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

студента *Левітан Ольги Сергіївни*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка програми підвищення обізнаності персоналу в процесі впровадження системи управління інформаційною безпекою*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.ф-м.н, проф. Гусєв О.Ю.	90	відмінно	
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.	90	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	95	відмінно	

Рецензент				

Нормоконтролер	ст. викл Мєшков В.І.	90	відмінно	

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Левітан Ользі Сергіївні* **академічної групи** *125м-22-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка програми підвищення обізнаності персоналу в процесі впровадження системи управління інформаційною безпекою*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз джерел загроз інформаційної та кібербезпеки на підприємстві, а також методів та засобів підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою	05.11.2023
Розділ 2	Попередня підготовка та затвердження рішення про створення СУІБ та розробка програми підвищення обізнаності персоналу	20.11.2023
Розділ 3	Визначення економічної доцільності та ефекту від провадження програми підвищення обізнаності персоналу	01.12.2023

Завдання видано _____ Олександр ГУСЄВ
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 01.09.2023

Дата подання до екзаменаційної комісії: 06.12.2023

Прийнято до виконання _____ Ольга ЛЕВІТАН
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 7 рис., 6 табл., 5 додатків, 13 джерел.

Об’єкт розробки: система управління інформаційною безпекою.

Предмет розробки: програма підвищення обізнаності персоналу.

Мета кваліфікаційної роботи: мінімізація інформаційних ризиків, пов’язаних з персоналом.

У першому розділі було проведено аналіз загроз, як окремому користувачу, так і на інформаційно-телекомунікаційній системі в цілому. Також проведено дослідження різних видів зовнішніх і внутрішніх загроз, які можуть виникнути в результаті дій людини і спричинити шкоду діяльності підприємства. Далі детально розглянуто методи та засоби підвищення рівня обізнаності персоналу на підприємстві, з урахуванням ефективності кожного з них.

У другому розділі було розглянуто загальні відомості про типове підприємство. Також була проведена попередня підготовка та було затверджено рішення про створення СУІБ. Далі були розглянуті необхідні складові документаційного забезпечення СУІБ. Також було розроблено програму підвищення обізнаності персоналу.

В економічній частині здійснені розрахунки капітальних витрат на придбання програми підвищення обізнаності персоналу. Також було проведено розрахунок річних експлуатаційних витрат на утримання і обслуговування програми підвищення обізнаності персоналу. Далі було проведено визначення річного економічного ефекту від провадження програми підвищення обізнаності персоналу. Також було проведено визначення та аналіз показників економічної ефективності.

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПРОГРАМА ПІДВИЩЕННЯ ОБІЗНАНОСТІ ПЕРСОНАЛУ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІНО-ТЕЛЕКОМУНІКАЦІЙНЕ ПІДПРИЄМСТВО.

ABSTRACT

Explanatory note: 81 p., 7 pictures, 6 tables, 5 applications, 13 sources.

Object of development: information security management system.

Subject of development: staff awareness program.

The purpose of the qualification work: minimization of information risks related to personnel.

In the first section, an analysis of threats was carried out, both to an individual user and to the information and telecommunication system as a whole. Research was also conducted on various types of external and internal threats that may arise as a result of human actions and cause damage to the company's activities. Next, the methods and means of raising the level of awareness of personnel at the enterprise are considered in detail, taking into account the effectiveness of each of them.

In the second section, general information about a typical enterprise was considered. Preliminary preparation was also carried out and the decision to create an ISMS was approved. Next, the necessary components of ISMS documentation support were considered. A staff awareness program was also developed.

In the economic part, the calculations of capital costs for the purchase of a program for raising staff awareness have been made. The calculation of the annual operating costs for maintenance and service of the staff awareness program was also carried out. Next, the annual economic effect of the implementation of the staff awareness program was determined. Determination and analysis of economic efficiency indicators were also carried out.

INFORMATION SECURITY POLICY, INFORMATION SECURITY MANAGEMENT SYSTEM, PERSONNEL AWARENESS PROGRAM, INFORMATION SECURITY, INFORMATION AND TELECOMMUNICATION ENTERPRISE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ- інформаційна безпека;

ІТ – інформаційні технології;

ПЗ – програмне забезпечення;

СДН – система дистанційного навчання;

СУІБ- система управління інформаційною безпекою;

GPS - Global Positioning System (Система глобального позиціювання);

IoT - Internet of Things (Інтернет речей);

NIST - National Institute of Standards and Technology (Національний інститут стандартів та технологій).

ЗМІСТ

ВСТУП

Об’єкт розробки: система управління інформаційною безпекою.

Предмет розробки: програма підвищення обізнаності персоналу.

Мета кваліфікаційної роботи: мінімізація інформаційних ризиків, пов’язаних з персоналом.

Існування кіберзлочинності становить досить серйозну проблему в умовах глобального процвітання інноваційно-технологічних ресурсів. Це впливає абсолютно на всіх, як на окремих фізичних та юридичних осіб, так і на об’єкти критичної інфраструктури й державні органи. Окрім, відповідної прямої шкоди, кіберзлочинність є величезною перешкодою для цифрової довіри, значною мірою підриваючи переваги кіберпростору.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних атак та їх негативні наслідки. Так, кількість кримінальних правопорушень у сфері інформаційних технологій постійно зростає. Зокрема, з огляду статистичних даних Генеральної прокуратури України випливає, що станом на 31 грудня 2022 року обліковано у звітному періоді 3 415 кримінальних правопорушень у сфері інформаційних технологій, що на 105 кримінальних правопорушень більше порівняно з 2021 роком та на 917 – більше порівняно з 2020 роком. Це свідчить в цілому про суттєве зростання, а саме – на 3,1% порівняно з 2021 роком та – на 26,8% порівняно з 2020 роком, кількості зареєстрованих кримінальних правопорушень.

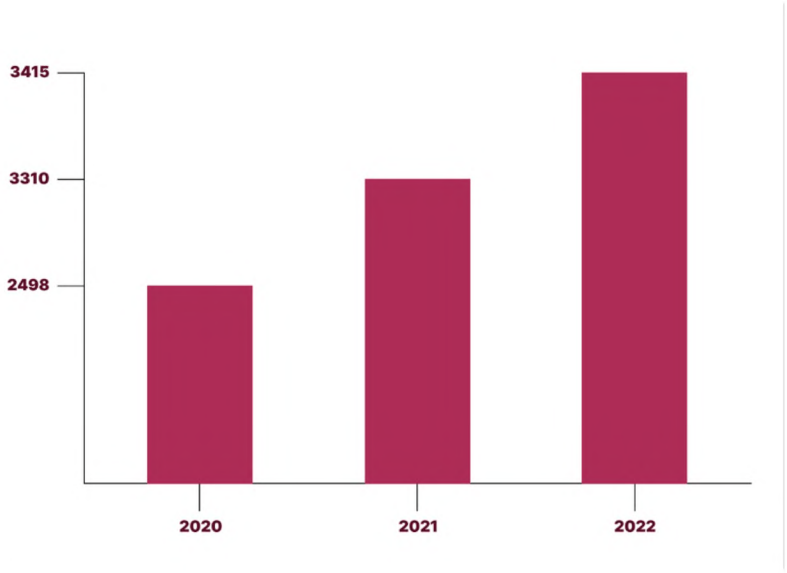


Рисунок 1 – Статистичні дані Генеральної прокуратури України.

Варто зазначити, що поширенню кіберзлочинності сприяють такі чинники: гіперпопит на різні види інформаційних послуг у розвинутих країнах світу; процеси глобалізації світової економіки; розвиток сучасних інформаційних технологій, особливо інтернет-ресурсів, що забезпечують майже неконтрольований процес формування спокус.

Враховуючи вищезазначене, питання боротьби з кіберзлочинністю є особливо актуальним, оскільки необхідно вживати відповідних заходів щодо зменшення проявів кібератак у мережі Інтернет. [1]

Раптовий перехід на відділений режим роботи спочатку через пандемію, потім через війну – найкращий момент для кіберзлочинців через велике зростання можливості зламу систем.

Люди є найвразливішою ланкою в системі кіберзахисту. Реалізація загрози відбувається миттєво: працівник недбало відкриває електронний лист, і вся ваша компанія зупиняється, що має тяжкі наслідки: зашифровані IT-системи, вимоги викупу, маніпуляції з даними та переривання процесів. За словами експертів з CISCO, успішність кібератак залежить на 91% саме від людських помилок (відкривання небезпечних посилань, успішний фішинг, завантаження шкідливих файлів, тощо) та лише на 9% від технічних проблем (слабка захищеність систем, відсутність спеціального програмного

забезпечення, тощо). Тому, в першу чергу важливо забезпечити захист кожного працівника вашої компанії, аби весь бізнес був у безпеці. Водночас, персональний захист — це не лише про встановлення антивірусу на робочий ноутбук, це ще і про обізнаність працівників. Обов'язкові тренінги та навчання необхідні для розуміння співробітників важливості своїх обов'язків щодо захисту IT, організаційних політик та те, як правильно їх використовувати та захистити довірені їм IT-ресурси.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз джерел загроз інформаційної та кібербезпеки на підприємстві

Питання інформаційної та кібербезпеки стали надзвичайно важливими для інформаційно-телекомунікаційних підприємств в сучасних умовах постійно зростаючих загроз та атак. Інформаційна безпека охоплює заходи для захисту конфіденційності, цілісності та доступності даних, тоді як кібербезпека спеціалізується на захисті систем та мереж від кіберзагроз.

Давайте розглянемо, чому ці аспекти є настільки важливими для інформаційно-телекомунікаційних підприємств.

Захист конфіденційної інформації є вагомим аспектом для інформаційно-телекомунікаційних підприємств, які зберігають значні обсяги конфіденційних даних, таких як особиста інформація клієнтів, фінансові дані, бізнес-секрети та інші ключові ресурси. Втрата або розголошення цих даних може спричинити фінансові втрати, шкоду репутації та юридичні проблеми. Забезпечення належної інформаційної безпеки та кібербезпеки є необхідним завданням для захисту цих даних.

Забезпечення надійності операцій стає немаловажним завданням для інформаційно-телекомунікаційних підприємств, які відхиляються від традиційних бізнес-моделей та переходять до цифрових систем і мереж. Будь-яке порушення функціонування цих систем може призвести до зупинок у роботі, що призводить до втрат прибутку та погіршення обслуговування клієнтів. Кібербезпека допомагає запобігти таким перервам, забезпечуючи надійність операцій.

Захист від кіберзагроз є надзвичайно важливим завданням в сучасному світі, оскільки кіберзлочинці постійно вдосконалюють свої методи атак і активно шукають нові цілі для вторгнень. Бізнес-середовище повинно бути готовим до різноманітних загроз, таких як віруси, шкідливі програми, фішинг, атаки на мережу та інші. Кібербезпека виступає як ефективний захист від цих загроз і сприяє відновленню систем у випадку кібератак.

Виконання вимог законодавства є обов'язковим завданням для багатьох країн, які встановлюють обов'язкові стандарти щодо захисту конфіденційної інформації та обов'язкової звітності про кіберінциденти. Інформаційно-телекомунікаційні організації повинні дотримуватися цих нормативів, і порушення може призвести до накладення штрафів та інших юридичних наслідків.

Збереження репутації є ключовим аспектом для будь-якого інформаційно-телекомунікаційного підприємства, оскільки репутація вважається одним з найцінніших активів. Втрата довіри клієнтів може мати негативний вплив на діяльність та фінансовий результат. Заходи з інформаційної та кібербезпеки сприяють уникненню витоку даних та інцидентів, які можуть порушити репутацію.

Інформаційна та кібербезпека стали необхідними елементами стратегії інформаційно-телекомунікаційних підприємств у цифровому світі. Забезпечення захисту конфіденційної інформації, надійності операцій, відповідності законодавству, захисту від кіберзагроз та збереження репутації є ключовими аспектами успішного бізнесу в сучасному світі [2]

Сучасний світ та суспільство з кожним днем стають все більш комп’ютеризованими та технологічно-залежними. Якщо раніше співробітники були прив’язані до офісу, то тепер вони мають можливість працювати де завгодно, просто підключившись до серверу компанії із свого особистого пристрою. Це забезпечує не тільки більший рівень гнучкості, але і більшу ефективність працівників.

Такий підхід пропонує все більша кількість підприємств, що дає працівникам можливість виконувати роботу в більш комфортних умовах. Близько 35% підприємств у Європі в даний момент пропонують можливість своїм співробітникам працювати з дому.

Збільшення кількості цих людей ставить перед ІТ-відділами компаній складні питання забезпечення безпеки. Загальні витрати на цю сферу

зростають із року в рік, а пробіли в системі безпеки IT обходяться все дорожче.

Насправді, існуючі ризики досить різноманітні, і втрата даних може виникати в різних формах, наприклад крадіжка пароля або навіть самого пристрою. Найбільший відсоток інцидентів безпеки в світі пов'язаний з «викраденням особистості». Такий кіберзлочин трапляється кожні дві секунди, і, в більшості випадків, основною його причиною є слабкі паролі.

Все це призводить до того, що злочинці можуть легко отримати конфіденційну, особисту або корпоративну інформацію. Тому багато підприємств не використовують в повній мірі можливості позаофісної роботи співробітників, адже інноваційні рішення, які мали б захищати працівників, можуть призвести до нових ризиків та загроз.

Загрози інформаційної безпеки набувають нового вигляду. Це стосується трьох типів задач, які мають вирішувати засоби захисту, включаючи загрози конфіденційності, цілісності та доступності:

– порушення роботи системи та інфраструктури, що забезпечує її підтримку;

– крадіжка інформації;

– загрози, які можуть виникнути внаслідок використання ненадійного захисту конфіденційної інформації.

Із загрозами інформаційної безпеки стикається практично кожен. Значні ризики представляє собою шкідливе ПЗ (віруси, черви, троянські програми, програми-вимагачі), фішинг (отримання доступу до логінів та паролів користувача) і крадіжка особистості (використання чужих персональних даних). Метою кібератаки можуть стати навіть акаунти в соціальних мережах чи додатках, дані банківських карт чи паспортні дані. Крім того, зловмисники активно займаються освоєнням нових сфер, таких як робототехніка, штучний інтелект та інтернет речей (IoT).

Для того, щоб захиститись від нових загроз, необхідні і нові засоби захисту. Які б сподівання ми не покладали на антивіруси, встановлені на ПК, все одно вони залишаються вразливими до різних атак.

Сьогодні важко виділити якусь окрему передову технологію захисту інформаційної системи. Одними з найбільш надійних елементів системи захисту є багатокомпонентні і багатофакторні системи автентифікації, які можуть працювати як окремо, так і поєднуючись між собою. Серед них є стандартні, такі як сканери відбитків пальців, а є і більш нові, наприклад, захист на основі IP-адрес і GPS-трекеру.

Важливим в будь-якій інформаційній системі є забезпечення конфіденційності, цілісності та доступності інформації. Якщо і далі використовувати традиційну парольну автентифікацію для доступу до інформаційних ресурсів, то ризик виникнення кібератак збільшується, адже близько 80 відсотків інцидентів в сфері інформаційної безпеки виникає внаслідок використання слабких паролів.

Альтернативою є багатофакторна автентифікація, до переваг якої відноситься її можливість захисту інформації як від внутрішніх загроз, так і від зовнішніх втручань. Вона ґрунтується на спільному використанні декількох факторів автентифікації, що значно підвищує рівень безпеки.

Отже, інформаційна та кібербезпека залежить, в першу чергу, від самого користувача. Адже саме він приймає рішення про встановлення того чи іншого ПЗ, перехід по посиланню або завантаження файла. Ніяка стратегія безпеки не є абсолютно ідеальною.

У таблиці 1.1 представлена типова модель загроз на підприємстві.

Таблиця 1.1 – Загрози та можливості їх реалізації

Загроза	Реалізація	Джерело
Стихійні явища (пожежа, аварія)	- Несправність обладнання - Легкозаймисті матеріали	Зовнішнє

Продовження таблиці 1.1

Загроза	Реалізація	Джерело
Відмови системи електроживлення	- Відсутність електричних запобіжників - стара чи неякісна електропроводка	Внутрішнє
Втрата чи пошкодження носіїв інформації	- відсутність резервного копіювання - відсутність хмарного сховища	Зовнішнє
Несанкціоноване підключення до ТЗ	- недосконала охоронна система	Зовнішнє
Зчитування даних на робочому екрані або залишення без нагляду робочих документів	- некомпетентність персоналу - відсутність політики безпеки	Зовнішнє
Втрата або розголошення паролів доступу до системи	- некомпетентність персоналу	Зовнішнє
Несанкціоноване підключення до каналів зв’язку	- відсутність захисту або використання застарілих протоколів захисту Інтернет мереж - некомпетентність персоналу - використання слабких паролей	Зовнішнє

Продовження таблиці 1.1

Загроза	Реалізація	Джерело
Соціальна інженерія	- низька мотивація працівників - низький рівень знань працівників - низька кваліфікація персоналу	Зовнішнє

Засоби, заходи протидії та політики безпеки мають бути ненав'язливими і не повинні негативно впливати на продуктивність користувачів. Єдиного засобу захисту бути не може. Очевидно, він ще буде доповнюватися і розширюватися, адже забезпечення інформаційної безпеки – це не готове рішення, а процес. І засоби захисту мають іти в ногу з загрозами, що еволюціонують, та забезпечувати ефективну протидію їм.

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

Недостатня обізнаність співробітників та непорозуміння відповідальності за порушення вимог інформаційної безпеки можуть призвести до фінансових збитків та негативних наслідків для компанії.

Поширення інформації серед співробітників підприємства щодо правил та положень, пов'язаних з інформаційною безпекою, є важливим кроком. Набуття таких знань працівниками та їх відношення до інформаційної безпеки сприятимуть усіляким заходам, спрямованим на захист організації від фізичних або інформаційних інцидентів. Головною метою інформаційної безпеки є навчання людей методам безпеки в Інтернеті та забезпечення ефективного захисту від кіберзлочинності.

Досягнення цілей з обізнаності в галузі безпеки стає можливим, коли вчинки співробітників ґрунтуються на передовій практиці, рекомендованій

для впровадження в рамках політики і програм підвищення обізнаності, розроблених підприємством. Зрозуміло, що у багатьох випадках увага підприємств зосереджується на технічних рішеннях в галузі інформаційної безпеки, замість того, щоб акцентувати постійне оновлення знань співробітників для досягнення стійкої обізнаності з питань безпеки.

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

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.

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»[3].

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 [4].

Ціль навчання персоналу – формування та підтримування необхідного рівня кваліфікації персоналу, з урахуванням вимог підприємства у сфері ІБ і забезпечення високого рівня безпеки у ІБ.

Задачі політики підприємства в області вивчення питань ІБ:

1. Формування і дотримання правил по захисту інформації;

2. Розробка та використання системи навчання, включаючи виявлення потреб у навчанні, плануванні та бюджетування, організування навчання та контролювання його результативності;

3. Розробка навчання відповідно зі специфікою бізнес-процесів підприємства;

4. Формування стандартів навчання;

5. Включення передового досвіду, знань, ефективних методів організації праці у процесі навчання персоналу ІБ;

6. Мотивація співробітників до підвищення безпеки та забезпечення надійності роботи;

7. Регулярна перевірка знань у сфері ІБ та їх застосування на практиці.

Під програмою обізнаності співробітників розуміється використання процесу , регулярного підвищення рівня знань співробітників підприємства у області ІБ.

Основні вимоги, яким всі рішення, що розглядаються, повинні задовольняти:

1. Надавати можливість регулярного навчання співробітників незалежно від їхнього територіального місцезнаходження та без відриву від робочого процесу;

2. Подавати матеріал користувачам у простій та зрозумілій формі;

3. Вартість всіх рішень, що впроваджуються, повинна бути адекватною, і не повинна бути в прямій залежності від кількості учнів.

Виходячи з перелічених вище вимог, зрозуміло, що для вирішення цього завдання підходять різні системи корпоративного дистанційного навчання або ті чи інші «нестандартні» рішення.

Системи дистанційного навчання.

Основним засобом для навчання великої кількості працівників підприємства в даний час, безумовно, є різні системи дистанційного навчання (СДН). Зрозуміло, що СДН – переважно не навчальна програма, а засіб доставки до кінцевого користувача інформації (навчальних матеріалів), яка закладена. Тому при виборі СДН, як правило, слід звертати увагу на два параметри: основний функціонал (управління процесом навчання співробітників, гнучкість формування звітів тощо) та набір навчальних матеріалів, що надаються разом із системою.

"Нестандартні" засоби.

Під «нестандартними» засобами підвищення кваліфікації співробітників компанії в галузі ІБ розуміються різні методи та засоби, які, як правило, не використовуються для навчання, завдяки яким на емоційному та підсвідомому рівні співробітник запам'ятовує навчальний матеріал та розуміє важливість вимог ІБ. Деякими методами такого навчання є:

1. Скринсейвери;

2. Фільми, мультфільми, ролики;

3. Новини з ІБ;

4. Офісне приладдя.

Оцінка кваліфікації працівників

Огляд методів навчання співробітників питанням ІБ не можна було б назвати повним без розгляду можливих методів оцінки ефективності впровадженої в компанії програми навчання.

Одним із прикладів оцінки саме практичних, а не теоретичних знань співробітників є використання соціальної інженерії, коли імітуються ситуації, в яких дії неписьменного користувача можуть призвести до порушення ІБ.

Навчені основним правилам в області ІБ співробітники підприємства і, особливо, які використовують отримані знання практично, істотно знижують ризик порушення ІБ і, як наслідок, зменшують можливі збитки підприємства. При цьому навчання співробітників у галузі ІБ при грамотний підхід не вимагає значних матеріальних та тимчасових витрат.

В даний час існує велика кількість різних методів підвищення обізнаності співробітників в галузі ІБ.

Найбільша ефективність, досягається при комплексному використанні різних елементів.

1.3 Постановка задачі

Відповідно до теоретичних матеріалів, що були проаналізовані, стосовно всіх можливих загроз, які можуть впливати на діяльність підприємства, з подальшим розглядом внутрішніх та зовнішніх ризиків, що можуть бути ініційовані людиною, прийнято висновок щодо доцільності впровадження програми підвищення обізнаності персоналу. Збільшення темпу розвитку інформаційних загроз ускладнює завдання слідкувати за всім, особливо, якщо інформаційна безпека не є головною спеціалізацією працівника. Аналіз матеріалів, що стосуються підвищення обізнаності персоналу в компанії, показав, що використані методи не відповідають сучасним вимогам. Багато з цих методів застарілі, а надана інформація вже неактуальна.

На підставі отриманих даних визначено завдання для розробки програми підвищення обізнаності персоналу на типовому підприємстві галузі телекомунікацій в питаннях інформаційної та кібербезпеки. Також необхідно розробити рекомендації щодо організації підвищення обізнаності персоналу

та надання засобів підтримки інформованості на підприємстві сфери телекомунікацій.

1.4 Висновки до першого розділу

У першому розділі було проведено аналіз загроз, як окремому користувачу, так і на інформаційну-комунікаційній системі в цілому. Встановлено, що основною загрозою інформаційній безпеці підприємства є людина, як співробітник компанії (інсайдер), так і зовнішні зловмисники. Їхні цілі можуть бути подібні, але методи виконання відрізняються через доступність конкретних інструментів, що допомагають досягти поставлених завдань. Також проведено дослідження різних видів зовнішніх і внутрішніх загроз, які можуть виникнути в результаті дій людини і спричинити шкоду діяльності підприємства. Далі детально розглянуто методи та засоби підвищення рівня обізнаності персоналу на підприємстві, з урахуванням ефективності кожного з них. Визначено, що обізнаність в інформаційній безпеці в значній мірі залежить від індивідуальних знань людини. Освіченість щодо методів зловмисників та їхніх тактик може значно зменшити ризик атаки на підприємство або самого співробітника.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Відомості про типове підприємство

У роботі буде розглядатись підприємство галузі телекомунікацій (далі – кол-центр оператора мобільного зв’язку), яке займається обробкою звернень та інформуванням по голосових каналах зв'язку в інтересах головної організації.

На підприємстві циркулює інформація, що містить конфіденційну інформацію клієнтів, персональні дані працівників та технологічну інформацію.

Основний робочий склад працівників кол-центру оператора мобільного зв’язку функціонує цілодобово.

Офіс кол-центру оператора мобільного зв’язку займає 4 поверхи нежилої багатоповерхової будівлі. На території підприємства є паркувальний майданчик, територія охороняється силами самого підприємства.

Підприємство оснащене системою контролю та управління доступом на кожен вхід. Кожний працівник компанії має магнітний ключ, за допомогою якого здатний пройти до офісного приміщення свого відділу.

Пропуск сторонніх осіб на територію здійснюється лише із узгодженням з керівництвом.

Кол-центр оператора мобільного зв’язку складається з наступних працівників:

- керівник філіалу
- заступник керівника
- бухгалтер філіалу
- керівники секторів обслуговування
- оператори
- тренери
- рекрутери
- охоронці
- прибиральниці

- працівники технічного відділу

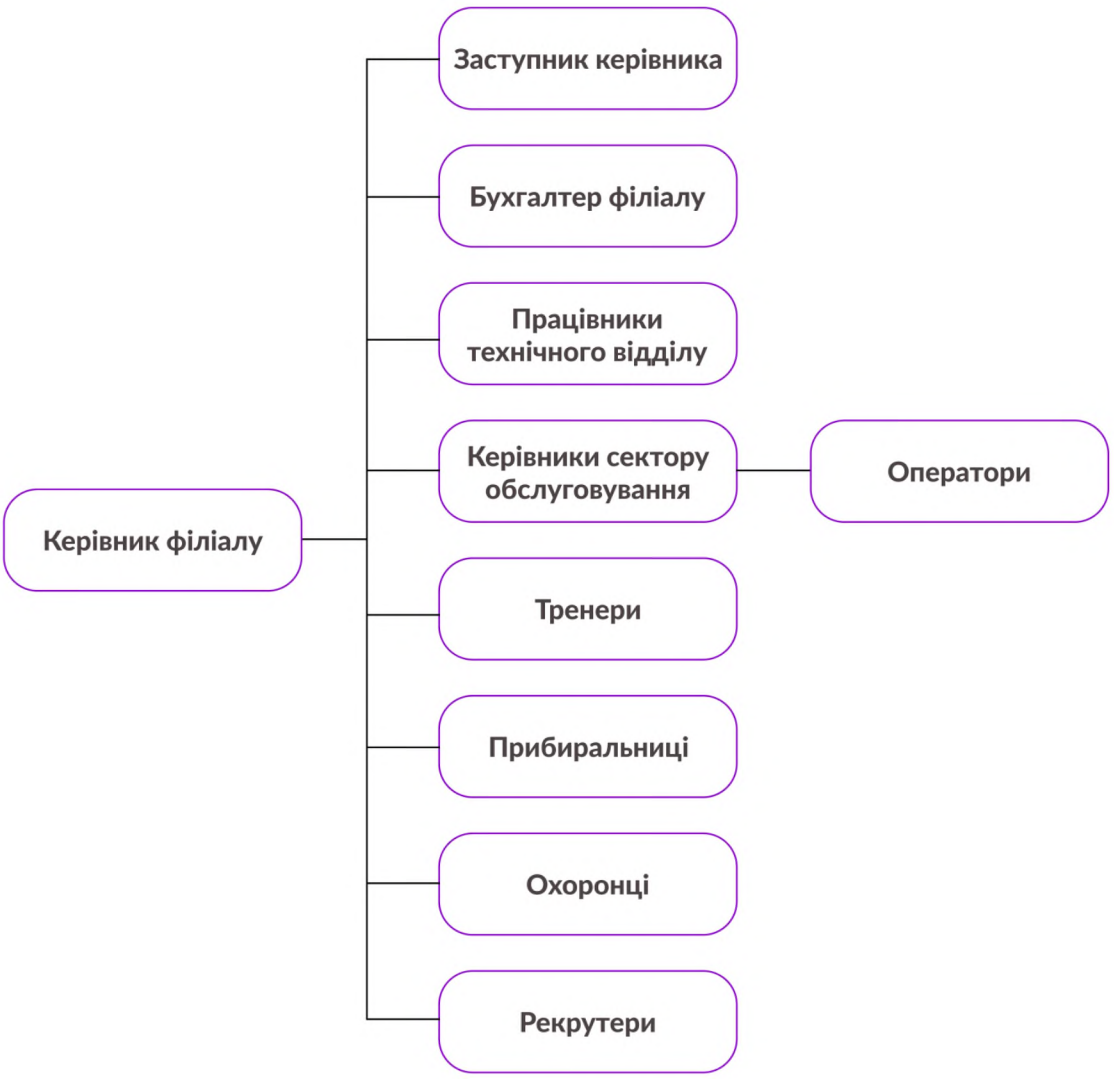


Рисунок 2.1 – Організаційна структура підприємства

Організаційна структура класифікується, як лінійно-функціональна. Відповідно з такою структурою кожен співробітник організації підпорядковується керівництву свого функціонального блоку, а керівники відділів і команд керівнику філіалу.

2.2 Попередня підготовка та затвердження рішення створення СУІБ

Для прийняття рішення про створення СУІБ необхідне створення робочої групи та призначення керівника. До її складу мають увійти: представники керівництва організації, представники відділів, старші спеціалісти, що забезпечують інформаційну безпеку в компанії. Дані

співробітники повинні бути усвідомленні про механізми систем менеджменту. До складу робочої групи можуть входити також консультанти, що спеціалізуються на питаннях СУІБ. Робоча група повинна мати всю необхідну нормативно-методичну базу для успішного створення, відповідно вимогам [5, 6].

Попередній аналіз оцінює галузі діяльності організації, які будуть охоплені СУІБ. При виборі області діяльності, в якій робоча група буде впроваджувати механізми СУІБ, повинні враховуватися наступні критерії: діяльність та послуги, що надаються організацією своїм партнерам і клієнтам, цільова інформація, безпека якої повинна бути забезпечена, бізнес - процеси, що забезпечують обробку інформації, відділи і співробітники організації, задіяні в даних бізнес – процесах, програмно - технічні засоби, що забезпечують функціонування даних процесів, територія компанії, в рамках яких відбуваються збір, обробка та передача інформації. Результатом є узгоджена та затверджена з керівництвом область діяльності організації, в рамках якої планується створення СУІБ[5, 6].

Також в процесі створення системи потрібно постійно аналізувати та виявляти невідповідності до нормативних документів. Для уточнення обсягу робіт і необхідних витрат на створення і подальшу сертифікацію СУІБ, члени робочої групи проводять роботи з виявлення й аналізу невідповідностей існуючих в організації заходів захисту до вимог стандарту. При цьому аналізуються як прийняті організаційні заходи по плануванню, впровадженню, аудиту та модернізації, так і використовувані програмно - технічні засоби і механізми захисту інформації. На даному етапі компанія також може вибрати незалежний орган з сертифікації систем менеджменту, що має відповідну акредитацію. [6].

2.3 Необхідні складові документаційного забезпечення СУІБ

Список, що містить мінімальний набір документів та облік записів, необхідні для ISO/IEC 27001 версії 2022 року наведений у таблиці 1.1-1.2.

Також ті документи, які виходять з додатку А в цьому стандарті(номер пункту починається з неї) є необов'язкові, якщо підприємство вирішує, що не буде ніяких ризиків або інших вимог для використання СУІБ.

Цей список не є остаточним і може доповнюватись або змінюватись, тому що сам стандарт має гнучкість для використання альтернативних документів. Згодом при необхідності підприємство може додавати до списку інші документи, які так чи інакше будуть підвищувати рівень ІБ та основуватися на вимогах СУІБ та досвіду[7].

Таблиця 2.1 – мінімальний набір записів

№	Записи	Номер пункту стандарту
1	Записи про рівень підготовки, навички, досвід та кваліфікації	7.2
2	Моніторинг та вимірювання результатів	9.1
3	Програма внутрішнього аудиту	9.2
4	Результати внутрішніх аудитів	9.2
5	Результати аналізу з боку керівництва	9.3
6	Результати коригуючих дій	10.2

Таблиця 2.2 – мінімальний набір документів

№	Документи	Задовольняє номер пункту стандарту
1	Визначення сфери застосування системи управління інформаційною безпекою	4.3
2	Політика інформаційної безпеки	5.2, 6.2
3	Оцінка ризиків інформаційної безпеки	6.1.2
4	Положення щодо застосовності	6.1.3
5	План оброблення ризиків	6.1.3
6	Оцінювання ризиків	8.2

Продовження таблиці 2.2

№	Документи	Задовольняє номер пункту стандарту
7	Процедура управління документами	7.5, 7.5.3
8	Процедура управління записами	7.5, 7.5.2
9	Внутрішній аудит	9.2
10	Невідповідності й корегувальні дії	10.2
11	Визначення ролей та обов'язків	7.2
12	Інвентаризація ресурсів СУІБ	8.1
13	Припустиме використання ресурсів СУІБ	8.1
14	Політика контролю доступу	9.1

Політика інформаційної безпеки - набір законів, заходів, правил, вимог, обмежень, інструкцій, нормативних документів, рекомендацій тощо, що регламентують порядок обробки інформації та спрямованих на захист інформації від певних видів загроз.[7]

Політика інформаційної безпеки є фундаментальним документом забезпечення всього циклу безпеки інформації в компанії. Тому вище керівництво компанії має бути зацікавлене у знанні та чіткому дотриманні основних її пунктів усім персоналом компанії. Усі співробітники підрозділів, які відповідають за режим інформаційної безпеки компанії, мають бути ознайомлені з політикою інформаційної безпеки під розпис. Адже на них ляже відповідальність за перевірку дотримання вимог політики інформаційної безпеки та знання основних її пунктів персоналом компанії в частині, що їх стосується. Також має бути визначено процес проведення таких перевірок, обов'язки посадових осіб, які здійснюють такі перевірки, та розроблено графік перевірок.

Політика інформаційної безпеки може бути розроблена як окремого компонента інформаційної системи, так інформаційної системи загалом. Політика інформаційної безпеки має враховувати такі особливості

інформаційної системи: технологію обробки інформації, обчислювальне середовище, фізичне середовище, середовище користувачів, правила розмежування доступу тощо.

Політика інформаційної безпеки має забезпечувати комплексне використання правових, морально-етичних норм, організаційних та технічних заходів, програмних, апаратних та програмно-апаратних засобів забезпечення інформаційної безпеки, а також визначати правила та порядок їх використання. Політика інформаційної безпеки має базуватися на таких принципах: безперервність захисту, достатність заходів та засобів захисту, їх відповідність ймовірності реалізації загроз, рентабельність, гнучкість структури, простота управління та використання тощо.

Політика безпеки – це комплекс превентивних заходів щодо захисту конфіденційних даних та інформаційних процесів на підприємстві. Політика безпеки включає вимоги на адресу персоналу, менеджерів і технічних служб. Основні напрямки розробки політики безпеки[8]:

1. Визначення які дані та наскільки серйозно необхідно захищати;

2. Визначення хто і яку шкоду може завдати фірмі в інформаційному аспекті;

3. Обчислення ризиків та визначення схеми зменшення їх до прийнятної величини.

Існують дві системи оцінки поточної ситуації у сфері інформаційної безпеки на підприємстві. Вони отримали образні назви "дослідження знизу вгору" та "дослідження зверху вниз". Перший метод досить простий, вимагає набагато менших капітальних вкладень, але й має менші можливості. Він заснований на відомій схемі: "Ви - зловмисник. Ваші дії?". Тобто служба інформаційної безпеки, ґрунтуючись на даних про всі відомі види атак, намагається застосувати їх на практиці з метою перевірки, а чи можлива така атака з боку реального зловмисника.

Метод "згори вниз" є, навпаки, детальний аналіз всієї існуючої схеми зберігання та обробки інформації. Першим етапом цього є, як і завжди,

визначення, які інформаційні об'єкти і потоки необхідно захищати. Далі слід вивчення поточного стану системи інформаційної безпеки з метою визначення, що з класичних методик захисту інформації вже реалізовано, в якому обсязі і на якому рівні. На третьому етапі проводиться класифікація всіх інформаційних об'єктів на класи відповідно до її конфіденційності, вимог до доступності та цілісності (незмінності).

Далі слідує з'ясування, наскільки серйозні збитки можуть завдати фірмі розкриття чи інша атака на кожен конкретний інформаційний об'єкт. Цей етап зветься "обчислення ризиків". У першому наближенні ризиком називається твір "можливих збитків від атаки" на "ймовірність такої атаки".

Політика інформаційної безпеки має містити пункти, в яких була б присутня інформація наступних розділів:

1. Концепція безпеки інформації;

2. Визначення компонентів та ресурсів інформаційної системи, які можуть стати джерелами порушення інформаційної безпеки та рівень їх критичності;

3. Зіставлення загроз із об'єктами захисту;

4. Оцінка ризиків;

5. Оцінка величини можливих збитків, пов'язаних із реалізацією загроз;

6. Оцінка витрат на побудову системи інформаційної безпеки;

7. Визначення вимог до методів та засобів забезпечення інформаційної безпеки;

8. Вибір основних рішень щодо забезпечення інформаційної безпеки;

9. Організація проведення відновлювальних робіт та забезпечення безперервного функціонування інформаційної системи;

10. Правила розмежування доступу.

2.4 Розробка програми підвищення обізнаності персоналу

У сучасних умовах, поряд зі знанням та виконанням трудових обов'язків, від працівника потрібне знання специфічних питань, пов'язаних із

забезпеченням ІБ, що обумовлено не лише нормативними документами Компанії, а й елементарними вимогами безпеки та необхідністю збереження конфіденційної інформації в таємниці.

На жаль, значна кількість інцидентів ІБ, пов'язаних насамперед із витоками конфіденційної інформації, вірусними зараженнями або знищенням/спотворенням інформації, відбувається з вини працівників. Таким чином, рівень обізнаності користувачів у сфері інформаційної безпеки є одним із основних факторів, які суттєво впливають на стан ІБ у Компанії.

На підприємстві має бути організована документально оформлена та затверджена керівництвом робота з персоналом у цьому напрямі, включаючи розробку та реалізацію планів та програм навчання та підвищення обізнаності в галузі ІБ та контролю результатів виконання зазначених планів. Тут же йдеться про періодичність навчання та зміст програм:

- За існуючими політиками ІБ;
- Щодо застосовуваних захисних заходів;
- Щодо правильного використання захисних заходів відповідно до внутрішніх документів;
- За значимістю та важливістю діяльності працівників для забезпечення ІБ.

У випадку до системи підвищення обізнаності працівників підприємства пред'являються такі вимоги:

- Можливість регулярного навчання будь-якої кількості працівників, незалежно від їхнього територіального місцезнаходження та без відриву від робочого процесу;
- Простота та доступність навчальних матеріалів для різних категорій працівників;
- Можливість оперативного внесення змін до програм підвищення обізнаності та навчальних матеріалів.

Важливим аспектом роботи щодо підвищення обізнаності персоналу з питань ІБ є безперервність цього процесу. Законодавство та вимоги

регуляторів швидко змінюються, з'являються нові загрози ІБ, нові інформаційні системи – все це необхідно оперативно відображати у програмах підвищення обізнаності. Для працівників компанії безперервність навчання полягає у повторенні вимог та правил ІБ (щоб вони не забували). Також важливо інформувати всіх працівників про зміни, що відбулися, у політиках безпеки та процедурах забезпечення ІБ.

Кінцевою метою реалізації вищезгаданих програм є зниження збитків та втрат (матеріальних, моральних, репутаційних) від загроз, пов'язаних з людським фактором при роботі з інформаційними ресурсами компанії.

Як і будь-яка система навчання, система підвищення обізнаності має на увазі використання певних форм, видів та методів навчання. Вибір того чи іншого методу або форми залежить від цілого ряду факторів, таких як: цілі організації, кадрова політика, характеристики персоналу, що навчається, його чисельність і фінансування.

У документі NIST SP 800-50 «Створення програми підвищення кваліфікації та навчання безпеки інформаційних технологій» описується три компоненти успішних програм підвищення обізнаності щодо кібербезпеки [9]:

1. Розробка політики безпеки, яка відображає бізнес-потреби, обмежені відомими ризиками;

2. Інформування користувачів про їхні обов’язки щодо безпеки ІТ, як це задокументовано в політиці безпеки та процедурах підприємства;

3. Встановлення процесів моніторингу та перегляду програми.

Ефективна програма з підвищення обізнаності та навчання в галузі ІТ-безпеки може бути успішною, лише якщо матеріал, який використовується в програмі, чітко базується на політиці програми ІТ-безпеки підприємства та політиках щодо конкретних ІТ-проблем. Якщо політика написана чітко та лаконічно, то інформованість і навчальний матеріал – на основі політики – будуть побудовані на міцній основі.

Крім того, виділяють наступні компоненти розробки програми обізнаності персоналу:

- Залучення вищого керівництва передбачає, що керівництво має підтримувати інформаційну програму, щоб користувачі були осведомлені про участь вищого керівництва і реагували відповідно.

- Наполегливість: в рамках програми підвищення обізнаності ефективним підходом є розробка річного плану з чітким визначенням конкретних етапів навчання на протязі року.

- Актуальність: програми з кібербезпеки повинні відповідати потребам та щоденним завданням користувачів, для яких конкретно розробляється програма інформування про кібербезпеку.

- Зворотній зв'язок: Здійснення практичних тренувань підсилює заходи, спрямовані на підвищення обізнаності, які включені до кампанії або програми.

- Оцінювання: для визначення потрібних корегувань необхідно розуміти, з якого етапу розпочалася програма та як вона прогресує.

Враховуючи всі аспекти, програма підвищення обізнаності з кібербезпеки повинна охоплювати всіх працівників підприємства, при цьому важливо, щоб керівництво взяло на себе провідну роль і служило прикладом для всіх користувачів. Така програма виступає засобом розповсюдження інформації всередині організації та постійно підтримується в актуальному стані, адаптуючись до поточних загроз і змін у стратегії реагування організації на ці загрози.

Відповідно до NIST SP 800-50 потрібно розглянути ролі на промисловому підприємстві та відповідні ролям обов’язки персоналу, який буде розробляти програму. Дані ролі наведено в Таблиці 2.3.

Таблиця 2.3 – Ролі та обов'язки персоналу, який буде розробляти програму на підприємстві

Посада	Обов'язки
Керівник філіалу	Переконання в тому, що програма реалізована. Призначення відповідальності для відділів інформаційних технологій та ІБ.
Керівник ІТ відділу	Переконання в тому, що керівники розуміють розроблену програму, а також проінформовані про хід цієї програми Створення загальної обізнаності цієї програми та створення відповідної стратегії
Тренери	Забезпечення ознайомлення та розробки навчальних матеріалів, які є своєчасними та доречними для цільової аудиторії
Керівники	Обговорення з керівництвом їх відповідальність в програмі. Переконання в тому, що всі оператори пройшли належну та відповідну підготовку для виконання обов'язків щодо кібербезпеки для систем, до яких вони мають доступ
Оператори	Проходження належного навчання, правил поведінки та вивчення матеріалів, до яких вони мають доступ Дотримання політик безпеки та процедур кібербезпеки на підприємстві
Інші працівники	Приймання участі в розробці та впровадженні програми з підвищення обізнаності персоналу у відповідній ролі.

Далі важливо розглянути модель програми підвищення обізнаності. Організація може обрати централізований чи розподілений підхід до адміністрування різних аспектів програми інформування про кібербезпеку, враховуючи свою структуру та наявні ресурси. Згідно з NIST SP 800-50 [9], існують три основні стратегії для проектування, розробки та впровадження програм 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.

Для більшості інформаційно-телекомунікаційних 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.

Разглянемо детальніше цю модель:

Модель 1. Централізована політика, стратегія та реалізація:

У цій моделі відповідальність і бюджет для всієї організації з обізнаності з IT-безпекою та програми навчання покладаються на центральний орган. Усі директиви, розробка стратегії, планування та планування координуються цим органом «обізнаності та навчання з питань безпеки». Модель зображено на рис 2.2

Оскільки стратегія підвищення обізнаності та навчання розробляється центральним органом влади, оцінка потреб, яка допомагає визначити стратегію, також проводиться центральним органом. Центральний орган влади також розробляє навчальний план, а також інформаційні та навчальні матеріали. Метод(и) впровадження матеріалу в усій організації визначається та виконується центральним органом. Як правило, у такій організації і IT-директор, і менеджер програми IT-безпеки організаційно розташовані в цьому центральному органі.

Комунікація між центральним органом влади та організаційними підрозділами відбувається в обох напрямках. Центральний орган передає організаційним підрозділам політичні директиви агентства щодо обізнаності з IT-безпеки та навчання, стратегію проведення програми, а також матеріали та метод(и) впровадження. Організаційні підрозділи надають інформацію на

запит центрального органу. Наприклад, для виконання своїх обов'язків центральний орган може збирати дані про кількість відвідувачів інформаційних сесій, кількість людей, які пройшли підготовку з певної теми, та кількість людей, які ще мають відвідати інформаційні та навчальні сесії. Організаційний підрозділ також може надати зворотній зв'язок щодо ефективності інформування та навчального матеріалу та відповідності методу(ів), використаного(их) для впровадження матеріалу. Це дозволяє центральному органу точно налаштовувати, додавати або видаляти матеріал або змінювати метод(и) реалізації.

Цю централізовану модель управління програмою часто використовують агентства, які:

- Є відносно невеликими або мають високий ступінь структурованості та централізованого управління більшістю IT-функцій;
- Володіють на рівні штабу необхідними ресурсами, досвідом і знаннями місії(й) і операцій на рівні підрозділу;
- Мають високий ступінь подібності місії та оперативних цілей у всіх його компонентах.

Рисунок 2.2 – Модель 1: Централізована політика, стратегія та реалізація

Оцінка потреб — це процес, який можна використовувати для визначення потреб організації в обізнаності та навчанні. Результати оцінки потреб можуть надати обґрунтування, щоб переконати керівництво виділити достатні ресурси для задоволення визначених потреб у обізнаності та навчанні.

У проведенні оцінки потреб важливо залучити ключовий персонал. Як мінімум, з точки зору будь-яких потреб у спеціальному навчанні, слід звернути увагу на наступні ролі:

- Виконавче управління – керівники організацій повинні повністю розуміти директиви та закони, які є основою для програми безпеки. Вони також повинні розуміти свою керівну роль у забезпеченні повної відповідності користувачів у своїх підрозділах.

- Персонал служби безпеки (керівники програм безпеки та офіцери служби безпеки) – ці особи виступають експертами-консультантами для своєї організації, тому мають бути добре обізнаними щодо політики безпеки та загальноприйнятих найкращих практик.

- Власники систем – власники повинні мати широке уявлення про політику безпеки та високий ступінь розуміння засобів контролю безпеки та вимог, що застосовуються до систем, якими вони керують.

- Системні адміністратори та IT-персонал підтримки – яким доручено високий рівень повноважень щодо операцій підтримки, що мають важливе значення для успішної програми безпеки, цим особам потрібен вищий рівень технічних знань щодо ефективних методів безпеки та впровадження.

- Операційні менеджери та користувачі системи – ці особи потребують високого рівня обізнаності з безпекою та навчання щодо контролю безпеки та правил поведінки для систем, які вони використовують для здійснення бізнес-операцій.

Різноманітні джерела інформації в агентстві можуть бути використані для визначення потреб у обізнаності з IT-безпекою та навчання, і існують

різні способи збору такої інформації. Ось основні методи збору інформації, як частини оцінки потреб:

- Інтерв'ю з усіма визначеними ключовими групами та організаціями

- Організаційні опитування

- Огляд і оцінка доступних ресурсних матеріалів, таких як поточні інформаційні та навчальні матеріали, графіки навчання та списки учасників

- Аналіз показників, пов'язаних із обізнаністю та навчанням (наприклад, відсоток користувачів, які пройшли необхідний сеанс підвищення обізнаності або контакту, відсоток користувачів зі значними обов'язками щодо безпеки, які пройшли навчання з матеріалами для певних ролей)

- Огляд планів безпеки для загальних систем підтримки та основних програм для визначення власників систем і програм і призначених представників безпеки

- Огляд системної інвентаризації та баз даних ідентифікаторів користувачів програм, щоб визначити всіх, хто має доступ

- Огляд будь-яких висновків та/або рекомендацій від наглядових органів (наприклад, розслідування Конгресу, генерального інспектора, внутрішньої перевірки/аудиту та програми внутрішнього контролю) або перегляд програм щодо програми IT-безпеки

- Бесіди та інтерв'ю з керівництвом, власниками загальних систем підтримки та основних програм, а також іншим персоналом організації, чиї бізнес-функції залежать від IT

- Аналіз подій (таких як атаки на відмову в обслуговуванні, пошкодження веб-сайтів, викрадення систем, використаних у наступних атаках, успішні вірусні атаки) може вказувати на необхідність навчання (або додаткового навчання) певних груп людей

- Перегляд внесення технічних або інфраструктурних змін

- Вивчення тенденцій, вперше виявлених у галузевих, академічних чи урядових публікаціях або навчальними/освітніми організаціями.

Використання цих «систем раннього попередження» може дати розуміння проблеми в організації, яка ще не розглядається як проблема.

Рисунок 2.3 ілюструє загальні питання, що стосуються конкретного підприємства, які необхідно зрозуміти на початку оцінки потреб. Техніки, показані на рисунку 2.3, повинні надати інформацію, яка дозволить зрозуміти ці проблеми. Ці питання повинні внести необхідну інформацію в процес оцінки потреб. Розуміння їх допоможе сформувати стратегію та розробку програми навчання та обізнаності з IT-безпеки.

Рисунок 2.3 – Розуміння загальних проблем, що стосуються конкретного підприємства

Аналіз зібраної інформації має дати відповіді на ключові запитання:

1. Яка обізнаність, навчання та/або освіта потрібні (тобто, що потрібно)?

2. Що зараз робиться для задоволення цих потреб?

3. Який поточний стан щодо вирішення цих потреб (тобто, наскільки ефективні поточні зусилля)?

4. Де розрив між потребами та тим, що робиться (тобто, що ще потрібно зробити)?

5. Які потреби найбільш критичні?

Іншим важливим аспектом оцінки потреб є відповідна обізнаність щодо ІТ-безпеки та вимоги програми навчання. Наприклад, якщо просвітницькі та навчальні матеріали будуть представлені з використанням технології комп'ютерного навчання, технічну оцінку слід провести на платформі обробки організації (наприклад, локальна мережа, робочі станції, відеокарти, колонки), щоб визначити, чи існуюче середовище підтримуватиме нову або розширену програму інформування та навчання. Подібним чином, якщо організація планує забезпечити навчання в аудиторії, оцінка потреб повинна визначити, чи існує достатній простір для ефективного навчального середовища. Можуть також виникнути проблеми з персоналом, включаючи працівників з обмеженими можливостями та особливими потребами.

Після завершення оцінки потреб буде доступна інформація, необхідна для розробки плану інформування та навчання. План має охоплювати всю організацію та включати пріоритети, визначені оцінкою потреб.

Розробка стратегії та плану інформування та навчання

Завершення оцінки потреб дозволяє агентству розробити стратегію для розробки, впровадження та підтримки своєї програми навчання та обізнаності з ІТ-безпекою. План – це робочий документ, що містить елементи, що складають стратегію. План має обговорювати такі елементи:

- Існуюча національна та місцева політика, яка вимагає інформування та навчання;

- Обсяг програми інформування та навчання;

- Ролі та обов'язки персоналу агентства, який повинен розробляти, розробляти, впроваджувати та підтримувати інформаційний і навчальний матеріал, і який повинен гарантувати, що відповідні користувачі відвідують або переглядають відповідний матеріал;

- Цілі, яких необхідно досягти для кожного аспекту програми (наприклад, обізнаність, навчання, освіта, професійний розвиток);

- Цільові аудиторії для кожного аспекту програми;

- Обов'язкові (і якщо застосовано, додаткові) курси або матеріали для кожної цільової аудиторії;

- Навчальні цілі для кожного аспекту програми;

- Теми, які розглядаються на кожній сесії чи курсі;

- Методи розгортання, які будуть використовуватися для кожного аспекту програми;

- Документація, відгуки та докази навчання для кожного аспекту програми;

- Оцінка та оновлення матеріалу для кожного аспекту програми;

- Частота, з якою кожній цільовій аудиторії слід надавати матеріал.

Розвиток обізнаності та навчальний матеріал:

Після розробки програми підвищення обізнаності та навчання можна розробити допоміжні матеріали. Матеріал слід розробляти з урахуванням наступного:

- Яку поведінку ми хочемо зміцнити?» (обізнаність);

- «Яким навичкам ми хочемо навчити аудиторію?»

В обох випадках увага має бути зосереджена на конкретному матеріалі, який учасники мають включити у свою роботу. Учасники будуть уважні та включатимуть те, що вони побачать або почують під час сеансу, якщо вважають, що матеріал розроблено спеціально для них. Будь-яка презентація, яка «здається» законсервованою — безособовою та настільки загальною, що може бути застосована до будь-якої аудиторії — буде видалена як ще одна із щорічних сесій «ми тут, тому що ми повинні бути тут». Однак програма підвищення обізнаності та навчання може бути ефективною, якщо матеріал цікавий і актуальний.

У якийсь момент буде поставлено запитання: «Я розвиваю обізнаність чи просто читаю навчальний матеріал?» Загалом, оскільки мета просвітницького матеріалу – просто зосередити увагу на належній практиці безпеки, повідомлення, яке надсилається під час просвітницької роботи, має

бути коротким і простим. Повідомлення може торкатися однієї теми або кількох тем, про які аудиторія має знати.

Аудиторія поінформованості повинна включати всіх користувачів в організації. Повідомлення, яке буде поширене через програму підвищення обізнаності або кампанію, має інформувати всіх людей про їхні спільні обов'язки щодо ІТ-безпеки. З іншого боку, повідомлення на тренінгу спрямоване на певну аудиторію. Повідомлення в навчальних матеріалах має містити все, що стосується безпеки, що учасники повинні знати, щоб виконувати свою роботу. Навчальний матеріал, як правило, набагато глибший, ніж матеріал, який використовується під час просвітницької сесії чи кампанії.

Розвиваючий довідковий матеріал

Питання, на яке потрібно відповісти, починаючи розробляти матеріал для загальноорганізаційної програми або кампанії, таке: «Що ми хочемо, щоб усі співробітники агентства знали про ІТ-безпеку?» План інформування та навчання повинен містити перелік тем. Консультації електронною поштою, веб-сайти щоденних новин з ІТ-безпеки в Інтернеті та періодичні видання є гарним джерелом ідей і матеріалів. Політика агентства, перевірки програм, внутрішні аудити, перевірки програм внутрішнього контролю, самооцінки та вибіркові перевірки також можуть визначити додаткові теми для розгляду.

Вибір тем для підвищення обізнаності

Значну кількість тем можна згадати та коротко обговорити під час будь-якої сесії чи кампанії. Теми можуть включати:

- Використання та керування паролем, включаючи створення, частоту змін і захист;

- Захист від вірусів, троянів та іншого шкідливого коду – сканування, оновлення визначення;

- Політика – наслідки недотримання;

- Невідомий електронний лист/вкладення;

- Використання Інтернету – дозволене чи заборонене; моніторинг активності користувачів

- Спам;

- Резервне копіювання та зберігання даних – централізований або децентралізований підхід;

- Соціальна інженерія;

- відповідь на випадок – до кого звертатися? «Що мені робити?»

- Зміни в системному середовищі – збільшення ризиків для систем і даних (наприклад, вода, вогонь, пил або бруд, фізичний доступ);

- Інвентаризація та передача власності – визначте відповідальну організацію та обов'язки користувачів (наприклад, санітарна обробка медіа);

- Проблеми особистого користування та отримання проблем – системи на роботі та вдома;

- Питання безпеки портативних пристроїв – вирішуйте проблеми як фізичної, так і бездротової безпеки;

- Особисті системи та програмне забезпечення на роботі – вкажіть, дозволено чи ні (наприклад, авторські права);

- Проблеми з обмеженнями ліцензії на програмне забезпечення – вирішуйте, коли копії дозволені та заборонені;

- Індивідуальна відповідальність – поясніть, що це означає в організації;

- Контроль відвідувачів і фізичний доступ до приміщень – обговоріть відповідну політику та процедури фізичної безпеки, наприклад, кидайте виклик незнайомцям, повідомляйте про незвичну діяльність;

- Безпека робочого столу – обговоріть використання заставок, обмеження перегляду відвідувачами інформації на екрані (запобігання/обмеження «серфінгу плечем»), пристрої резервного живлення від акумулятора, дозволений доступ до систем;

- Захист конфіденційної інформації – у системі, в архіві, на резервних носіях, у паперовій формі та до знищення;

- Етикет електронної пошти – прикріплені файли та інші правила.

Джерела інформаційного матеріалу

Існують різноманітні джерела матеріалів щодо обізнаності з питань безпеки, які можна включити в програму підвищення обізнаності. Матеріал може стосуватися конкретної проблеми або, в деяких випадках, може описувати, як розпочати розробку цілої програми підвищення обізнаності, сесії чи кампанії. Джерела актуальних матеріалів можуть включати:

- Повідомлення електронною поштою, надіслані галузевими групами новин, академічними установами чи відділом ІТ-безпеки організації;

- Професійні організації та постачальники;

- Щоденні відвідування веб-сайтів новин ІТ-безпеки в Інтернеті;

- Періодичні видання;

- Конференції, семінари та курси.

Інформаційний матеріал можна розробляти, використовуючи одну тему за раз, або створювати шляхом поєднання кількох тем чи повідомлень у презентацію. Наприклад, плакат або слоган на інструменті підвищення обізнаності має містити одну тему, тоді як заняття під керівництвом інструктора чи веб-презентація можуть містити багато тем. Незалежно від обраного підходу, обсяг інформації не повинен перевищувати аудиторію. Коротка згадка про вимоги (політику), проблеми, які вимоги були розроблені для вирішення, і дії, які необхідно вжити, є основними темами, які повинні бути висвітлені в типовій презентації поінформованості.

Техніки для надання інформаційного матеріалу:

Існує багато методів, щоб отримати повідомлення про безпеку ІТ або серію повідомлень, які поширюються на підприємстві. Обраний метод(и) залежить від ресурсів і складності повідомлення(ів).

Методи, які агентство може розглянути, включають, але не обмежуються:

- Повідомлення на засобах підвищення обізнаності (наприклад, ручки, брелоки, листівки, блокноти, аптечки першої допомоги, набори для

прибирання, дискети з повідомленням, закладки, фрісбі, годинники, картки «попався»)

- Плакати, «списки дій і заборон» або контрольні списки

- Заставки та попереджувальні банери/повідомлення

- Інформаційні бюлетені

- Сповіщення між робочими столами (наприклад, друкований односторінковий бюлетень яскравих кольорів – або по одному на стіл, або надсилається через офіс, – який розповсюджується через поштову систему організації)

- Повідомлення електронної пошти в межах підприємства

- Відеокасети

- Веб-сесії

- Комп'ютерні сесії

- Особисті заняття під керівництвом інструктора

- Дні IT-безпеки або подібні заходи

- Спливаючий календар із контактною інформацією служби безпеки, щомісячними порадами щодо безпеки тощо.

- Кросворди

- Програма нагородження (наприклад, таблички, чашки, листи подяки)

Деякі методи, які піддаються розповсюдженню одного повідомлення, включають використання інструментів обізнаності, плакатів, списків доступу, заставок і попереджувальних банерів, сповіщень від столу до столу, повідомлень електронної пошти в межах підприємства та програм нагород.

Методи, які можуть бути досить недорогими для впровадження, включають повідомлення про інструменти підвищення обізнаності, плакати, списки доступу, списки «що робити і чого не можна робити», контрольні списки, заставки та банери з попередженнями, сповіщення між робочими столами, повідомлення електронною поштою для всього агентства, в - індивідуальні заняття під керівництвом інструктора та програми винагород.

Методи, які можуть вимагати більше ресурсів, включають інформаційні бюлетені, відеокасети, веб-сеанси, комп'ютерні сеанси та сеанси телеконференцій.

На додаток до того, щоб зробити інформаційний матеріал цікавим і актуальним, повторення інформаційного повідомлення та використання різноманітних способів представлення цього повідомлення може значно покращити утримання користувачами уроків або проблем, пов'язаних з інформуванням. Наприклад, обговорення під час сеансу під керівництвом інструктора про те, як уникнути атаки соціальної інженерії, можна підкріпити плакатами, періодичними повідомленнями електронної пошти для всього агентства та повідомленнями про засоби підвищення обізнаності, які розповсюджуються серед користувачів.

Техніка подачі навчального матеріалу

Методи ефективної доставки навчального матеріалу повинні використовувати переваги технології, яка підтримує такі функції:

- Простота використання (наприклад, легкий доступ і легке оновлення/обслуговування);

- Масштабованість (наприклад, можна використовувати для різних розмірів аудиторії та в різних місцях);

- Підзвітність (наприклад, збір і використання статистики щодо ступеня завершеності);

- Широка база галузевої підтримки (наприклад, достатня кількість потенційних постачальників, кращі шанси знайти подальшу підтримку).

Деякі з найпоширеніших методів, які можуть використовувати підприємства, включають:

- Інтерактивне відеонавчання – є одним із кількох методів дистанційного навчання, доступних для доставки навчального матеріалу. Ця технологія підтримує двосторонню інтерактивну аудіо- та відеоінструкцію. Інтерактивна функція робить техніку більш ефективною, ніж неінтерактивні, але вона дорожча.

- Веб-навчання – ця методика зараз є найпопулярнішою для розподілених середовищ. «Учасники» веб-сесії можуть навчатися самостійно та навчатися у власному темпі. Функції тестування та підзвітності можуть бути вбудовані для вимірювання продуктивності. Моделі навчання, що включають цю техніку, починають надавати додаткові переваги взаємодії між викладачем і студентом або між студентами.

- Навчання за допомогою комп'ютера, не пов'язане з Інтернетом – ця методика залишається популярною навіть за наявності Інтернету. Це може бути ефективним методом розповсюдження навчальних матеріалів, особливо якщо доступ до веб-матеріалів неможливий. Подібно до веб-навчання, ця техніка не передбачає взаємодії між викладачем і студентами або між студентами

- Навчання на місці під керівництвом інструктора (включаючи презентації однолітків і наставництво) – це одна з найстаріших, але одна з найпопулярніших методик донесення навчального матеріалу до аудиторії. Найбільшою перевагою методики є інтерактивність навчання. Однак ця техніка має кілька потенційних недоліків. У великій організації можуть виникнути труднощі з плануванням достатньої кількості занять, щоб їх могла відвідувати вся цільова аудиторія. В організації, яка має широко розподілену робочу силу, можуть бути значні витрати на проїзд викладачів і студентів. Хоча існують проблеми для розподілених середовищ, деякі учні віддають перевагу цьому традиційному методу над іншими.

- Використання технології штучного інтелекту

Поєднання різних методів навчання в одній сесії може бути ефективним способом подати матеріал і утримати увагу аудиторії. Наприклад, показ відео під час уроку під керівництвом інструктора дозволяє аудиторії зосередитися на іншому джерелі інформації. Відео також може підкріпити те, що презентував інструктор. Інтерактивне відеонавчання, веб-навчання, і комп'ютерне навчання без Інтернету також можна

використовувати як частину навчального сеансу під керівництвом інструктора.

Ефективні програми навчання та інформування про безпеку є багатофакторними. У таблиці 2.4 наведені дії, які включаються у програму навчання та їх регулярність.

Таблиця 2.4 – Дії, які включаються у програму навчання та їх регулярність.

Дії	Регулярність
Розгортання навчальних модулів, які охоплюють критичні для організації теми, пов'язані з поведінкою, політикою чи очікуваннями відповідності	1 раз на рік
Імітація атак фішингу та соціальної інженерії, завдяки чому співробітники змушені шукати «червоні прапорці» в будь-якому отриманому повідомленні	На регулярній основі
Додаткові допоміжні повідомлення, методи доставки інформації, канали зв'язку та інтерактивні дії, щоб організація мала найкращий шанс ефективно розвинути стале мислення щодо безпеки в кожному співробітнику, посадовій особі, підрозділі та регіоні	1 раз на тиждень

Продовження таблиці 2.4

Дії	Регулярність
Знання та навички, які мають відношення до персональної поведінки працівника та загальної гігієни безпеки, і їх можна застосувати	1 раз на тиждень

Індивідуальна програма для інформаційно – телекомунікаційного підприємства має посприяти підвищенню обізнаності персоналу з питань інформаційної та кібербезпеки.

Нижче запропоновано розроблений приклад шаблонної політики, що регулює захист комп'ютерних систем і активів. Цей документ містить базову основу для широких тем для розгляду. Виноски містять підказки для інших загальних міркувань і питань для обговорення. Кожна організація має унікальні ризики та міркування, які обов'язково вимагають адаптації.

Приклад політики навчання з питань кібербезпеки

Призначення:

Метою цієї політики є визначення програми навчання з питань інформаційної та кібербезпеки на підприємстві та встановлення мінімальних вимог до програми.

Застосування:

Ця політика поширюється на працівників усіх рівнів, членів правління, консультантів, підрядників, тимчасового персоналу, третіх осіб тощо та до тих, хто має доступ до мережі інформаційно-телекомунікаційного підприємства.

Область застосування:

Ми розуміємо, що для успішної програми навчання з питань інформаційної та кібербезпеки необхідно навчити всіх осіб, які

використовують комп'ютерні інформаційні ресурси та обробляють конфіденційну інформацію, а саме, як захищати цю інформацію та що від них очікується.

Політика:

У цьому документі описано програму навчання з питань інформаційної та кібербезпеки, необхідну для співробітників, користувачів і, за необхідності, зовнішніх підрядників, консультантів, продавців, постачальників тощо для підтримки наших політик і процедур інформаційної безпеки.

Програма навчання з питань інформаційної та кібербезпеки може включати різні типи навчання, як брифінги для нових співробітників, брифінги з питань безпеки, нагадування про безпеку, електронні листи, загальні тренінги з безпеки, тренінги з безпеки для конкретних програм і тренінги з безпеки для роботи.

Види програми навчання з питань інформаційної та кібербезпеки:

- Загальні тренінги з питань безпеки будуть надаватися як частина орієнтації для нових співробітників і для наявних співробітників на періодичній основі. Наприкінці навчання працівник підписує підтвердження про його проходження.

- Особистий брифінг, який проводить відділ кадрів і стосується політики та процедур інформаційної безпеки. Інші засоби можуть використовуватися, але не обмежуючись цим, веб-навчання, онлайн-курси, вебінари, навчання, що надається третіми особами тощо. Для непрацівників, таких як підрядники, консультанти та треті сторони, політика безпеки може бути встановлена контрактом.

- Тренінги, що проводяться співробітниками відділу кадрів з безпеки для певного програмного забезпечення або веб-додатку. У ньому наголошується на типах конфіденційної інформації, до якої здійснюється доступ і яка обробляється в певній програмі, а також на важливих функціях

контролю доступу для захисту та обробки конфіденційної інформації підприємства, яка міститься в програмі.

- Спеціальне навчання безпеки для працівників, які мають доступ до конфіденційної інформації підприємства.

- Навчання з безпеки реагування на інформацію для фахівців з інформаційних технологій для спеціалістів з інформаційних технологій, щоб знати, як реагувати на можливий інцидент або запобігати перетворенню загрози в інцидент. Цей тренінг допомагає зменшити ризик завдяки відповідній підготовці осіб, які першими реагують.

- Навчання з безпеки в Інтернеті (наприклад, відео з питань безпеки та брифінги/презентації з безпеки в Інтернеті) може бути використано для підвищення обізнаності щодо безпеки щодо обробки, передачі та зберігання конфіденційної інформації, включаючи підрядників, консультантів і сторонніх третіх осіб.

- Регулярна відправка нагадувань про безпеку, такі як електронні листи, інформаційні бюлетені, статті, публікації.

- Інструктажі з питань безпеки для всього персоналу проводитимуться щонайменше раз на рік.

Загальні елементи програми навчання з питань інформаційної та кібербезпеки:

- Усі працівники, члени правління, підрядники або треті сторони, які мають доступ до конфіденційної інформації підприємства, повинні ознайомитися з короткою інформацією про політику інформаційної безпеки. Короткий виклад політики інформаційної безпеки, якщо це можливо, буде надано представником IT відділу.

- Програма включає навчання з прийнятного використання щодо обробки, передачі, зберігання та захисту конфіденційної інформації підприємства.

- Програма включає фізичну політику безпеки та процедури.

- Програма включає загальні тренінги з інформаційної безпеки, такі як процедури входу/виходу з системи, як ініціювати заблоковану екранну заставку, керування паролями та інші процедури для захисту від шкідливого програмного забезпечення чи загроз.

- Програма включає, як розпізнавати потенційний інцидент із безпекою або загрозу мережі підприємства та повідомляти про них.

- Програма надає оновлення щодо нововведень або змін у політиках і процедурах безпеки.

Плани навчальних курсів

Нижче наведено елементи, які можна використовувати для формування плану курсу для кожного типу навчання:

- Мета

- Область застосування

- Учасники навчання (наприклад, співробітники, оператори, керівники та треті сторони)

- Підхід (тобто навчити тренера або навчити кінцевих користувачів)

- Методологія (тобто особиста, веб-інтерфейс, аудіо, самонавчання)

- Результати (наприклад, план навчання, посібник інструктора, відеодоріжка, PowerPoint)

- Цілі навчання

- Розклад

- Сертифікація або підтвердження

- Перегляд та оцінка курсу

Навчальну документацію з комп'ютерної безпеки слід підтримувати за допомогою сертифікатів про навчання або списків відвідувачів.

Відповідальність

Порушення цієї політики може призвести до призупинення або скасування системних привілеїв та/або дисциплінарних стягнень, аж до звільнення. Підприємство залишає за собою право повідомляти відповідні органи про будь-які порушення закону.

Відповідальність

Інформаційна безпека несе відповідальність за координацію з відділом інформаційних технологій і відділом людських ресурсів, щоб забезпечити наявність відповідних навчальних матеріалів і регулярне планування навчання.

Відділ інформаційних технологій і людських ресурсів відповідає за те, щоб підтвердження користувача було підписано перед наданням доступу до мережі підприємства.

Інформаційні технології відповідають за забезпечення дотримання цієї політики та засобів контролю, створених для захисту мережі підприємства. Усі порушення цієї політики будуть задокументовані та повідомлені керівнику відділу та вищому керівництву для перевірки та вжиття відповідних заходів.

Винятки

Будь-які оновлення, зміни або винятки з цієї політики повинні бути схвалені вищим керівництвом.

На основі політики було розроблено програму підвищення обізнаності персоналу у інформацій та кібербезпеці. У таблиці 2.5 наведений план програми підвищення обізнаності персоналу на інформаційно-телекомунікаційному підприємстві.

Таблиця 2.5 – План програми підвищення обізнаності персоналу на інформаційно-телекомунікаційному підприємстві.

Тема	Навчальні заходи	Тривалість	Співробітники
Необхідність дотримання правил ІБ	- Лекція на тему: «Роль співробітників у забезпеченні ІБ підприємства» - Лекція на тему: «Відповідальність співробітників за порушення правил ІБ»	3 дні	Весь персонал

Продовження таблиці 2.5

Тема	Навчальні заходи	Тривалість	Співробітники
Плавила безпечної роботи з конфіденційною інформацією	- Лекція на тему: «Класифікація інформації у інформаційно-телекомунікаційному підприємстві» - Тренінг на тему «Принцип «володар інформації»» - Лекція на тему: «Процедури по поводженню з інформацією обмеженого доступу» - Тренінг на тему: «Політика «Чистого столу», збереження документів і інформації за межами підприємства»	5 днів	Весь персонал
Правила роботи з ПК	- Тренінг на тему: «Ім'я користувача та пароль. Відповідальність за дії» - Лекція на тему: «Використання корпоративних інформаційних ресурсів у персональних цілях» - Лекція на тему: «Використання мережевих інформаційних ресурсів»	3 дні	Весь персонал
Парольна політика	- Тренінг на тему: «Використання паролів (створення, частота заміни, складність та безпека, способи збереження та передачі 3-им особам)» - Відеолекція на тему «Критерії стійкості паролю»	3 дні	Весь персонал

Продовження таблиці 2.5

Тема	Навчальні заходи	Тривалість	Співробітники
Правила роботи з корпоративною електронною поштою	- Відеолекція на тему: «Зовнішні повідомлення – адресація, шифрування, сповіщення» - Практичні заняття на тему: «Архівування поштової скриньки» - Відеолекція на тему: «Система запобікання витоку конфіденційної інформації» - Відеолекція на тему: «Підпис і перевірка підпису під повідомленнями»	3 дні	Весь персонал
Антивірусна політика	- Відеолекція на тему: «Антивірусне ПЗ» - Практичні заняття на тему: «Дії співробітників у разі вірусного зараження» - Тренінг на тему: «Небезпека відкриття файлів-вкладень, отриманих від невідомих адресатів»	3 дні	Весь персонал
Правила роботи у мережі Інтернет	- Лекція на тему: «Розміщення інформації у мережі Інтернет» - Лекція на тему: «Нецільове використання ресурсов мережі Інтернет» - Тренінг на тему: «Шахрайство з використанням мережі Інтернет» - Семінар на тему: «Види шахрайства, які зустрічаються у мережі Інтернет – фішинг, соціальна інженерія, викрадення паролів»	3 дні	Весь персонал

Продовження таблиці 2.5

Тема	Навчальні заходи	Тривалість	Співробітники
Інциденти ІБ	- Тренінг на тему: «Куди необхідно звертатись у разі інцидентів ІБ» - Практичні заняття на тему: «Дії у нештатних ситуаціях»	3 дні	Весь персонал
Протидія шахрайству	- Відеолекція на тему: «Основні канали використання шахрайства» - Практичні заняття на тему: «Дії, у разі підозри на шахрайство»	3 дні	Весь персонал
Використання конкретних програм підприємства	- Тренінг на тему: «Використання корпоративної платформи Microsoft Teams» - Тренінг на тему: «Використання корпоративної платформи Microsoft Outlook» - Тренінг на тему: «Використання програми Microsoft Excel»	3 дні	Весь персонал
Введення у програму ІБ підприємства	- Брифінг на тему: «Що таке ІБ» - Брифінг на тему: «Протидія шахрайству на підприємстві»	1 день	Нові співробітники

Після кожної теми, описаної у таблиці 2.5, персонал підприємства повинен проходити обов'язкові тестування. У кінці всього навчання буде загальний тест на перевірку знань, здобутих у процесі навчання.

Програма підвищення обізнаності персоналу в питаннях по інформаційній та кібербезпеці на інформаційно-телекомунікаційному

підприємстві проводиться в 9 етапів. Кожен етап займає різну тривалість часу, загальний обсяг часу на програму – 34 дні.

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 оскільки, дана програма впроваджується протягом робочого дня, то співробітникам ще потрібно виконувати свої прямі обов'язки, тобто 34 дні це "золота середина" для програми підвищення рівня обізнаності персоналу.

Також, у програму буде введено наступне:

- Імітація фішингових атак на підприємтво, за використання електронної пошти працівників, щоб отримати відсоток працівників, які клікнуть на шкідливе посилання. Приклад попереджувального листа про введення програми та можливі фішингові атаки наведено на рис 2.4 Після змодельованої фішингової атаки, співробітники отримають лист зі статистикою переходу за шкідливим посиланням та будуть запрошені до навчання. На рис 2.5 наведений приклад даного листа.

Як ви всі знаєте, підвищення обізнаності про інформаційну та кібербезпеку важливо для безпеки нашого підприємства.

Я рада повідомити, що ми співпрацюємо з компанією LeviSave - провідна у світі організація по навчанню підвищення обізнаності персоналу про інформаційну та кібербезпеку на підприємстві. Їх сучасна платформа включає в себе навчання по питанням безпеки і симуляцію фішингових атак, які допоможуть нам створити "людський брандмауер", за допомогою навчання наших співробітників тому, як виявити і повідомити про шкідливі електронні листи.

Ми почнемо з відправки змодельованого фішингового електронного листа, щоб визначити на скільки вірогідно, що наші працівники попадуть під фішингову атаку. Потім я заплануюю (для всього підприємства) навчання і раз на 2 тижні фішингові тести для всіх працівників. Потім ми розповімо нашим співробітникам про найкращий метод повідомлення про ці змодельовані фішингові листи.

Наступним кроком, ми призначимо нашим працівникам тренінг по підвищенню обізнаності про інформаційну та кібербезпеку. Для початку всі пройдуть 45-хвилинний курс загальної безпеки. Окремим відділам також потрібно буде пройти окремі курси в залежності від їх посадових обов'язків. Навчання захоплююче і не потребує завершення за один раз.

Наша кінцева ціль - підвищити обізнаність про інформаційну та кібербезпеку та зменшити кількість кліків по шкідливим електронним листам.

Я рада, що ця нова програма підвищення обізнаності про інформаційну та кібербезпеку була у рамках програми безпеки, і я приймаю будь-які питання або проблеми.

Дякую,
Ольга Левітан

Рисунок 2.4 – Попереджувальний листи про введення програми та можливі фішингові атаки

Можливо, ви знаєте, що нещодавно ми провели симуляцію тесту на фішинг. Метою цього тесту було визначити, як наша організація відреагує на справжню фішингову атаку. Відсоток користувачів, які натиснули посилання в цій імітованій атаці, становив [XX] відсотків.

Фішинг — це різновид кіберзлочинності, коли хакери намагаються отримати доступ до вашої особистої інформації, такої як імена користувачів і паролі. Щоб допомогти боротися зі зростанням кіберзлочинності, наприклад фішингових атак, ми вирішили співпрацювати з LeviSave. Усі співробітники пройдуть навчання LeviSave з питань безпеки.

Ви отримаєте електронний лист із запрошенням пройти навчання LeviSave з питань безпеки. Ми також продовжуватимемо надсилати змодельовані фішингові тести, щоб ви могли практикувати навички, які ви отримаєте під час навчання. Слідкуйте за такими електронними листами у своїй папці "Вхідні".

Ми покладаємося на вас як на останню лінію захисту від кіберзлочинності.

Дякую,
Ольга Левітан

Рисунок 2.5 – Лист зі статистикою переходу за шкідливим посиланням та запрошення до навчання.

- Інформаційні бюлетені, які будуть розміщені по всьому периметру підприємства (ліфти, кабінети, робочі місяця). Приклади банерів наведено У ДОДАТКУ Б.

- Банери на екрані блокування ПК співробітників, які будуть нагадувати про важливість обізнаності з приводу інформаційної та кібербезпеки

- Телеграм-канал з важливою інформацією у сфері ІТ, про нові та оновлені загрози та правила боротьби з ними

Проведення програми підвищення обізнаності персоналу здійснюється співробітниками 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. Приклад попередження про імовірну атаку наведено на рис. 2.6

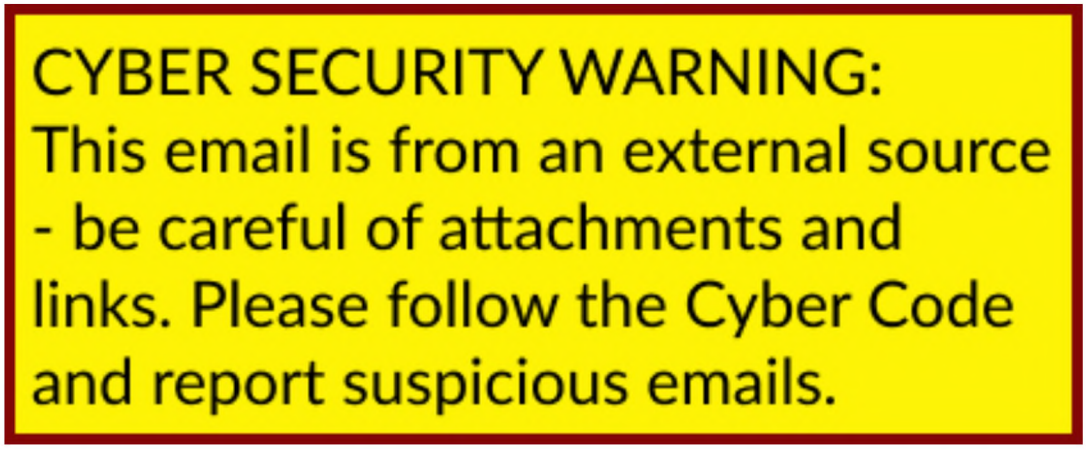


Рисунок 2.6 – Приклад попередження про імовірну атаку.

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

Результати опитування після проходження програми підвищення обізнаності показали наступні:

- розпізнавання масованої фішингової атаки зросло з 17% до 74%;
- розпізнавання цільових електронних листів зросло з 19% до 72%;
- розпізнавання вебшахрайства зросло з 15% до 67%;
- показник співробітників, які можуть загрожувати інформаційній безпеці підприємства знизився від 29% до 8%;
- показник обізнаності персоналу, який пройшов програму зріс від початку програми на 81%.

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.

2.5 Висновок до другого розділу

В другому розділі проводилась розробка програми підвищення обізнаності персоналу з інформаційної та кібербезпеки на інформаційно-телекомунікаційному 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 політики 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. Запропонована програма дозволить систематизувати знання та підходи персоналу у області інформаційної та кібербезпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

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 підвишення обізнаності персоналу та методів і засобів підтримки проінформованості 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:

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

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

$t_{в}$-тривалість вивчення ТЗ, літературних джерел за темою тощо, год,

$t_{пр}$- тривалість розробки програми та засобів програми, год;

$t_{д}$- тривалість документування та оформлення результатів, год.

$$t=27\text{год} +77\text{год} +160\text{год} +160\text{год}=424\text{год}$$

Витрати на розробку програми підвищення обізнаності персоналу на промисловому підприємстві $К_{пз}$ 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 $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} \quad (3.2)$$

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

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

де t – загальна тривалість розробки програми підвищення обізнаності персоналу на інформаційно-телекомунікаційному підприємстві, год;

Зіб – середньогодинна заробітна плата спеціаліста з ІБ з нарахуваннями грн/год.

$$З_{зп} = 425*210 = 89250 \text{ грн}$$

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 1години машинного часу ПІК, грн/год.

Вартість 1години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = Р * t_{нал} * С_е + (Ф_{зал} * \frac{На}{Fp}) + (К_{ліз} * \frac{Напз}{Fр}), \text{ грн} \quad (3.5)$$

де Р- 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;

$Н_а$ - річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ - річна норма амортизації на ліцензійне ПЗ, частки одиниці;

$К_{ліз}$ - вартість ліцензійного ПЗ, грн;

$Е_р$ -річний фонд робочого часу (за 40-годинного робочого тижня Fр=1920).

На промислових підприємствах середня потужність дорівнює Р = 0,4, а тариф на електричну енергію становить 5,64 грн/кВт*год, отже:

$$С_{мч} = 0.4 * 1 * 5.64 + (12700 * \frac{0.5}{1920}) + (4370 * \frac{0.4}{1920}) = 6{,}48 \text{ грн}$$

$$З_{мч} = t_{пр} * С_{мч} + t_д = 160 * 6.48 + 160 = 1196{,}80 \text{ грн}$$

$$К_{пр} = З_{зп} + З_{мч} = 89250 + 1196{,}80 = 90446{,}80 \text{ грн}$$

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 3000 грн (програма WordPress);

$К_{рп}$ - вартість розробки програми підвищення обізнаності складає 35 500 грн;

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

$К_{дм}$ - вартість допоміжних матеріалів: 4 плакати (200грн/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.

$$К = 90446,8 + 3000 + 35500 + 800 = 129\ 746,80 \text{ грн}$$

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

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

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

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

$С_{к}$ - витрати на керування 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 ($С_а$):

$$С_а = \frac{15*27\ 500}{5} + \frac{60\ 000}{10} = 88\ 500 \text{ грн}$$

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 – 23 000 грн, додаткова заробітна плата -25% від основної зарплати:

$$С_з = 23\ 000 * 12 + 23\ 000 * 12 * 0.25 = 345\ 000 \text{ грн}$$

Ставка ЄСВ для всіх категорій платників складає 22%:

$$С_{єв} = 345\ 000 * 0{,}22 = 75\ 900 \text{ грн}$$

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

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

де Р- встановлена потужність ПК, кВт;

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

$F_р$- річний фонд робочого часу.

$$С_{ел} = 1 * 1920 * 5{,}64 = 10\ 828{,}80 \text{ грн}$$

Витрати на технічне й організаційне адміністрування програми визначаються в відсотках від капітальних витрат - 2% ($С_{тос}$ = 129 746,80 * 0,02 = 2594,90 грн).

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

$С_к$ = 37 900 + 88 500 + 345 000 + 75 900 + 10 828,80 + 2594,90 = 560 723,70

Таким чином, річні поточні витрати складають:

С= 25 000 + 560 723,7= 585 723,7 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:

$$E = B * R – C, \quad (3.11)$$

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:

$$B = \Sigma_i \Sigma_n U, \text{ грн}, \quad (3.12)$$

де І - 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:

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

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 намісяць;

$t_п$ - час простою мережі підприємства внаслідок атаки, год.

Витрати на відновлення працездатності мережі підприємства включають:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.15)$$

де $П_{ви}$ - витрати на повторне уведення інформації, грн;

$П_{пв}$ - витрати на відновлення мережі підприємства, грн,

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації розраховуються:

$$П_{ви} = \frac{ЗЗс}{F} * t_{ви}, \quad (3.16)$$

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

Витрати на відновлення мережі підприємства визначаються:

$$П_{пв} = \frac{ЗЗо}{F} * t_{в}, \quad (3.17)$$

де $t_в$ - час відновлення після атаки персоналом, що обслуговує мережу підприємства, год,

$З_о$ - заробітна плата обслуговуючого персоналу, грн на місяць.

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

$$V = \frac{О}{Fг} * (t_в + t_п + t_{ви}), \quad (3.18)$$

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

$F_г$ - річний фонд часу роботи підприємства становить 2080 ч.

Визначення річного економічного ефекту:

$$V = \frac{9\,190\,900}{2080} * (6 + 2 + 4) = 53\,024 \text{ грн}$$

$$П_{пв} = \frac{370\,300}{176} * 6 = 12\,623{,}90 \text{ грн}$$

$$П_{ви} = \frac{270\,500}{176} * 4 = 6\,147{,}70 \text{ грн}$$

$$П_в = 12\,623{,}9 + 6\,147{,}7 = 18\,771{,}60 \text{ грн}$$

$$П_п = \frac{270\,500}{176} * 2 = 3\,073{,}90 \text{ грн}$$

$$U = 18\,771{,}6 + 3\,073{,}9 + 53\,024 = 74\,869{,}50 \text{ грн}$$

$$B = \Sigma_2\, \Sigma_{14}\, 74\,869{,}5 = 2 * 14 * 74\,869{,}5 = 2\,096\,346 \text{ грн}$$

$$E = 2\,096\,346 * 0.35 - 585\,723{,}7 = 204\,997{,}40 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованого в кваліфікаційній роботі проектного 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.

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

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

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

$$\text{ROSI} = \frac{E}{K} = \frac{204\,997{,}4}{129\,746{,}8} = 1{,}60$$

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

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років} \qquad (3.20)$$

$$T_o = \frac{К}{Е} = \frac{129\,746{,}80}{204\,997{,}40} = 0.6 \text{ рока (7 місяців)}$$

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 інформаційно-телекомунікаційному 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 та означає, що на 1 грн. капітальних витрат приходиться 1,60 грн. економічного ефекту. Період окупності при цьому складе 7 місяців. Капітальні витрати складають 129 746,80 грн, а експлуатаційні 585 723,70 грн.

ВИСНОВКИ

У першому розділі було проведено аналіз загроз, як окремому користувачу, так і на інформаційну-комунікаційній системі в цілому. Встановлено, що основною загрозою інформаційній безпеці підприємства є людина, як співробітник компанії (інсайдер), так і зовнішні зловмисники. Їхні цілі можуть бути подібні, але методи виконання відрізняються через доступність конкретних інструментів, що допомагають досягти поставлених завдань. Також проведено дослідження різних видів зовнішніх і внутрішніх загроз, які можуть виникнути в результаті дій людини і спричинити шкоду діяльності підприємства. Далі детально розглянуто методи та засоби підвищення рівня обізнаності персоналу на підприємстві, з урахуванням ефективності кожного з них. Визначено, що обізнаність в інформаційній безпеці в значній мірі залежить від індивідуальних знань людини. Освіченість щодо методів зловмисників та їхніх тактик може значно зменшити ризик атаки на підприємство або самого співробітника.

В другому розділі проводилась розробка програми підвищення обізнаності персоналу з інформаційної та кібербезпеки на інформаційно-телекомунікаційному 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 політики 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. Запропонована програма дозволить систематизувати знання та підходи персоналу у області інформаційної та кібербезпеки.

У третьому розділі, в результаті розрахованих витрат на розробку та впровадження програми обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою на інформаційно-телекомунікаційному

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 та означає, що на 1 грн. капітальних витрат приходиться 1,60 грн. економічного ефекту. Період окупності при цьому складе 7 місяців. Капітальні витрати складають 129 746,80 грн, а експлуатаційні 585 723,70 грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кіберзлочинність: виклики часу [Електронний ресурс]. - 2023- Режим доступу до ресурсу: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/

2. Інформаційна та кібербезпека: чому це важливо для бізнесу [Електронний ресурс]. - 2023- Режим доступу до ресурсу: https://www.softline.kiev.ua/news/informatsiina-ta-kiberbezpeka-chomu-tse-vazhlyvo-dlia-biznesu.html

3. HM Government, "Технічний звіт" 2015.

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

5. Офіційний сайт ISACA. COBIT [Електроний ресурс]. – Режим доступу https://www.isaca.org/resources/cobit/

6. Information technology. Security techniques. Information management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/64120.html

7. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - No22 - (Нормативний документ системи технічного захисту інформації).

8. Что такое политика информационной безопасности предприятия? [Електронний ресурс]. Режим доступу «http://www.infobezpeka.com/publications/?id=393»

9. NIST SP 800-501 [Електронний ресурс]. - 2003. -Режим доступу до ресурсу:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf.

10. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17 с.

11. 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.

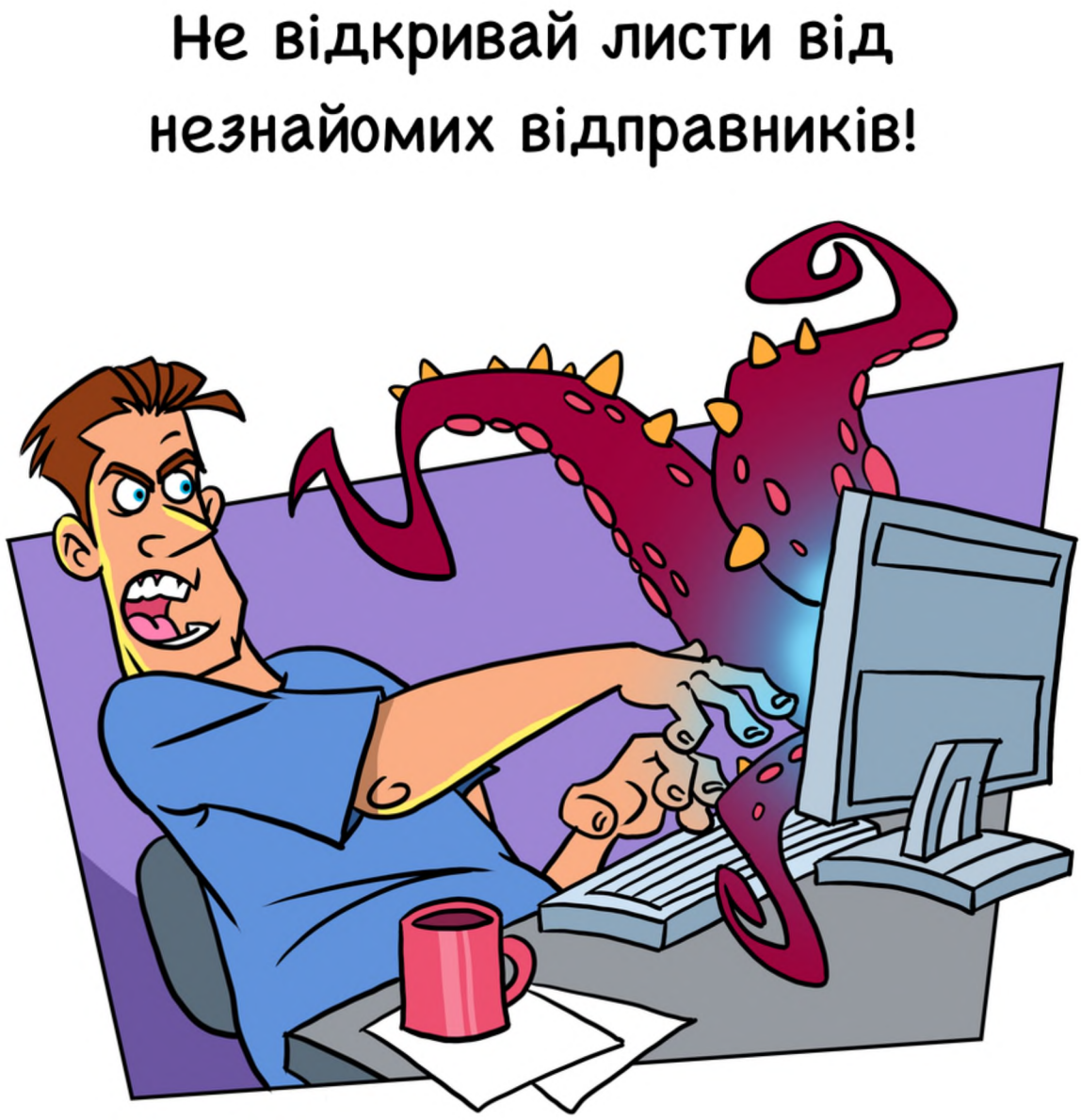
12. МЕТОДЫ ОБУЧЕНИЯ ПЕРСОНАЛА ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [Електронний ресурс]. Режим доступу: https://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf

13. Курсы кибергигиены: основа информационной безопасности компании [Електронний ресурс]. Режим доступу: https://securitymedia.org/info/kursy-kibergigieny-osnova-informatsionnoy-bezopasnosti-kompanii.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	11	
5	А4	2 Розділ	38	
6	А4	3 Розділ	10	
7	А4	Висновки	2	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	4	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	

ДОДАТОК Б. Приклади банерів, які будуть розміщені по всьому периметру підприємства (ліфти, кабінети, робочі місяця).




Негайно
повідомляй про
проблеми безпеки

Поради з інформаційної безпеки

1. Використовуй складні паролі
2. Створюй резервні копії важливої інформації
3. Використовуй антивіруси
4. Не тримай комп'ютер включеним, коли ти ним не користуєшся
5. Не відкривай листи від незнайомих відправників


Май імунітет до всіх вірусів
GET WELL
GET WELL SOON

ДОДАТОК В. Перелік матеріалів на оптичному носії

Левітан_О.С._125м-22-2.docx

Левітан_О.С._125м-22-2.pptx

Левітан_О.С._125м-22-2.pdf

ДОДАТОК Г. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 95 б. («відмінно»).

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

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студентки групи 125м-22-2 Левітан Ольги Сергіївни на тему: «Розробка програми підвищення обізнаності персоналу в процесі впровадження системи управління інформаційною безпекою»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 81 сторінці.

Метою кваліфікаційної роботи є мінімізація інформаційних ризиків, пов'язаних з персоналом

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз джерел загроз інформаційної та кібербезпеки на підприємстві, а також методів та засобів підвищення обізнаності персоналу в питаннях, пов'язаних з інформаційною та кібербезпекою

Розроблені політика та програма для підвищення обізнаності персоналу на інформаційно-телекомунікаційному підприємстві

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні обізнаності персоналу, за рахунок розробки спеціальної програми.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Левітан О.С. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

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

Кваліфікаційна робота заслуговує оцінки «90»(відмінно).

Керівник роботи _____ _____

(підпис) (ініціали, прізвище)