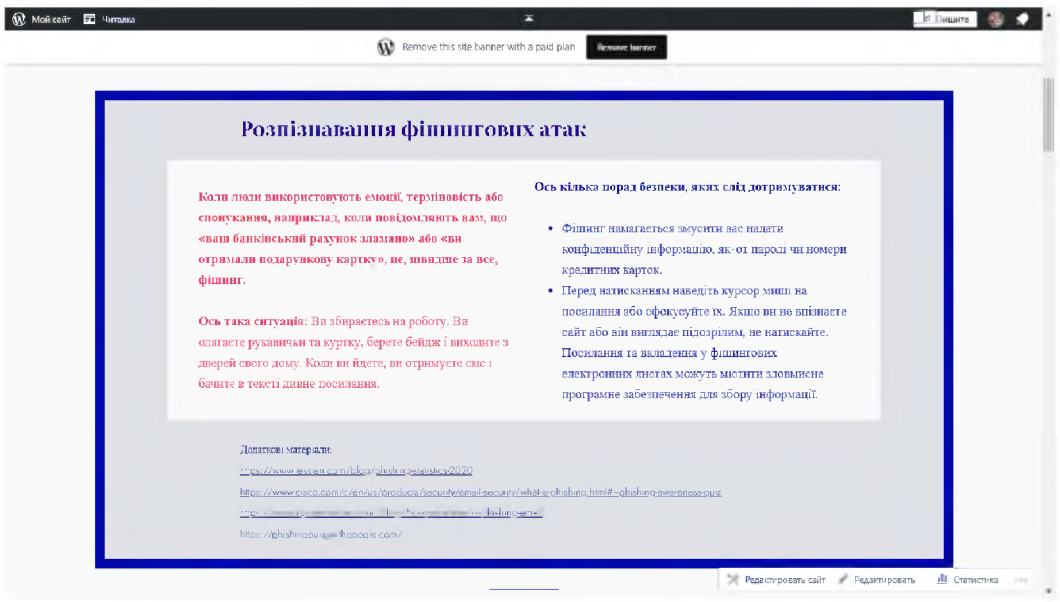

Рисунок 2.10 – Сторінка «Підготовка»

Рисунок 2.11 – Сторінка «Підготовка»

Сторінка “Тестування” (рисунок 2.12). Відповідно до назви, на даній сторінці проводиться тестування за вивченим матеріалом з сторінки “Підготовка”. Тестування відбувається за допомогою програмного забезпечення для адміністрування опитувань Google Forms. За кожну правильну відповідь

співробітник отримує 1 бал. Оцінювання необхідне для розуміння засвоєння вивченого матеріала.

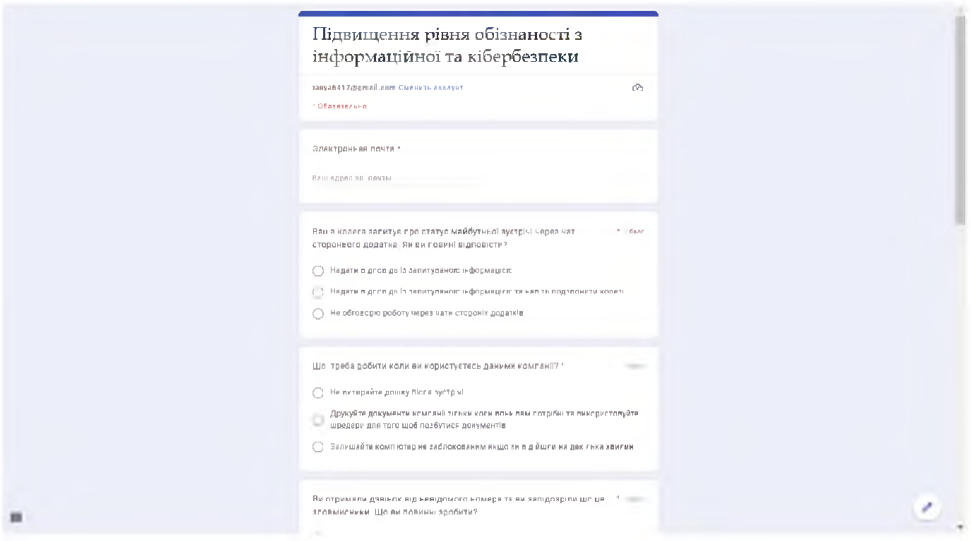

Рисунок 2.12 – Сторінка «Тестування»

Сторінка “Отримати сертифікат” (рисунок 2.13). Ця сторінка зроблена для того щоб кожний співробітник зміг отримати сертифікат про закінчення проходження програми підвищення обізнаності персоналу.

Рисунок 2.13 – Сторінка «Отримати сертифікат»

Четвертий блок – “Переваги та особливості програми” (рисунок 2.14). Головними перевагами та особливостями програми є: відповідність стандартам (кожна тема узгоджується з елементами контролю обізнаності про інформаційну безпеку таких стандартів відповідності як NIST SP 800–53r4 та ISO 27001), можливість розгортання навчання за лічені хвилини (наявність під рукою всіх необхідних матеріалів для проходження навчання онлайн), покращене зберігання вмісту (розроблена програма підходить для певних категорій віку людей і через те, краще вивчається та засвоюється) .

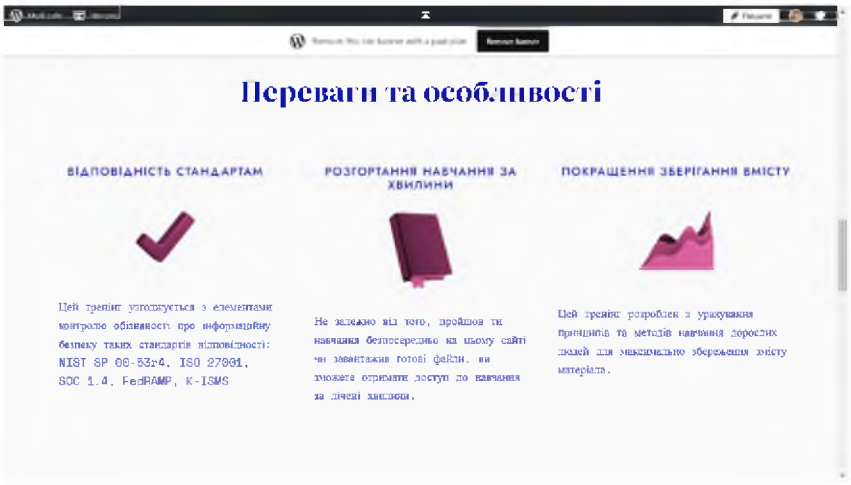

Рисунок 2.14 – Блок сайту «Переваги та особливості програми»

Шостий блок – “Про автора сайту” (рисунок 2.15). Автор та розробник сайту головна людина, яка створює сам сайт та підлаштовується під всі можливі запити програми.

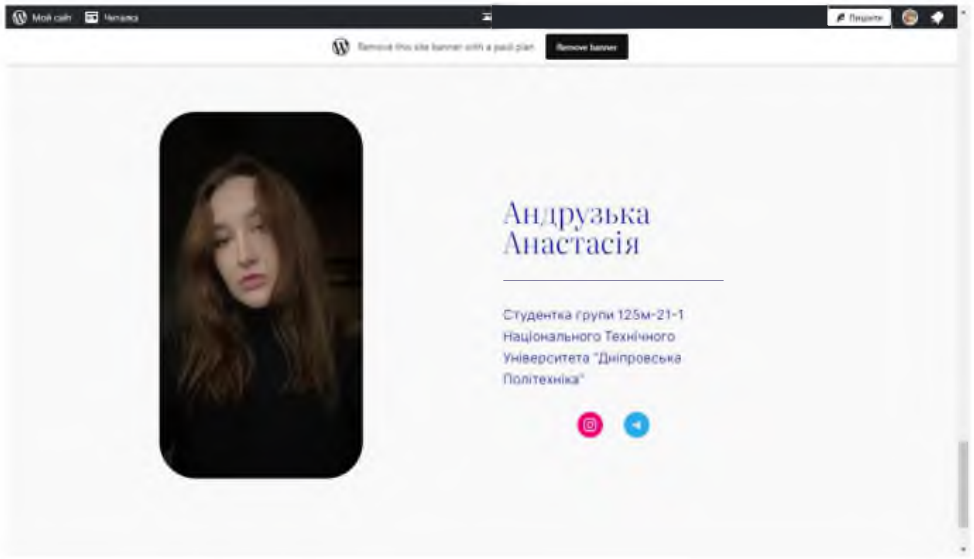

Рисунок 2.15 – Блок сайту «Про мене»

Так виглядає один з головних засобів підвищення обізнаності персоналу на промисловому підприємстві.

Засоби підтримки поінформованості персоналу включаючи додатковий перегляд використаних матеріалів, збереження, за потребою, всіх мультимедійних засобів, які використовувалися під час навчання, є головними засобами підвищення обізнаності персоналу.

Базовані на відео методи доставки інформації.

Підприємства не часто використовують доставку відео контенту як частину своєї програми інформування про кібербезпеку. Методи доставки на основі відео можна поєднати з вправами на читання та тестами, щоб надати користувачеві більш ефективний досвід. Це скоріше альтернативний метод розробки самої програми підвищення обізнаності персоналу, але після закінчення програми це краща альтернатива, а ніж просту інформування за допомогою електронної пошти чи буклетів. Для створення відео–контенту потрібно більше часу, тому що зворотній зв'язок у режимі реального часу відсутній в даному випадку, і тому потрібно чітко розуміти потреби в необхідній інформації.

Методи доставки інформації на основі моделювання.

Методи доставки на основі моделювання дуже інтерактивні. Цей тип доставки часто використовується під час тренувань з фішингу, щоб перевірити вразливість користувачів до методів фішингу, і часто супроводжується навчанням. Наприклад, створення та розсилка електронних листів повинні навчити персонал визначати, що це фішингова розсилка (рисунок 2.16), яка націлена на дані користувача чи це звичайний спам–лист, який не несе шкоди. Наприклад, отримання від відомої компанії листа про підтвердження електронної пошти – малюнок. Співробітники повинні зрозуміти – це лист, який несе в собі загрозу чи це реальний лист. Потрібно завжди звертати увагу на відправника листа та інформацію, що знаходиться в середині самого листа. Спочатку треба детально прочитати лист, перевірити пошту відправника – офіційні пошти є на будь–якому офіційному сайті, їх легко знайти. Все ж потрібно зважувати кожний клік в листах електронної пошти.

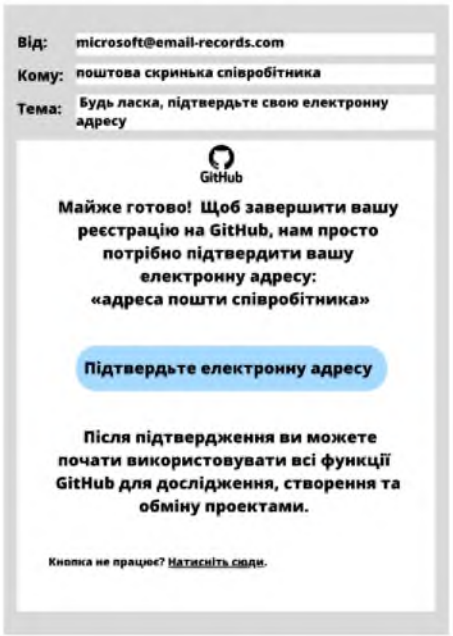

Рисунок 2.16 – Приклад фішингово листа

Розсилка електронних листів під час програми несе лише ознайомчий та дослідницький характер.

Базовані на грі методи доставки інформації.

Методи доставки інформації, які базується на іграх є інтерактивними та пропонують ефективну альтернативу більш традиційним методам доставки вмісту. Ці ігри можуть базуватися як на комп'ютері, поєднуючи комп'ютерну графіку з навчальною програмою щоб створити інтерактивне навчальне середовище.

Комп'ютерні ігри та інші інтерактивні засоби навчання є дуже популярними засобами вивчення матеріалу. Багато комп'ютерних ігор представлено на сайті центра розвитку досконалої безпеки (Security Awareness Games [44]). Це директорат агентства оборонної контррозвідки та безпеки Сполучених Штатів Америки. На цьому сайті існують наступні розділи з іграми: контррозвідка, кібербезпека, промислова безпека, ІБ, внутрішні загрози. Кожний з цих розділі має щонайменше по 2 гри в 1 розділі. Наприклад, в розділі "Кібербезпека" є гра "Інтернет завтрашнього дня" (рисунок 2.16, рисунок 2.17). Дана гра є виключно на англійській мові, але знаючи основні терміни можно з легкістю її пройти.

Рисунок 2.17 – Онлайн гра «Інтернет завтрашнього дня»

Ця гра орієнтована на тіж самі теми, що вивчаються і в програмі підвищення обізнаності персоналу(малюнок).

Рисунок 2.18 – Онлайн гра «Інтернет завтрашнього дня»

Інші розділи мають також цікаві ігри, кросворди та челленджи. Інформація для вивчення, яка подана у вигляді гри є більш зрозумілою через те, що сприймається більше як гра, а ніж як інформація, яку просто розповідають.

Всі вище перелічені методи та відповідні їм засоби підвищення обізнаності персоналу та подальшої підтримки поінформованості співробітників є основними, що використовувались під час розробки даної програми. Кожний з засобів був обран через їх адаптивність, зрозумілість та інтерактивність. Засоби підтримки поінформованості повинні підтримувати вже вивчені знання на програмі, а також нові матеріалі, які через ці засоби транслюються.

2.4 Висновки до другого розділу

В другому розділі проводилась розробка програми підвищення обізнаності персоналу з інформаційної та кібербезпеки на промисловому підприємстві.

Розробка програми починалась з аналізу існуючої політики безпеки, визначення основних ролей та обов'язків на підприємстві, визначення моделі підприємства та проведення оцінки необхідних потреб, після цього відбувалась розробка стратегії та плану програми, пошук необхідних інформаційних матеріалів для програми. Заключним етапом розробки програми було впровадження та проведення програми підвищення обізнаності персоналу, а також проведення заходів після закінчення програми.

Окрім розробки програми, проводилась розробка рекомендацій щодо організації програми підвищення обізнаності персоналу на підприємстві та розробка засобів підтримки поінформованості персоналу.

Розробка рекомендацій включала в себе написання порад, яких, за можливістю, треба дотримуватись для організування програми підвищення обізнаності персоналу.

Розробка засобів для підтримки поінформованості включала в себе створення сайту для підтримки поінформованості персоналу, розробка плакатів та інфографіки на тему кібербезпеки, а ще розробка прикладу фішингового листа для перевірки співробітників після вивчення відповідної теми в програмі. Розробка сайту підвищення рівня обізнаності персоналу в кібербезпеці є головним засобом програми підвищення обізнаності персоналу, в питаннях пов'язаних з інформаційною та кібербезпекою на підприємстві. Сайт містить всі необхідні засоби для підтримки поінформованості: навчальний матеріал, тестуанння та отримання сертифіката. Окрім засобів були також обрані найкращі методи доставки розроблених засобів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є визначення того, чи буде доцільним розробка програми підвищення обізнаності персоналу та методів і засобів підтримки поінформованості персоналу з кібербезпеки. На основі розрахованих показників можна буде визначити розмір капітальних витрат та експлуатаційних витрат, які необхідні для розробки та впровадження програми підвищення обізнаності персоналу та методів і засобів підтримки поінформованості співробітників, а також річний економічний ефект від впровадження даної програми. На основі розрахунків можна бути зробити висновок, чи є доцільним розробка та впровадження програми підвищення обізнаності персоналу.

3.1 Розрахунок капітальних витрат на придбання і налагодження системи ІБ або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення програми підвищення обізнаності персоналу

Трудомісткість створення програми підвищення обізнаності персоналу визначається тривалістю кожної робочої операції:

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{пр}} + t_{\text{д}}\text{, годин} \qquad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку програми, год;

$t_{\text{в}}$– тривалість вивчення ТЗ, літературних джерел за темою тощо, год;

$t_{\text{пр}}$– тривалість розробки програми та засобів програми, год;

$t_{\text{д}}$– тривалість документування та оформлення результатів, год.

$$t = 25 \text{ год} + 70 \text{ год} + 150 \text{ год} + 150 \text{ год} = 395 \text{ год}$$

Витрати на розробку програми підвищення обізнаності персоналу на промисловому підприємстві $К_{пр}$ складаються з витрат на заробітну плату спеціаліста з ІБ (розробника програми) $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки програми підвищення обізнаності персоналу на підприємстві $З_{мч}$ за формулою 3.2:

$$К_{пр} = З_{зп} + З_{мч}, \text{грн} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

$$З_{зп} = t * З_{іб}, \text{грн} \quad (3.3)$$

де t – загальна тривалість розробки програми підвищення обізнаності персоналу на промисловому підприємстві, год;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з ІБ з нарахуваннями, грн/год.

$$З_{зп} = 395 * 208 = 82\,160 \text{ грн}$$

Вартість машинного часу для розробки програми підвищення обізнаності персоналу на ПК визначається за формулою 3.4:

$$З_{мч} = t_{пр} * С_{мч} + t_{д}, \text{грн} \quad (3.4)$$

де $t_{пр}$– трудомісткість розробки програми та засобів програми підвищення обізнаності персоналу на ПК , год;

$t_д$ – тривалість документування та оформлення результатів, год;

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P * t_{нал} * С_е + \left(Ф_{зал} * \frac{H_а}{F_р}\right) + \left(К_{лпз} * \frac{H_{апз}}{F_р}\right), \text{грн} \quad (3.5)$$

де P – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість задіяних робочих станцій при розробці програми, год;

$С_е$ – тариф на електричну енергію, грн/кВт*год;

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

$H_а$ – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне ПЗ, частки одиниці;

$К_{лпз}$ – вартість ліцензійного ПЗ, грн;

$F_р$ – річний фонд робочого часу (за 40–годинного робочого тижня $F_р$=1920).

На промислових підприємствах середня потужність дорівнює P = 0,4, а тариф на електричну енергію становить 1,44 грн/кВт*год, отже:

$$С_{мч} = 0{,}4 * 1 * 1{,}44 + \left(12500 * \frac{0{,}5}{1920}\right) + \left(3860 * \frac{0{,}4}{1920}\right) = 4{,}91 \text{ грн}$$

$$З_{мч} = t_{пр} * С_{мч} + t_д = 150 * 4{,}91 + 150 = 886{,}5 \text{ грн}$$

$$К_{пр} = З_{зп} + З_{мч} = 82\,160 + 886{,}5 = 85\,046{,}5 \text{ грн}$$

Капітальні (фіксовані) витрати на розробку та впровадження програми підвищення обізнаності складають:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{дм} + К_{навч} + К_н \quad (3.6)$$

де $К_{пр}$ – вартість розробки програми підвищення рівня обізнаності та залучення для цього зовнішніх консультантів, тис.грн. Сторонні організації не наймалися, тому даний коефіцієнт не враховується при розрахунках;

$К_{зпз}$ – вартість закупівель ліцензійного основного та додаткового ПЗ, складає 2000 грн (програма WordPress);

$К_{рп}$ – вартість розробки програми підвищення обізнаності складає 28 500 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення, грн. Для даної програми покупка апаратного забезпечення не потрібна;

$К_{дм}$ – вартість допоміжних матеріалів: 10 плакатів (150 грн/шт);

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн. Дані витрати не враховуються під час розрахунку формули, тому що фахівці не проходили платного навчання.

$К_{н}$ – витрати на встановлення обладнання та налагодження системи ІБ, грн. Даних витрат не було, оскільки програма націлена на підвищення рівня знань у працівників підприємства.

$$К = 85\,046,5 + 2\,000 + 28\,500 + 1\,500 = 117\,046,5 \text{ грн}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання і обслуговування програми підвищення обізнаності персоналу

Річні поточні (експлуатаційні) витрати на функціонування програми підвищення обізнаності складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн} \qquad (3.7)$$

де $С_{в}$ – вартість відновлення й модернізації системи;

$С_{к}$ – витрати на курування програмою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів.

Витрати на керування програмою підвищення обізнаності персоналу складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_{єв} + С_{тос}, \text{ грн} \quad (3.8)$$

Річний фонд амортизаційних відрахувань ($С_а$) :

$$С_а = \frac{15*23\,700}{5} + \frac{50\,000}{10} = 76\,100 \text{ грн}$$

Річний фонд заробітної плати персоналу, що обслуговує програму ($С_з$) складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн} \quad (3.9)$$

Основна заробітна плата спеціаліста з інформаційної безпеки на місяць – 20 000 грн, додаткова заробітна плата – 8% від основної зарплати:

$$С_з = 20\,000 * 12 + 20\,000 * 12 * 0{,}08 = 259\,200 \text{ грн}$$

Ставка ЄСВ для всіх категорій платників складає 22%:

$$С_{єв} = 259\,200 * 0{,}22 = 57\,024 \text{ грн}$$

Вартість електроенергії, що споживається ноутбуками протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = P * F_p * Ц_е, \text{ грн} \quad (3.10)$$

де Р – встановлена потужність ПК, кВт;

$Ц_е$ – тариф на електричну енергію, грн/кВт*год .

F – річний фонд робочого часу.

$$С_{ел} = 1 * 1920 * 2{,}14 = 4\ 108{,}8 \text{ грн}$$

Витрати на технічне й організаційне адміністрування програми визначаються в відсотках від капітальних витрат – 2% ($С_{тос}$ = 117 046,5 * 0,02 = 2 340,9 грн).

Витрати на керування програмою підвищення обізнаності персоналу ($С_к$) дорівнюють:

$$С_к = 32800 + 76100 + 259200 + 57024 + 4108{,}8 + 2340{,}9 = 431\ 473{,}7 \text{ грн}$$

Таким чином, річні поточні витрати складають:

$$С = 25\ 000 + 431\ 573{,}7 = 456\ 573{,}7 \text{ грн}$$

3.3 Визначення річного економічного ефекту від впровадження програми підвищення обізнаності персоналу

Загальний ефект від провадження програми ІБ визначається з урахуванням ризиків порушення ІБ підприємства і становить:

$$E = B * R - C \qquad (3.11)$$

,

де В – загальний збиток від атак на мережу підприємства, грн;

R – очікувана ймовірність атаки на мережу підприємства, частки одиниці;

С – щорічні витрати на оновлення програми підвищення обізнаності персоналу, грн.

Загальний збиток від атаки на мережу підприємства складає:

$$В = \sum_i \sum_n U, \text{ грн} \quad (3.12)$$

де I – число атакованих мереж підприємства;

N – середнє число атак на рік;

U – упущена вигода від простою атакованої мережі підприємства.

Упущена вигода від простою атакованою мережі підприємства становить:

$$U = П_п + П_в + V \quad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованої мережі підприємства, грн;

$П_в$ – вартість відновлення працездатності мережі підприємства;

V – втрати від зниження обсягу продажів за час простою атакованої мережі підприємства, грн.

Втрати від зниження продуктивності співробітників атакованої мережі підприємства являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} * t_п \quad (3.14)$$

де F – місячний фонд робочого місяця (при 40–а годинному робочому тижні становить 176 ч);

$З_с$ – заробітна плата співробітників атакованої мережі на підприємства, грн на місяць;

$t_{\text{п}}$ – час простою мережі підприємства внаслідок атаки, год.

Витрати на відновлення працездатності мережі підприємства включають:

$$\text{П}_{\text{в}} = \text{П}_{\text{ви}} + \text{П}_{\text{пв}} + \text{П}_{\text{зч}} \quad (3.15)$$

де $\text{П}_{\text{ви}}$ – витрати на повторне уведення інформації, грн;

$\text{П}_{\text{пв}}$ – витрати на відновлення мережі підприємства, грн;

$\text{П}_{\text{зч}}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації розраховуються:

$$\text{П}_{\text{ви}} = \frac{\sum \text{З}_{\text{с}}}{F} * t_{\text{ви}} \quad (3.16)$$

де $t_{\text{ви}}$ – час повторного введення загубленої інформації співробітниками атакованої мережі підприємства, год.

Витрати на відновлення мережі підприємства визначаються:

$$\text{П}_{\text{пв}} = \frac{\sum \text{З}_{\text{о}}}{F} * t_{\text{в}} \quad (3.17)$$

де $t_{\text{в}}$ – час відновлення після атаки персоналом, що обслуговує мережу підприємства, год;

$\text{З}_{\text{о}}$ – заробітна плата обслуговуючого персоналу, грн на місяць.

Втрати від зниження очікуваного обсягу продажів за час простою атакованої мережі підприємства визначаються:

$$V = \frac{O}{F_{\text{Г}}} * (t_{\text{в}} + t_{\text{п}} + t_{\text{ви}}) \quad (3.18)$$

де О – обсяг продажів атакованої мережі підприємства, грн у рік;

Fг – річний фонд часу роботи підприємства становить 2080 ч.

Визначення річного економічного ефекту:

$$V = \frac{8\,504\,700}{2080} * (7 + 2 + 4) = 53\,154 \text{ грн}$$

$$П_{пв} = \frac{327\,200}{176} * 7 = 13\,013{,}6 \text{ грн}$$

$$П_{ви} = \frac{220\,500}{176} * 4 = 5\,011{,}3 \text{ грн}$$

$$П_{в} = 13\,013{,}6 + 5\,011{,}3 = 18\,024{,}9 \text{ грн}$$

$$П_{п} = \frac{220\,500}{176} * 2 = 2\,505{,}6 \text{ грн}$$

$$U = 18\,024{,}9 + 2\,505{,}6 + 53\,154 = 73\,684{,}5 \text{ грн}$$

$$В = \sum_{2}\sum_{14} 73\,684{,}5 = 2 * 14 * 73\,684{,}5 = 2\,063\,166 \text{ грн}$$

$$E = 2\,063\,166 * 0{,}35 - 456\,573{,}7 = 265\,534{,}4 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованого в кваліфікаційній роботі проєктного рішення

Оцінка економічної ефективності програми підвищення рівня обізнаності, здійснюється на основі визначення та аналізу наступний показників:

1. Сукупна вартість володіння (ТСО);
2. Коефіцієнт повернення інвестицій (ROSI);

3. Термін окупності капітальних інвестицій T_o.

Коефіцієнт повернення інвестицій (ROSI) показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження програми підвищення обізнаності персоналу.

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \quad (3.19)$$

де Е – загальний ефект від впровадження програми підвищення обізнаності персоналу, грн;

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

$$ROSI = \frac{E}{K} = \frac{265\,534{,}4}{117\,046{,}5} = 2{,}3$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження програми підвищення обізнаності персоналу:

$$T_o = \frac{K}{E} = \frac{1}{ROSI}, \text{ років} \quad (3.20)$$

$$T_o = \frac{K}{E} = \frac{117\,046{,}5}{265\,534{,}4} = 0{,}4 \text{ рока (5 місяців)}$$

3.5 Висновки про економічну доцільність проєктного рішення

В результаті розрахованих витрат на розробку та впровадження програми обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою на промисловому підприємстві було доведено економічну доцільність розробки програми, методів та засобів підвищення обізнаності персоналу з кібербезпеки на промисловому підприємстві. Такі висновки зроблені, виходячи з коефіцієнту

повернення інвестицій ROSI, який складає 1,4 та означає, що на 1 грн. капітальних витрат приходиться 2,3 грн. економічного ефекту. Період окупності при цьому складе 5 місяців. Капітальні витрати складають 117 046,5 грн, а експлуатаційні – 456 573,7 грн.

ВИСНОВКИ

У кваліфікаційній роботі розроблялись програма підвищення обізнаності персоналу з інформаційної та кібербезпеки на промисловому підприємстві, а також методи та засоби підтримки поінформованості співробітників промислового підприємства. Перед розробкою програми проводився аналіз існуючих внутрішніх та зовнішніх антропогенних загроз кібербезпеці на промисловому підприємстві, а також аналіз методів та засобів підвищення обізнаності персоналу на підприємстві.

В другому розділі проводилась розробка програми підвищення обізнаності персоналу з інформаційної та кібербезпеці на промислову підприємстві. Програма підвищення обізнаності ґрунтується на проаналізованих внутрішніх та зовнішніх антропогенних загрозах, які становлять або можуть в майбутньому становить загрозу інформаційній безпеці підприємства. Аналіз методів та засобів підвищення обізнаності персоналу був взятий за основу для розробки методів і засобів підвищення обізнаності співробітників на підприємстві. Були обрані найкращі методи доставки інформації та створені відповідні методам засоби, які найкраще підходять для співробітників промислового підприємства. Під час розробки методів та засобів головну увагу приділялось саме подачі інформації – основними характеристиками для інформації були її доступність та зрозумілість.

В економічному розділі були проведені розрахунки та проаналізовані економічна ефективність програми, яка розроблена для підвищення обізнаності персоналу з інформаційної та кібербезпеки на промисловому підприємстві. Отримані розрахунки свідчать про те, що розробка програми є доцільною.

ПЕРЕЛІК ПОСИЛАНЬ

1. Коваленко Ю. О. Забезпечення ІБ на підприємстві [Електронний ресурс] / Ю. О. Коваленко – Режим доступу до ресурсу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/24811/st_51_18.pdf?sequence=1.

2. Про національну безпеку України: Закон України від 19 червня 2018 року № 2469–VIII // Відомості Верховної Ради України. – 2018. – № 31. – Ст. 241

3. Про Стратегію національної безпеки України: Указ Президента України від 12 лютого 2007 року № 105/200 // Офіційний вісник України. – 2007. – № 11. – Ст. 389.

4. Найбільші виклики кібербезпеці у 2022 році [Електронний ресурс] – Режим доступу до ресурсу: https://www.checkpoint.com/cyber–hub/cyber–security/what–is–cybersecurity/biggest–cybersecurity–challenges–in–2022/.

5. Чому люди є головними воротами для кіберкомпромісу? [Електронний ресурс] – Режим доступу до ресурсу: 5. https://www.securityinfowatch.com/cybersecurity/article/21281583/why–humans–are–the–top–gateway–to–cyber–compromise.

6. Сутність промислового підприємства [Електронний ресурс] – Режим доступу до ресурсу: https://www.academia.edu/62772779/The_nature_of_the_industrial_enterprise.

7. Повний звіт IBM Security X–Force Threat Intelligence Index 2022 [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.ibm.com/downloads/cas/ADLMYLAZ.

8. Людський фактор у кібербезпеці: ризики та вплив [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: http://www.securityscience.edu.rs/index.php/journal–security–science/article/view/54/34.

9. Аналіз сучасного стану загроз інформаційній безпеці підприємств [Електронний ресурс] – Режим доступу до ресурсу:

https://cyberleninka.ru/article/n/analiz–sovremennogo–sostoyaniya–ugroz–informatsionnoy–bezopasnosti–predpriyatiy/viewer.

10. Конфіденційність, цілісність і доступність – тріада КЦД [Електронний ресурс] – Режим доступу до ресурсу: https://www.certmike.com/confidentiality–integrity–and–availability–the–cia–triad/.

11. Тристоронній підхід до кібербезпеки: захист даних та інформації [Електронний ресурс] – Режим доступу до ресурсу: https://www.dnv.com/article/the–three–pillar–approach–to–cyber–security–data–and–information–protection–165683.

12. Балановська А. В. Джерела виникнення та наслідки реалізації загроз інформаційній безпеці промислових підприємств / А. В. Балановська. – 2015. – №3.

13. Що таке внутрішні загрози в кібербезпеці? [Електронний ресурс] – Режим доступу до ресурсу: https://www.aspirets.com/blog/what–are–internal–threats–cyber–security/.

14. Як виникають внутрішні загрози [Електронний ресурс] – Режим доступу до ресурсу: https://www.knowitallninja.com/lessons/how–internal–threats–occur/.

15. Чи є у вашій стратегії безпеки саботаж персоналу та крадіжки? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.barrybros.com/2020/02/do–staff–sabotage–and–employee–theft–feature–in–your–security–strategy/.

16. Несанкціонований доступ: що це таке та як цьому запобігти [Електронний ресурс] – Режим доступу до ресурсу: https://www.mitrefinch.co.uk/blog/workforce–management/how–to–prevent–unauthorised–access–to–your–building/#:~:text=Unauthorised%20access%20refers%20to%20an,keys%2C%20security%20passes%2C%20or%20fobs.

17. 10 поширених причин втрати даних [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://consoltech.com/blog/10–common–causes–of–data–loss/.

18. Що таке внутрішня загроза? [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application–security/insider–threats/.

19. Як виникають зовнішні загрози [Електронний ресурс] – Режим доступу до ресурсу: https://www.knowitallninja.com/lessons/how–external–threats–occur/.

20. Зовнішні та внутрішні ризики кібербезпеки: знайте різницю [Електронний ресурс] – Режим доступу до ресурсу: https://ermprotect.com/blog/external–vs–internal–cybersecurity–risks–know–difference/.

21. Що таке зловмисне програмне забезпечення та як захиститися від атак зловмисного програмного забезпечення [Електронний ресурс] – Режим доступу до ресурсу: https://www.paloaltonetworks.com/cyberpedia/what–is–malware.

22. Що таке хакерство? Як це працює? [Електронний ресурс] – Режим доступу до ресурсу: https://www.echosec.net/blog/what–is–hacking–how–does–it–work.

23. Соціальна інженерія [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application–security/social–engineering–attack.

24. 9 прикладів атак соціальної інженерії [Електронний ресурс] – Режим доступу до ресурсу: https://terranovasecurity.com/examples–of–social–engineering–attacks/.

25. Б. Хан, К. С. Алгатбар, С. І. Набі та М. К. Хан, «Ефективність методів усвідомлення ІБ на основі психологічних теорій», в Африканському журналі управління бізнесом, 2011 р., том. 5, № 26, стор. 10862–10868

26. А. Башорун, А. Ворвуі та Д. Паркер, «Інформаційна безпека: щоб визначити рівень її обізнаності в організації», у 2013 р. 7–а Міжнародна конференція із застосування інформаційно–комунікаційних технологій, 2013 р., стор. 1–5.

27. Поінформованість про інформаційну безпеку: огляд методів, проблем і рішень [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/331843030_Information_Security_Awareness_A_Review_of_Methods_Challenges_and_Solutions.

28. Шоуверман С. Cyberheist / Стью Шоуверман., 2016. – 240 с. – (KnowBe4).

29. M. Siponen, M. Adam Mahmood та S. Pahnila, «Дотримання співробітниками політики ІБ: дослідницьке польове дослідження», Inf. кер., вип. 51, вип. 2, стор. 217–224, 2014.

30. Е. Шериф, С. Фернелл і Н. Кларк, «Обізнаність, поведінка та культура: азбука розвитку відповідності вимогам безпеки», 2015 10th Int. конф. Інтернет–технологія. Secur. пер. ICITST 2015, стор. 90–94, 2016 рік.

31. С. Бауер, Е. Бернройдер і К. Чудзіковскі, «Програми підвищення ІБ кінцевих користувачів для покращення ІБ в банківських організаціях: попередні результати дослідницького дослідження», Proc. Восьма робота перед ICIS. Інф. Secur. 2013. – С. 1–16.

32. HM Government, “Технічний звіт” 2015.

33. G. Information and S. Survey, «Боротьба за усунення розриву», 2012.

34. П. Боуен, Дж. Хеш і М. Вілсон, «Спеціальна публікація NIST 800–100 – Довідник з ІБ: Керівництво для менеджерів», 2006 р.

35. С. Фернелл і К.–Л. Томсон, «Від культури до непокори: Визнання різного сприйняття ІТ–безпеки користувачами», Comput. Fraud Secur., том. 2009, № 2, стор. 5–10, лютий 2009.

36. К. Дж. Кнапп, Р. Франклін Морріс, Т. Е. Маршалл і Т. А. Берд, «Політика ІБ: модель процесу на організаційному рівні», в «Комп'ютери та безпека», 2009, том. 28, вип. 7, стор. 493–508.

37. Уека А. Створення програми підвищення обізнаності про кібербезпеку / А. Уека, Б. Менлі, Л. Роджерс. – 2020.

38. NIST SP 800–50r1 [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800–50/final.

39. Політика ІБ [Електронний ресурс] – Режим доступу до ресурсу: https://idev–hub.com/uk/politika–informacijnoi–bezpeki/.

40. 5 кроків до створення ефективних програм навчання [Електронний ресурс] – Режим доступу до ресурсу: https://explorance.com/blog/5–steps–to–creating–effective–training–programs/.

41. 12 елементів політики ІБ Що таке політика ІБ? [Електронний ресурс] – Режим доступу до ресурсу: https://www.exabeam.com/explainers/information–security/the–12–elements–of–an–information–security–policy.

42. Шість настільних вправ, які допоможуть підготувати вашу команду з кібербезпеки [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisecurity.org/insights/white–papers/six–tabletop–exercises–prepare–cybersecurity–team.

43. Викладання кібербезпеки в середній школі. // Робочий пакет 3: Вплив на громаду та сталість / , 2020. – С. 19–60.

44. Гра: Інтернет завтрашнього дня [Електронний ресурс] – Режим доступу до ресурсу: https://securityawareness.usalearning.gov/cdse/multimedia/games/TomorrowsInternet/story.html.

45. Кваліфікаційна робота магістра. Методичні рекомендації до виконання для студентів спеціальності 125 «Кібербезпека» (освітньо–професійна програма «Кібербезпека») / Упоряд.: О.Ю.Гусєв, В.І.Корнієнко,

В.І.Магро, Д.С. Тимофєєв; М–во освіти і науки України, Нац. техн. ун–т «Дніпровська політехніка». – Д.: НТУ «ДП», 2022. – 34 с.

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

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	31	
6	А4	Спеціальна частина	39	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік матеріалів на оптичному носії

- Андрузька А.М._125м–21–1.docx
- Андрузька А.М._125м–21–1.pdf
- Андрузька А.М._125м–21–1.pdf.p7s
- Андрузька А.М._125м–21–1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 94 б. (« відмінно »).

Керівник розділу _____ доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студентки групи 125м-21-1
Андрузької Анастасія Максимівни
на тему: «Методи та засоби підвищення обізнаності персоналу з кібербезпеки на промисловому підприємстві»

Пояснювальна записка ст. Андрузької Анастасії Максимівни складається зі вступу, трьох розділів і висновків, викладених на 102 сторінках. Кваліфікаційна робота присвячена актуальній темі забезпечення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах промислового підприємства за рахунок підвищення рівня обізнаності персоналу за допомогою різних методів та засобів.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення мети у кваліфікаційній роботі вирішуються наступні задачі: аналіз антропогенних загроз промисловим підприємствам; аналіз методів та засобів підвищення обізнаності персоналу; розробка методів та засобів підтримки поінформованості персоналу.

Практичне значення роботи полягає у визначені основних антропогенних загроз з кібербезпеки на промисловому підприємстві та розробці програми та методів і засобів підтримки поінформованості персоналу з інформаційної та кібербезпеки.

Кваліфікаційна робота виконана відповідно до вимог і може бути допущена до захисту, оцінка – 95 (відмінно). Андрузька А.М. заслуговує присвоєння звання магістра з кібербезпеки за спеціальністю 125 Кібербезпека, освітня програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Керівник кваліфікаційної роботи

Керівник спец. розділу