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 *Тітова Дмитра Сергійовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення рівня обізнаності співробітників підприємства з питань кібербезпеки з використанням методів гейміфікації*

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

Рецензент				

Нормоконтролер	ст.в. Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Тітову Дмитру Сергійовичу* **академічної групи** *125м-20-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення рівня обізнаності співробітників підприємства з питань кібербезпеки з використанням методів гейміфікації*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 №1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Дослідження теоретичної бази у сфері обізнаності персоналу в питаннях інформаційної та кібербезпеки.	03.11.2021
Розділ 2	Аналіз рекомендацій щодо створення та підтримки комплексної програми підвищення обізнаності та навчання у рамках програми IT-безпеки організації.	20.11.2021
Розділ 3	Розробка та застосування програми підвищення обізнаності персоналу на прикладі підприємства.	14.12.2021
Розділ 4	Визначення економічної доцільності впровадження програми навчання, розрахунки витрат та ефекту від впровадження програми.	28.12.2021

Завдання видано _____ Тимофєєв Д.С.
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: _01.09.2021_____

Дата подання до екзаменаційної комісії: ____18.01.2022_____

Прийнято до виконання _____ Тітов Д. С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 72 с., 8 рис., 11 табл., 2 додатки, 18 джерел.

Об'єкт дослідження: процес підвищення обізнаності персоналу з питань кібербезпеки.

Предмет дослідження: методи гейміфікації в формуванні обізнаності персоналу з питань кібербезпеки.

Мета кваліфікаційної роботи: формування достатнього рівня обізнаності персоналу з питань кібербезпеки з застосуванням методів гейміфікації.

У першому розділі було досліджено теоретичну базу у сфері обізнаності персоналу в питаннях інформаційної та кібербезпеки. З методів підвищення обізнаності персоналу було виділено метод гейміфікації. Проаналізовні загрози кібербезпеки повязані з персоналом.

У другому розділі представлені рекомендації щодо створення та підтримки комплексної програми підвищення обізнаності та навчання у рамках програми IT-безпеки організації, починаючи від проектування, розробки та реалізації програми підвищення обізнаності та навчання до оцінки програми після впровадження.

В третьому розділі була розроблена та застосована програма підвищення обізнаності персоналу на прикладі підприємства.

В економічному розділі визначено економічну доцільність впровадження програми підвищення обізнаності персоналу. Проведено розрахунки капітальних витрат, поточних витрат, розраховано вірогідность реалізації загроз до та після підвищення обізнаності.

Наукова новизна роботи полягає у розробці програми підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки із застосуванням методів гейміфікації.

ПРОГРАМА ПІДВЩЕННЯ ОБІЗНАНОСТІ, ПОЛІТИКА БЕЗПЕКИ, ОБІЗНАНІСТЬ ПЕРСОНАЛУ, МОДЕЛЬ ЗАГРОЗ, ГЕЙМІФІКАЦІЯ.

ABSTRACT

Explanatory Note 72 p., 8 pictures., 11 tab., 2 applications., 18 sources.

Object of development: cybersecurity awareness raising program

Subject of research: methods of gamification in the formation of staff awareness of cybersecurity.

The purpose of the qualification work: formation of a sufficient level of awareness of staff on cybersecurity with the use of gamification methods.

The first section explored the theoretical basis in the field of staff awareness in information and cybersecurity. The method of gamification was singled out from the methods of raising staff awareness. Analytical threats to cybersecurity are related to personnel.

The second section provides recommendations for creating and maintaining a comprehensive awareness-raising and training program within the organization's IT security program, from designing, developing, and implementing an awareness-raising and training program to evaluating the program after implementation.

In the third section, a program to raise staff awareness was developed and implemented on the example of the company.

The economic section identifies the economic feasibility of implementing a staff awareness program. Calculations of capital expenditures, current expenditures were made, the probability of realization of threats before and after awareness raising was calculated.

The scientific novelty of the work is to develop a program to raise awareness of staff on information and cybersecurity using gamification methods.

AWARENESS RAISING PROGRAM, SECURITY POLICY, STAFF AWARENESS, THREAT MODEL, GAMIFICATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ТОВ – товариство з обмеженою відповідальністю;

ІТ – інформаційні технології;

ІКТ– інфомаційно-комунікаційні тхнології;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ЕОМ – електронно-обчислювальна машина

NIST – national institute of standards and technjlogy;

ISO – international organization for standartization.

Зміст

ВСТУП

Одним із нагальних питань в роботі будь-якої сучасної компанії є підвищення обізнаності персоналу у питаннях інформаційної безпеки. Хоча багато роботодавців стверджують, що вони запровадили ефективну політику, яка допомагає працівникам керувати кіберзагрозами, реальність малює іншу картину, і деякі дослідження показують, що цілих дві третини кібер-порушень спричинені недбалістю чи злочинністю працівників. Як цитується в аудиторських звітах, періодичних виданнях та презентаціях конференцій, спеціалістами в області IT, люди є однією з найслабших ланок у спробах захисту системи та мереж. «Людський фактор», а не технології, є ключовим для забезпечення адекватного та відповідного рівня безпеки. Якщо люди є ключовими, але вони також є слабкою ланкою, слід приділяти більшої і кращої уваги до цього "активу". Надійна та всеосяжна програма обізнаності та навчання є найважливішою для забезпечення людей розумінням своїх обов'язків щодо захисту IT, організаційних політик та те, як правильно їх використовувати та захистити довірені їм IT -ресурси. Метою роботи є розробка ефективної програми підвищення рівня обізнаності у питаннях інформаційної та кібербезпеки.

У роботі поставлені наступні завдання:

- дослідження існуючих методів підвищення обізнаності персоналу;
- розробка програми підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки із застосуванням методів гейміфікації;
- визначення капітальних та експлуатаційних витрат на реалізацію запропонованої програми підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки.

Об'єктом досліджень є процес управління обізнаністю персоналу.

Предметом досліджень є рівень персоналу у питаннях інформаційної та кібербезпеки.

Наукова новизна роботи полягає у розробці програми підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки із застосуванням методів гейміфікації.

РОЗДІЛ 1. СТАН ПИТАННЯ ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз поточного стану кібербезпеки

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що інтернет, цифрові послуги, інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами. Зі зростанням залежності від використання ІКТ у бізнесі і підприємництві відповідно зростають кіберризики і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення та обізнаності з факторами ризику всіх зацікавлених сторін. Сьогодні ми живемо в епоху інформаційного суспільства, що охоплює усі сфери життєдіяльності як людини, так і держави в цілому. Проте, з прогресом комп'ютерних технологій, приходять разом з ними і проблеми, що наразі, становлять чи не найбільшу загрозу для людства. Кіберзброя — одна з найбільш небезпечних інновацій суспільства, що здатна уразити комунікаційні системи всіх форм власності. Сьогодні майже всі фахівці у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. Організована злочинність дедалі частіше використовує Інтернет з метою приховання своєї діяльності. За даними, наданими Національною поліцією України[1], кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилась на 36 %.

У Законі України "Про основні засади забезпечення кібербезпеки України"[2] кібербезпеку визначено як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі. Водночас кіберзахист – це сукупність організаційних,

правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем, тоді як кіберзлочин (комп'ютерний злочин) – суспільно небезпечне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Найпоширеніші види кіберзлочинів:

- кардинг – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки. У будь-якому разі основною метою злочинців є отримання доступу до чужих грошових коштів. Для досягнення цієї мети зловмисники вигадують різноманітні способи отримання потрібної інформації в неуважних і легковірних співробітників. Одним із таких способів є фішинг;

- фішинг – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію;

Фішинг буває кількох видів:

- смс-фішинг, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку. Варіацій СМС-повідомлень безліч, тому потрібно бути особливо уважними й обачними, якщо ви отримуєте повідомлення;

- інтернет-фішинг, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів

тощо. На жаль, не всі уважно перевіряють назву сайта, уводячи дані кредитної картки, що на руку кібершахраям;

- Вішинг – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків (шахраї часто представляються працівниками банку й намагаються вивідати у власника картки ПІН-код чи примусити здійснити якісь дії зі своїм рахунком) ;

- шкідливе ПЗ – створення та поширення вірусів і шкідливого програмного забезпечення;

- соціальна інженерія - метод отримання необхідного до інформації, засноваий на особливості психології людини. Основна ціль соціальної інженерії отримання доступу до конфіденційної інформації, паролів, банківскім даним і іншим захищеним системам;

- викрадення паролів, слабкі паролі - оди н з найлегших способі потрапити у сисетму - через слабкі та ненадійні паролі.

Більшість цих загроз посилилося через можливості, що виникли під час спалаху COVID-19.

Активне переведення співробітників на віддалену роботу та виведення внутрішніх сервісів компаній на мережевий периметр, зумовлені пандемією COVID-19, вплинули на ландшафт кіберзагроз у всьому світі. Лише деякі компанії, які й так практикували роботу в режимі «віддалення», були готові впоратися з усіма складнощами у забезпеченні безпеки, решта зіткнулася з нестачею часу на продумування та реалізацію всіх необхідних заходів захисту.

Одна з причин сплеску кібератак може бути пов'язана з тим, що деякі малі та середні підприємства використовують підхід BYOD на відміну від підходу COPE. Що означає, що працівники можуть використовувати особисті пристрої (телефони, планшети або ноутбуки) для доступу до корпоративної інформації. Робота з дому не гарантує того ж рівня кібербезпеки, що й офісне середовище. При використанні персонального комп'ютера або ноутбука для доступу до корпоративних файлів та даних користувачі більш схильні до кібератак. Наприклад, співробітники можуть не запускати антивірусне сканування або

сканування на наявність шкідливих програм регулярно або взагалі не запускати його. Домашнє робоче середовище не має складних заходів запобігання та виявлення як на підприємстві. Крім того, домашні мережі Wi-Fi набагато простіше атакувати.

Людська помилка - ще одна проблема, що викликає занепокоєння. До пандемії людський фактор уже був однією з основних причин «кібербезпеки»: співробітники неусвідомлено або необережно відкривали доступ не тим людям. Однак із роботою вдома проблема стала ще більшою. Коли вони працюють з дому, співробітники можуть відволікатися від роботи членами сім'ї або відвідувачами. Ці фактори, що відволікають, можуть зробити людей більш безтурботними.

Схоже, що багато хакерів покращують свої методи і, щоб отримати вигоду з нового переходу компаній до віддаленої роботи, вони розробили нові шкідливі ПЗ для атак і проникнення в системи. На основі обширних даних, зібраних між клієнтами Cynet[3] було визначено, що до пандемії близько 20% кібератак використовували раніше невідомі шкідливі програми чи методи. У час пандемії ця частка зросла до 35%. Деякі з нових атак використовують форму машинного навчання, яка адаптується до свого середовища та залишається непоміченою. Наприклад, атаки фішингу стають все більш витонченими і використовують різні канали, такі як SMS і голос (вішинг). Більш того, новини про розробки вакцин використовуються для фішингових кампаній. Атаки програм-вимагачів також стають дедалі досконалішими. Наприклад, хакери об'єднують атаки по витоку даних із програмами-вимагачами, щоб переконати жертв заплатити викуп.

Це зростання кібератак потребує нових "передових" механізмів виявлення для протидії загрозі, таких як "аналіз поведінки користувачів та сутностей". Це аналізує нормальну поведінку користувачів та застосовує ці знання для виявлення випадків аномальних відхилень від нормальних шаблонів.

Пандемія коронавірусу створила нові проблеми для підприємств, оскільки вони адаптуються до операційної моделі, де робота вдома стала «новою нормою». Компанії прискорюють цифрову трансформацію і тепер кібербезпека є серйозною

проблемою. Якщо не брати до уваги ризики кібербезпеки, це може мати серйозні наслідки для репутації, експлуатації, законодавства та дотримання нормативних вимог.

У червні 2020 року Swissinfo.ch[4] повідомив дані NCSC (Національного центру кібербезпеки), які показують, що у квітні у Швейцарії було зареєстровано 350 випадків кібератак (фішинг, шахрайські веб-сайти, прямі атаки на компанії тощо). У порівнянні з нормою 100–150. Пандемія коронавірусу та зростання кількості працюючих вдома розглядалися як основна причина цього збільшення, оскільки люди, що працюють вдома, не користуються таким самим рівнем невід'ємних заходів захисту з боку робочого середовища (наприклад, інтернет-безпеки).

Збільшення віддаленої роботи вимагає більшої уваги до кібербезпеки через більшу схильність до кіберрисків. Це очевидно, наприклад, через те, що 47% людей потрапляють на фішингову аферу, працюючи вдома. Кібер-зловмисники розглядають пандемію як можливість активізувати свою злочинну діяльність, використовуючи вразливість працівників, що працюють з дому, і отримують вигоду з великого інтересу людей до новин, пов'язаних з коронавірусом (наприклад, шкідливих підроблених веб-сайтів, пов'язаних з коронавірусом). Ще одне важлива міркування полягає в тому, що середня вартість витоку даних в результаті віддаленої роботи може досягати 137 000 доларів. 8 липня поліція Лондону[5] повідомила, що з січня 2020 через шахрайство з COVID-19 було втрачено більше 11 мільйонів фунтів стерлінгів. У Швейцарії кожен сьомий респондент зазнав кібератаки під час пандемії.

Згідно звіту ENISA ETL 2021[6], який охоплює період з квітня 2020 року до липня 2021 року, було виявлено такі основні загрози:

- програми-вимагачі;
- шкідливе ПЗ;
- криптоджекінг;
- загрози, пов'язані з електронною поштою;
- загрози даним;

- загрози доступності та цілісності;

- дезінформація ;

- нешкідливі загрози.

Друга половина 2020 року продемонструвала безпрецедентні зміни ландшафту кіберзагроз: зловмисники максимально збільшують площу атак, щоб масштабувати загрози у всьому світі. Зловмисники виявилися дуже гнучкими, створюючи хвилі руйнівних та витончених атак.

Атаки націлені на велику кількість віддалених співробітників. Такі висновки наведено у новому піврічному дослідженні FortiGuard Labs Global Threat Landscape Report, підготовленому компанією Fortinet.

Крім того, йдеться у звіті, кіберзагрози продемонстрували вражаючу гнучкість у спробах націлюватися на цифрові ланцюжки поставок і навіть базову мережу.

Головне зі звіту FortiGuard Labs Global Threat Landscape за II півріччя 2020 року:

- натиск програм-вимагачів продовжується: дані FortiGuard Labs показують семиразове збільшення загальної активності програм-вимагачів порівняно з першим півріччям 2020 року, причому зростання активності обумовлене кількома тенденціями. Умови для такого інтенсивного зростання створюють такі фактори: розвиток RaaS (програма-вимагач як послуга), наголос на великі викупи за великі цілі та загроза розкриття вкрадених даних у разі невиконання вимог. Крім того, з різною мірою поширеності найбільш активними з відстежуваних типів вимагачів були Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING і BazarLoader. Сектори економіки, які зазнавали серйозних атак програм-здирників, включають охорону здоров'я, сферу послуг, держсектор, фінансові організації. Щоб ефективно боротися зі зростанням ризиків, пов'язаних з цим типом шкідливих даних, необхідно забезпечити своєчасне, повне та безпечне резервне копіювання даних за межами корпоративної мережі. Також, щоб мінімізувати ризик, слід вивчити стратегії доступу з нульовою довірою та сегментації, щоб мінімізувати ризик;

- зловмисники націлені на дії користувачів в Інтернеті: вивчення найпоширеніших категорій шкідливих програм дозволяє виявити найпопулярніші методи, які кіберзлочинці використовують для закріплення своїх позицій в організаціях. Головною метою атак були платформи Microsoft, пов'язані з документами, які більшість людей використовують протягом звичайного робочого дня. Веб-браузери залишалися ще одним фронтом. У цю категорію HTML входили фішингові сайти та скрипти, що містять шкідливі програми, які вводять прихований код або перенаправляють користувачів на шкідливі сайти. Ці типи загроз неминуче зростають під час глобальних проблем або періодів інтенсивної онлайн-торгівлі. Співробітники, які зазвичай користуються послугами веб-фільтрації при перегляді з корпоративної мережі, продовжують залишатися вразливішими, коли роблять це за межами такого захисного фільтра;

- домашній офіс залишається під прицілом: бар'єри між будинком та офісом значно зруйнувалися у 2020 році, а це означає, що націлення на будинок наближає зловмисників на один крок до корпоративної мережі. У другій половині 2020 року експлойти, спрямовані на пристрої Інтернету речей (IoT), такі як ті, що існують у багатьох будинках, були у верхній частині списку найпоширеніших шкідників. Кожен пристрій IoT є новим «кордоном» мережі, який необхідно захищати і моніторити;

- зловмисники виходять на глобальний рівень: групи Advanced Persistent Threat (APT) продовжують у різний спосіб використовувати пандемію COVID-19. Найбільш поширеними серед них були атаки, спрямовані на масовий збір особистої інформації, крадіжку інтелектуальної власності та збір розвідданих, що відповідають національним пріоритетам APT-групи. У міру наближення кінця 2020 року спостерігалося зростання активності APT, націленої на організації, що беруть участь у роботі, пов'язаній з COVID-19, включаючи дослідження вакцин та розробку внутрішньої або міжнародної політики охорони здоров'я щодо пандемії. Цільові організації включали урядові установи, фармацевтичні фірми, університети та медичні дослідницькі фірми;

- згладжування кривої експлойтів уразливостей: патчі та виправлення є постійними пріоритетами для організацій, оскільки кіберзлочинці продовжують спроби використовувати вразливість у своїх інтересах. Дані демонструють, наскільки швидко та наскільки далеко розповсюджуються експлойти (на основі аналізу розвитку 1500 експлойтів за останні два роки). Хоча це не завжди так, схоже, що більшість експлойтів не поширюються дуже швидко. Серед усіх, що відстежуються за останні два роки, лише 5% було виявлено більш ніж у 10% організацій. За інших рівних умов, якщо вразливість обрана випадковим чином, дані показують, що ймовірність того, що організація зазнає атаки, становить приблизно 1 з 1000. Близько 6% експлойтів вразили більше 1% фірм протягом першого місяця, і навіть через рік 91% експлойтів не подолали цей поріг на 1%. Тим не менш, як і раніше, розумно зосередити зусилля з виправлення вразливостей з відомими експлойтами, і серед них віддати пріоритет тим, які найбільш швидко поширюються у вільних умовах.

Згідно з Глобальним дослідженням інформаційної безпеки, яке провела компанія EY[7], кіберзлочинні групи та хакери щодня відправляють понад 6,4 млрд. підроблених електронних листів по всьому світу. Це призводить до щоденної крадіжки персональних даних понад 2 млрд. приватних осіб, а збитки від таких кібердійств оцінюють у $3,5 млрд. на день. За даними Gartner Group[4], боротьба зі зростаючими глобальними кібератаками, як у державному, так і в приватних секторах, викликала зростання ринку кібербезпеки до 100 мільярдів доларів. на рік. Сукупне зростання обсягу закупівлі програмного забезпечення, обладнання та пов'язаних з ними професійних послуг у сфері кібербезпеки становить 12% відповідно до попереднього року (CAGR). І все ж, незважаючи на збільшення інвестицій у кібербезпеку, державний та приватний сектори, не вдається стежити за шахрайством, крадіжками та витоком даних, які викликані кібератаками, розмір втрат від яких до 2021 року може становити 4,2 трлн. $.

За оцінкою Forester Research[7], лише 2% від усіх спеціалістів у сфері інформаційних технологій мають необхідне навчання, підготовку, сертифікацію. Очевидно, що урядові організації, громадські та приватні компанії повинні більш

серйозно ставитися до загрози кібератак, вкладаючи більше ресурсів у створення ефективного кіберзахисту. Організаціям життєво необхідно додавати більше уваги освіті спеціалістів, оскільки понад 40% кібервразливостей безпосередньо пов'язані з особистими працівниками (дослідження Gartner Group)[4]. Для цього важливо підвищити обізнаність про кібербезпеку, проводити тренінги, використовувати відповідні симуляції, внаслідок чого персонал стане потужним щитом для захисту життєво важливих цифрових активів компанії.

У дослідженні Національного координаційного центру кібербезпеки Ради національної безпеки і оборони України та проекту USAID[8] зазначається, що понад 90% респондентів визнали необхідність впровадження системи тренінгів та професійного навчання для працівників, поточна ситуація залишається незадовільною. Наприклад, лише 13% вказали, що їхні працівники беруть участь у навчальних заходах щомісячно, в той час як 31% респондентів вказують, що це відбувається лише раз на квартал. Ще 28% вказали, що підвищення кваліфікації відбувається лише раз на рік, а 27% взагалі не проводять такого навчання. Не визначеною є ситуація з проведенням незалежного аудиту. Відповіді респондентів практично розділилися: 51% проводили і 49% не проводили аудит. При цьому лише у 50% висновки аудиту допомогли респондентам у підвищенні рівня кібербезпеки. На думку більшості респондентів (понад 60%), вимоги щодо організації роботи з кіберзахисту в їхніх організаціях визначені, при цьому вони регулюються переважно відомчими актами (понад 30%). Лише 10% респондентів відзначили наявність установлених на законодавчому рівні вимог. Більшість респондентів відзначили незадовільний рівень забезпечення роботи створеного підрозділу з кібербезпеки: понад 35% респондентів відзначили, що рівень кадрового забезпечення профільного кібербезпекового підрозділу становить менше 20% від потрібного (ще 38% — від 20 до 50% від потреби). 53% вказали, що рівень технічного забезпечення кібербезпекового підрозділу становить менше 20%. При цьому понад 70% респондентів відзначили, що їх працівники (в тому числі вище керівництво) знають, як реагувати на кіберзагрози, знають відповідні процедури. У частині оцінювання ризиків майже 80% респондентів відзначили, що

в них відсутні вимоги та практика оцінювання ризиків, пов'язаних із кіберзагрозами, а якщо таке оцінювання і проводиться окремими організаціями, то власними силами (понад 60% випадків). 70% респондентів зазначили, що в них відсутні інструменти підрахунку втрат організації при реалізації кіберзагроз. При цьому понад 60% респондентів вважають за необхідне розвивати систему страхування ризиків у сфері кібербезпеки.

1.2 Методи підвищення обізнаності персоналу у питаннях пов'язаних з інформаційною та кібербезпекою

Щоб успішно виконувати свої ролі в організації, працівники повинні отримати відповідні інструменти та підготовку. Правильні інструменти та навчання включають поєднання базової обізнаності з безпеки, основних навичок, спільного навчання або навчання на робочому місці, освіти, досвіду та знань, навичок і здібностей, які відповідають цій ролі. Безперервність навчання кібербезпеці допомагає забезпечити підхід до надання всієї необхідної інформації для окремих осіб.

Цілі навчання покликані забезпечити послідовний, загальнодержавний підхід для забезпечення того, щоб усі співробітники, які займаються IT-системами, інформаційними технологіями та діяльністю з кібербезпеки, незалежно від агенції, ролі, функції, роботи чи системи, отримали те саме, всебічне розуміння та навчання з безпеки. Цінністю послідовної програми навчання є переносимість основ кібербезпеки, коли співробітники змінюють роботу та організації.

Навчання є безперервним; воно починається з усвідомлення, розвивається до навчання і переростає в освіту. Безперервність навчання кібербезпеці надає контекст і взаємозв'язок між обізнаністю з безпеки, основами кібербезпеки, навчанням та освітою. Безперервність навчання демонструє, що основи обізнаності та кібербезпеки формують фундаментальну базу, необхідну для всіх людей, які займаються управлінням, експлуатацією, обслуговуванням, розробкою або використанням IT-систем, інформаційних технологій та кібербезпеки. Це

також демонструє, що рівні підготовки та освіти є більш вибірковими, заснованими на ролі та відповідальності.

Безперервність навчання з кібербезпеки є прогресом навчання у всьому спектрі ролей в організації. Навчання з питань безпеки проводиться для всіх користувачів в організації. Навчання з основи кібербезпеки проводиться для всіх користувачів, які працюють із IT-системами. Рольове навчання надається користувачам, які мають обов'язки щодо IT-систем. Знання, освіту та досвід здобувають спеціалісти та професіонали з IT-безпеки. Відповідний рівень обізнаності, навчання та освіти щодо кібербезпеки визначається роллю в організації. Особи отримують навички, беручи участь у рольовому навчанні разом зі своїм агентством.

Обізнаність з питань безпеки — це комбіноване рішення заходів, які сприяють безпеці, встановлюють підзвітність та інформують працівників про новини безпеки. Обізнаність прагне зосередити увагу людини на одній проблемі або групі проблем. Діяльність з підвищення обізнаності має на меті дозволити особам усвідомити проблеми IT/кібербезпеки та відповідним чином реагувати.

У діяльності з підвищення обізнаності учень є одержувачем інформації. Обізнаність покладається на охоплення широкої аудиторії за допомогою привабливих методів пакування. Навчання є більш формальним, має на меті формування знань та навичок для полегшення виконання роботи.

Навчання, досягнуте лише за допомогою активності усвідомлення, як правило, є короткостроковим, негайним і пов'язаним із певною проблемою. Наприклад, якщо метою навчання є «сприяти більш широкому використанню ефективного захисту паролем серед співробітників», діяльністю з підвищення обізнаності може бути використання наклейок-нагадувань для клавіатури комп'ютера або глобальних електронних листів для всіх співробітників, які підкреслюють використання ефективних паролів.

Обізнаність також прагне побудувати в середовищі користувачів інформаційної системи організації основи термінів і концепцій IT/кібербезпеки, на яких може базуватися подальше навчання на основі ролей, якщо потрібно.

Обізнаність інформує користувачів про загрози та вразливості, які впливають на їхню організацію та особисте робоче середовище, пояснюючи «що», але не «як» безпеки, а також повідомляючи, що дозволено, а що заборонено. Security Awareness не лише повідомляє про політику та процедури IT/кібербезпеки, яких необхідно дотримуватися, але й забезпечує основу для будь-яких санкцій та дисциплінарних заходів, накладених за недотримання. Усвідомлення безпеки використовується для пояснення правил поведінки при використанні інформаційних систем та інформації організації та встановлює рівень очікувань щодо прийнятного використання інформації та інформаційних систем.

Фундаментальна цінність програм підвищення обізнаності в галузі безпеки полягає в тому, що вони створюють основу для навчання, орієнтованого на роль, шляхом зміни ставлення, яке має почати змінювати організаційну культуру, що краще забезпечує місію організації за допомогою більш безпечних систем. Зміни, до яких потрібно прагнути, — це усвідомлення того, що IT/кібербезпека має вирішальне значення, оскільки збій безпеки має потенційно несприятливі наслідки для всіх. IT/кібербезпека – це робота кожного.

У діяльності з підвищення обізнаності учень є одержувачем інформації, тоді як учень у навчальному середовищі відіграє більш активну роль. Обізнаність покладається на охоплення широкої аудиторії за допомогою привабливих методів пакування. Навчання є більш формальним, має на меті формування знань та навичок для полегшення виконання роботи.

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

Інститут SANS визначив п’ять основних моделей зрілості інформаційної безпеки, що характеризують рівень обізнаності персоналу підприємств з точки зору кібербезпеки: [9]

1 Неіснуючий: Програми не існує. Працівники не мають уявлення про свою роль у підтриманні кібербезпеки на підприємстві, що їх дії безпосередньо впливають

на безпеку організації, не знають і не розуміють політику організації та легко стають жертвами методів соціальної інженерії.

2 Дотримання вимог: Програма призначена, перш за все, для задоволення конкретних критеріїв відповідності або аудиту. Навчання обмежується щорічною або спеціальною підготовкою. Працівники не знають організаційної політика та / або їх роль у захисті інформаційних активів їх організації.

3 Зміцнення поінформованості та зміни поведінки: програма визначає навчальні теми, що надають найбільший вплив на підтримку місії організації та зосереджена на цих ключових темах. Програма виходить за рамки простого щорічного навчання та включає постійне підкріплення протягом усього року. Програма впроваджується цікавим та позитивним способом, що сприяє зміні поведінки на роботі та вдома. В результаті люди розуміють політику організації, активно її дотримуються та визначають інциденти, запобігають їм й своєчасно повідомляють про них.

4 Довготривале заохочення та зміна культури: У програмі є процеси, ресурси та підтримка керівництва для довгострокового життєвого циклу, включаючи як мінімум щорічний огляд та оновлення програми. Таким чином, програма та кібербезпека є визначеною частиною культури організації.

5 Надійна структура метрик: Програма має надійну структуру метрик для відстеження прогресу та вимірювання впливу. Отже, програма постійно вдосконалюється і здатна продемонструвати рентабельність інвестицій. Показники є важливою частиною кожного етапу. Ця програма підкреслює, що для того, щоб по-справжньому мати зрілу модель інформаційної безпеки, підприємство повинне не тільки змінювати поведінку та культуру, але й мати структуру метрик для демонстрації цих змін.

Рисунок 1 - Ефективність моделей зрілості обізнаності про безпеку згідно SANS

За останні три роки спостерігається постійне зниження двох найбільш незрілих стадій: неіснуючих програм (з 7,6% до 4,36%) та програм, орієнтованих на дотримання вимог (з 27,1% до 21,1%). У той самий час спостерігається явний підйом двох найбільш зрілих стадіях - культурних змінах. та фреймворк метрик (на 5% більше). Це свідчить про повільне, але неухильне збільшення зрілості програми за останні три роки.

В рамках підвищення обізнаності в області ІБ навчання може проходити в наступних формах:- очного навчання (в своїй компанії або в спеціалізованих організаціях);

- дистанційного навчання (електронні курси, у формі тестування, вебінарів, онлайн-конференцій і т.п.);

- самостійного вивчення навчальних матеріалів.Розглядати очне навчання як метод регулярного підвищення обізнаності працівників з питань ІБ не завжди вигідно і ефективно, так як відрив від основної діяльності значної кількості працівників негативно впливає на бізнес компанії. Дана форма більше підходить для державних структур і невеликих компаній, де можна одночасно зібрати всіх працівників з мінімальним відривом від основної діяльності. Для великих компаній, що мають розгалужену регіональну мережу, найбільш підходящим є

використання систем дистанційного навчання, які дозволяють одночасно навчати та контролювати навчання великої кількості персоналу.

Додатково в процесі навчання можуть використовуватися так звані нестандартні засоби, що дозволяють підтримувати атмосферу ІБ, завдяки яким працівник запам'ятовує окремі положення політики безпеки та розуміє важливість вимог ІБ на емоційному та підсвідомому рівні: скрінсейвери, відеоролики, мультимедійні матеріали, блоки новин з ІБ, плакати, офісне приладдя з короткою інформацією щодо забезпечення ІБ.

Методи підвищення обізнаності можна розділити на три основні категорії: під керівництвом інструктора, звичайні та онлайн. Метод під керівництвом інструктора включає формальні презентації та тренінги. Звичайні методи для співробітників використовують плакати, буклети, тощо. В онлайн навчані використовуються технології для інформування співробітників про безпеку, наприклад комп'ютерні програми підвищення обізнаності. У таблиці 1.1 показані категорії:

Таблиця 1.1: Методи підвищення обізнаності про інформаційну безпеку

Категорії	Методи
Звичайні	плакати, наклейки, буклети, інформаційні бюлетені співробітників
Під керівництвом інструктора	Офіційні презентації чи навчальні заняття
Онлайн	Електронні статті або електронні листи
	Розподіл інформації про безпеку через Інтернет
	Повідомлення з попередженням про безпеку, наприклад, реєстрація повідомлень
	Гейміфікація

Методи, які можуть бути корисними при спробі підвищити обізнаність працівників щодо аспектів інформаційної безпеки. Ці методи наведені нижче:

- Читання матеріалів: обізнаність співробітників підвищується за рахунок читання політики безпеки, плакатів, інформаційних бюлетенів, веб-сайтів, електронних листів та довідників.

- На основі політик: організація надсилає попереджувальне повідомлення тим, хто не дотримувався її безпекової політики, якщо вона якимось чином була порушена.

- На основі подій: спеціальні заходи, які проводяться для підвищення обізнаності, такі як вступний інструктаж, очне навчання, тести, вікторини та автоматизовані анкети, особливо після серйозного порушення безпеки.

- На основі відео: користувачі відвідують сеанси підвищення поінформованості про безпеку за допомогою наочних посібників, таких як відеокасети, веб-сеанси, відеоігри та комп'ютерне навчання.

- Інструменти інформування про повідомлення (дрібничка): підвищення обізнаності за допомогою предметів, які співробітники використовують на робочому місці, наприклад ручок, брелоків для ключів, годинників, календарів, наклейок і блокнотів, що спливають. Прикладом цього є написання повідомлення «Не повідомляйте свій пароль» поверх наклейок календаря.

- Керівна підтримка: обізнаність та підтримка у навчанні з боку керівництва або групи інформаційної безпеки. Вони можуть відігравати значну роль у процесі підвищення обізнаності, створивши схему винагород або санкцій для тих, хто перебуває в рамках безпекової політики.

Таблиця 1.2: Ефективність методів підвищення обізнаності про інформаційну безпеку

Інструмент чи метод	Знання	Зміна відносин	Суб'єктивні норми	Увага	Зміна поведінки	Загальна ефективність
Освітня презентація	+	+	-	+	+	4
Електронні листи	+	+	-	+	-	3
Групове обговорення	+	+	+	-	+	4

Продовження таблиці 1.2

Інструмент чи метод	Знання	Зміна відносин	Суб'єктивні норми	Увага	Зміна поведінки	Загальна ефективність
Інформаційні бюлетені	+	+	-	-	-	2
Відеоігри	+	+	-	+	+	4
Комп'ютерне навчання	+	+	-	-	-	2
Плакаты	+	+	+	-	-	3

Таблиця 1.3: Оцінка методів підвищення обізнаності за їх перевагами та недоліками

Категорії	Методи	Переваги	Недоліки
Звичайні	плакати, наклейки, буклети, інформаційні бюлетені співробітників	-періодична інформація -може доставити більше одного повідомлення одночасно	-занадто багато інформації -часто розглядається спамом
Під керівництвом інструктора	Офіційні презентації чи навчальні заняття	-персональний моніторинг - Навчальними методами можна керувати -на запитання співробітників будуть надані відповіді під час сесії	-Дорого -деякі співробітники вважають це нудним -Залежить від досвіду інструктора
Онлайн	Електронні статті або електронні листи	-Ефективно, якщо співробітники їх читають -Недорого -періодична інформація	- часто розглядається спамом - розуміється тільки читаючи
Онлайн	Повідомлення з попередженням про безпеку, наприклад, реєстрація повідомлень	-інформаційне повідомлення, коли це необхідно	
	Гейміфікація	- може зацікавит та мотивувати співробітників -висока залученість співробітників -візуалізація досягнень та прогресу -можливість всіх співробітників проявити себе	-дорого і складно до впровадження - не відображає безпосередньо політику безпеки організації

Продовження таблиці 1.3

Онлайн	Інтернет тренінг щодо підвищення обізнаності	- дружелюбний та гнучкий -співробітники можуть навчатися на своєму місці	-співробітники завершують навчання за мінімальний час - призводить до почуття ізоляції -стає монотонною - не в змозі зацікавити співробітникам

Більше того, ситуації та події, які можуть статися в будь-якій організації, можуть призвести до запуску заходів щодо підвищення обізнаності з інформаційною безпекою. ENISA вказує на деякі важливі події та ситуації, які можуть означати, що необхідно підвищити обізнаність працівників щодо безпеки. Вони перераховані нижче:

- нові постанови чи закони;
- нова політика інформаційної безпеки та оновлення чи зміни в ній;
- впровадження нових технологій, продуктів та послуг;
- нові співробітники чи залучений персонал;
- нові ризики тощо.

Важливим аспектом роботи з підвищення обізнаності персоналу з питань ІБ є безперервність цього процесу. Законодавство і вимоги регуляторів швидко змінюються, з'являються нові загрози ІБ, нові інформаційні системи - все це необхідно оперативно відображати в програмах підвищення обізнаності. Для працівників компанії безперервність навчання полягає в повторенні вимог і правил ІБ (щоб вони не забувалися). Також важливо інформувати всіх працівників про зміни, що відбулися в політиках безпеки і процедурах забезпечення ІБ.

У програму підвищення обізнаності рекомендується включати основні теми: використання паролів (створення, частота зміни, складність і безпеку); антивірусний захист; поява електронних листів від незнайомих людей і відкриття вкладень; використання інтернету; спам; питання соціальної інженерії; реагування на інциденти; робота з дому і використання корпоративних систем для особистих цілей; захист конфіденційної інформації.

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

1.3 Дослідження методу гейміфікації

Оскільки кіберзлочинність продовжує посилюватися, певні організації та урядові установи шукають шляхи кращого залучення своїх співробітників до дійсно ефективного навчання з кібербезпеки. Гейміфікація - це використання ігрової механіки та ігрового мислення, щоб залучити користувачів до вирішення проблем та мотивувати їх шляхом запровадження елементів змагання та винагороди.

Багато компаній уже використовують гейміфікацію, щоб допомогти з адаптацією та залученням клієнтів, але тепер вони усвідомлюють переваги, які гейміфікація також може мати для навчання всієї компанії з кібербезпеки.

Метод гейміфікації, дозволяє підвищити залучення співробітників до робочих процесів, сприяє розвитку корпоративної культури організації, дозволяє в інноваційному форматі нарощувати професійні знання та навички, розвивати інноваційне мислення. Тому великі компанії використовують ігри як інструмент розвитку людського потенціалу та мотивації персоналу. Ігрові методи, що дозволяють представити реальні ситуації у метафоричній формі та моделювати реальні робочі ситуації та варіанти розвитку подій, успішно інтегруються у програми корпоративного навчання.

У дослідженні Growth Engineering[10] зазначено, що 85% співробітників виявляють більшу зацікавленість, коли в робочий процес запроваджуються методи гейміфікації. Також показний прогноз росту ігрової системи навчання на наступні 5 років по регіонах(рис. 1.2).

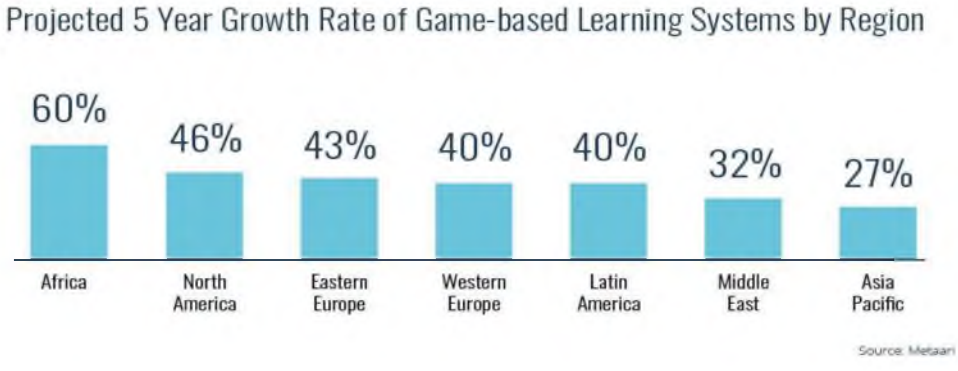

Рисунок 1.2 - Прогнозовані 5-річні темпи зростання ігрових систем навчання

Компаніям, які хочуть включити гейміфікацію в навчання з кібербезпеки необхідно розуміти, що сприяє найбільш успішному навчанню на основі ігор. В таблиці 1.4 представленні елементи успішної гейміфікації:

Таблиця 1.4 Елементи успішної стратегії гейміфікації

Елементи стратегії	Опис
Використовувати наочні посібники	Фотографії та відео можуть допомогти швидко донести точку зору, зберігаючи при цьому зацікавленість співробітників.
Короткі та доцільні тренінги	Найефективніші тренування короткі. Десятихвилинні заняття через день протягом 6 тижнів можуть бути набагато ефективніше, ніж одне тригодинне заняття.
Використовувати нагороди	Один з найбільш важливих елементів ігрового підходу, оскільки винагороди підтримують мотивацію і мотивацію користувачів.
Розглянути можливість використання штучного інтелекту і машинного навчання	Світ кібербезпеки постійно розвивається в міру того, як хакери освоюють нові і більш витончені підходи. Щоб не відставати від кіберзлочинців, деякі компанії впроваджують штучний інтелект і машинне навчання в свої ігрові кібер-тренування. Ця технологія дозволяє постійно оновлювати ігрове середовище на основі нових проблем і даних.
Знати аудиторію	Щоб отримати залученість, важливо розробити гру, яка буде викликати резонанс у цільової аудиторії. Дослідження того, що подобається працівникам, що їх мотивує та які пристрої вони найчастіше використовують, дасть міцну основу для створення ефективного навчання.
Переконатись у безперервності навчання	Навчання має бути безперервним і не обмежується одноразовим заходом. Відстеження прогресу співробітника через гру з винагородою на певних етапах може допомогти зберегти співробітників у довгостроковій перспективі.

Застосовувані методики навчання персоналу в організаціях, на сьогоднішній день не всі досить ефективні, тому що вони не завжди бувають цікавими і ніякої

залученості у персоналу не виникає. Тому можна запропонувати застосувати технологію гейміфікації для більш якісного навчання, і в результаті отримати не тільки добре навчений персонал, а й персонал, який отримав максимальне задоволення від навчання.

На першому етапі впровадження гейміфікації проводиться аналіз організації з точки зору навчання персоналу. Необхідно розглянути зовнішнє та внутрішнє середовище. В результаті аналізу внутрішнього середовища можна виділити слабкі сторони, які є майже в кожній організації: недостатній рівень навчання співробітників, висока плинність персоналу, яка пов'язана зі звільненням деяких співробітників, які були незадоволені ступенем навчання в організації; також можна зробити висновок, що традиційні методи навчання персоналу, що застосовуються, вже є малоефективними. Аналізуючи зовнішнє середовище можна спостерігати прогрес нових технологій з розвитку персоналу; зростання рівня конкуренції; збільшення інформаційного навантаження. На цьому етапі необхідно розглянути недоліки і переваги даної технології. До переваг можна віднести: високу залученність співробітників; візуалізацію досягнень та прогресу; можливість всіх співробітників проявити себе. До недоліків можна віднести: поверхневість, не всі співробітники можуть розуміти цю технологію як серйозний інструмент навчання; короткостроковий ефект; підвищений рівень конкуренції у співробітників може спричинити саботаж усередині колективу.

На наступному етапі формується мета гейміфікації. В першу чергу це створення системи навчання персоналу для підвищення обізнаності в питаннях інформаційної та кібербезпеки, підтримка постійної мотивації у персоналу до розвитку навичок в питаннях ІБ. Після того, як були сформульовані цілі гейміфікації, необхідно визначити категорію працівників, які навчатимуться за даною технологією.

Далі відбувається розробка структури інструментів гейміфікації. На цьому етапі необхідно: вибрати майданчик для реалізації гейміфікації; створити прості правила гри; обрати види заохочень (нагороди); створити конкурентне та рівне

для всіх учасників середовіще. На наступному етапі відбувається безпосереднє впровадження гейміфікації та навчання співробітників.

На заключному етапі впровадження технології гейміфікації передбачається отримати висококваліфікований персонал, який буде конкурентоспроможним і матиме всі знання, навички та вміння необхідні для успішного виконання поставлених цілей.

1.4 Висновки до першого розділу. Постановка задачі.

У першому розділі було досліджено теоретичну базу у сфері обізнаності персоналу в питаннях інформаційної та кібербезпеки. А саме, було проаналізовано поточний стан кібербезпеки та розглянуто основні загрози. Наступним етапом було розглянуто існуючі методи підвищення обізнаності персоналу. З методів підвищення обізнаності персоналу було виділено метод гейміфікації та проведено його аналіз.

Виходячи з результатів аналізу висновків до першого розділу, було поставлено задачі на подальше дослідження.

Отже необхідно розробити програму підвищення обізнаності персоналу в питаннях інформаційної та кібербезпеки з застосуванням методів гейміфікації.

Задля обґрунтування доцільності розробленої програми необхідно проаналізувати практичну та економічну ефективності запропонованої методики.

РОЗДІЛ 2. РОЗРОБКА ПРОГРАМИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА НАВЧАННЯ ПЕРСОНАЛУ У ПИТАННЯХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1Визначення моделі управління програмою підвищення обізнаності та навчання персоналу.

Програми підвищення обізнаності та навчання повинні розроблятися з урахуванням місії організації. Важливо, щоб програма підвищення обізнаності та навчання підтримувала бізнес-потреби організації і відповідала її культурі та IT-архітектурі. На етапі розробки програми визначаються потреби компанії в обізнаності та навчанні, розробляється ефективний план в масштабі всього підприємства та встановлюються пріоритети. Модель, яка використовується і встановлюється для нагляду за діяльністю програми підвищення обізнаності та навчання, залежить від розміру і географічного положення компанії, від її бюджету та певних організаційних ролей та обов'язків співробітників компанії. у стандарті NIST 800-20[11] приведено наступні моделі реалізації:

- модель 1: централізована політика, стратегія і реалізація;
- модель 2: централізована політика і стратегія, розподілена реалізація;
- модель 3: централізована політика, розподілена стратегія і реалізація.

Модель 1: Модель централізованого управління програмою (централізована політика, стратегія і реалізація).

У цій моделі відповідальність і бюджет програми навчання і підвищення обізнаності в області ІБ всієї організації покладається на центральне керівництво. Всі директиви, розробка стратегії, планування та складання графіків координуються через нього. Централізована модель управління програмами часто використовується компаніями, які:

- відносно невеликі або мають високий ступінь структурованості і централізованого управління більшістю IT-функцій;
- мають на рівні центрального офісу необхідні ресурси, досвід і знання про місії та операції на рівні підрозділу;
- мають високу ступінь схожості місії і оперативних цілей по всіх його компонентах.

Рис 2.1. Модель 1: Централізоване управління програмою навчання

Зв'язок між центральним органом влади і організаційними підрозділами здійснюється в обох напрямках. Центральний орган доводить до відома організаційних підрозділів директиви політики організації відносно обізнаності та навчання в області IT-безпеки, стратегію проведення програми, а також матеріали і методи її реалізації. Організаційні підрозділи надають інформацію, запитувану центральним органом. Наприклад, для виконання своїх обов'язків центральний орган може збирати дані про кількість учасників, ознайомлювальних сесій, кількості людей, які пройшли навчання з певної теми, і кількості людей, які ще не відвідали ознайомчі та навчальні заняття. Підрозділ організації також може надати зворотний зв'язок про ефективність обізнаності та навчальних матеріалів, а також про придатність методів, використовуваних для реалізації матеріалу. Це дозволяє центральному органу налаштовувати, додавати або видаляти матеріали або змінювати методи реалізації.

Модель 2: Модель частково децентралізованого управління програмою (централізована політика і стратегія; розподілене впровадження)

У цій моделі обізнаність про безпеку і політика і стратегія навчання визначаються центральним органом влади, але реалізація делегується посадовим особам лінійного керівництва в організації. Розподіл бюджету, розробка матеріалів і складання розкладу є обов'язками цих посадових осіб.

Оцінка потреб проводиться центральними органами, оскільки вони як і раніше визначають стратегію програми підвищення обізнаності та навчання. Політика, стратегія і бюджет передаються від центрального органу до організаційних підрозділів. На основі стратегії підрозділу організації розробляють власні плани навчання. Підрозділи організації розробляють навчальні матеріали, а також визначають методи використання матеріалу в своїх власних підрозділах.

Як і в випадку з централізованою моделлю управління програмою, в цій моделі зв'язок між центральним органом влади і організаційними підрозділами здійснюється в обох напрямках. Центральний орган повідомляє директиви політики агентства відносно обізнаності та навчання IT-безпеки, стратегії проведення програми і бюджету для кожного організаційного підрозділу. Центральний орган може також повідомити організаційних одиниць, що вони несуть відповідальність за розробку планів навчання та за реалізацію програми, і може надати керівництво або навчання організаційним одиницям, щоб вони могли виконувати свої обов'язки.

Рис. 2.2 Модель 2: Частково децентралізоване управління програмою навчання

Частково децентралізована модель управління програмами часто використовується компаніями, які:

- відносно великі або мають досить децентралізовану структуру з чіткими обов'язками, покладеними як на центральний орган влади, так і на рівень підрозділів;

- мають функції, які розкидані по широкій географічній області;

- мають організаційні підрозділи з різними завданнями, так що програми навчання можуть значно відрізнятися в залежності від потреб конкретних підрозділів.

Модель 3: Модель повністю децентралізованого управління програмою (централізована політика; розподілена стратегія і реалізація)

У цій моделі центральний орган з інформування та навчання безпеки (IT-директор, менеджер програми ІБ) поширює широку політику та очікування щодо обізнаності про безпеку і вимог до навчання, але передає відповідальність за виконання всієї програми іншим підрозділам організації. Ця модель зазвичай використовує серію директив розподілених повноважень, керованих центральним органом. Зазвичай це означає створення підсистеми IT-директорів і менеджерів програм IT-безпеки, підпорядкованих центральному IT-директору і співробітникові IT-безпеки.

Рис. 2.3 Модель 3: Повністю децентралізоване управління програмою навчання

Оцінка потреб проводиться кожним організаційним підрозділом, оскільки в цій моделі підрозділи самі визначають стратегію програми підвищення обізнаності та навчання. Політика і бюджет передаються від центрального органу

до організаційних підрозділам. На основі стратегії підрозділу організації розробляють власні плани навчання. Підрозділи організації розробляють свої навчальні матеріали, а також визначають методи використання матеріалу в своїх власних підрозділах.

Як і в разі моделі централізованого управління програмами і моделі частково децентралізованого управління програмами, в цій моделі зв'язок між центральним органом влади і організаційними підрозділами здійснюється в обох напрямках.

Повністю децентралізована модель управління програмами часто використовується організаціями, які:

- відносно великі;

- мають дуже децентралізовану структуру із загальними обов'язками, покладеними на центральний орган влади, і конкретними обов'язками, покладеними на рівні підрозділів;

- мають функції, які розкидані по широкій географічній області;

- мають автономні організаційні підрозділи з окремими і різними завданнями, тому програми навчання і обізнаності можуть сильно відрізнятися.

2.2 Оцінка потреб підприємства в обізнаності та навчанні персоналу.

Після того, як модель, яку слід використовувати, визначена, необхідно визначити підхід до проведення оцінки потреб відповідно до обраної організаційної моделі. Оцінка потреб - це процес, який можна використовувати для визначення потреб організації в обізнаності та навчанні. Результати оцінки потреб можуть служити обґрунтуванням, щоб переконати керівництво виділити адекватні ресурси для задоволення виявлених потреб в обізнаності та навчанні. При проведенні оцінки потреб важливо задіяти ключовий персонал. Як мінімум, такі ролі повинні бути розглянуті з точки зору будь-яких особливих потреб в навчанні:

- виконавче керівництво - керівники організацій повинні повністю розуміти директиви і закони, які складають основу програми безпеки. Їм також необхідно

розуміти свої керівні ролі в забезпеченні повної відповідності користувачам в своїх підрозділах;

- персонал служби безпеки (менеджери програм безпеки і співробітники служби безпеки) - ці люди виступають в якості експертів-консультантів для своєї організації і, отже, повинні бути добре обізнані про політики безпеки та загальноприйняті передові методи;

- власники систем - власники повинні добре розуміти політику безпеки і добре розбиратися в заходах безпеки і вимогах, які можна застосувати до систем, якими вони керують;

- системні адміністратори і персонал IT-підтримки - ці люди, що володіють високим ступенем повноважень щодо операцій підтримки, критично важливих для успішної програми забезпечення безпеки, потребують більш високих технічних знаннь в області ефективних методів забезпечення безпеки та їх реалізації;

- операційні менеджери і користувачі системи - цим особам потрібен високий рівень обізнаності про безпеку і навчання щодо заходів безпеки та правил поведінки для систем, які вони використовують для ведення бізнесу.

Різні джерела інформації в агентстві можуть використовуватися для визначення обізнаності в області IT-безпеки і потреб у навчанні. Існують наступні методи збору інформації в рамках оцінки потреб:

- інтерв'ю з усіма виявленими ключовими групами і організаціями;

- організаційні опитування;

- огляд та оцінка доступних довідкових матеріалів, таких як поточна обізнаність і навчальні матеріали, графіки навчання і списки учасників;

- аналіз показників, пов'язаних з обізнаністю і навчанням (наприклад, відсоток користувачів, які завершили необхідний сеанс ознайомлення, відсоток користувачів зі значними обов'язками з безпеки, які пройшли навчання матеріалами для конкретних ролей);

- огляд планів безпеки для систем загальної підтримки і основних додатків для визначення власників систем і додатків і призначених представників безпеки;

- огляд баз даних, ідентифікаторів користувачів, додатків для визначення всіх, у кого є доступ;

- огляд будь-яких рекомендацій наглядових органів;

- бесіди та інтерв'ю з керівництвом, власниками систем загальної підтримки і основних додатків, а також іншим персоналом організації, чиї бізнес-функції залежать від IT;

- аналіз подій, таких як атаки типу «відмова в обслуговуванні», пошкодження веб-сайтів, захоплення систем, використовуваних в наступних атаках, успішні вірусні атаки, може вказувати на необхідність навчання певних груп людей;

- перевірка технічних або інфраструктурних змін;

- вивчення тенденцій, вперше виявлених в галузевих, академічних або урядових публікаціях. Використання цих «систем раннього попередження» може дати уявлення про проблему в організації, яка ще не розглядається як проблема;

- метрики (таблиця 2.1) - важливий і ефективний інструмент, який можна використовувати для визначення обізнаності агентства в області IT-безпеки і потреб у навчанні. Метрики відстежують досягнення цілей і завдань програми підвищення обізнаності та навчання шляхом кількісної оцінки рівня реалізації обізнаності і навчання, а також ефективності і дієвості цієї програми, а також визначення можливих поліпшень.

Таблиця 2.1 - Метрики

Метрична назва	Що вимірюється	Як це вимірюється	Коли це вимірюється	Хто вимірює	Як оцінюється ризик	Загальний поточний бал
Час на виявлення інциденту	Показник фішингових кліків	Симуляції фішингу	Щомісячно	Команда безпеки	Клікабельність 0-3% дуже низька (1) 3-6% низька(2) 6-10% середня)3) 10-20% висока(4) 20%+дуже висока(5)	3

Продовження таблиці 2.1

Метрична назва	Що вимірюється	Як це вимірюється	Коли це вимірюється	Хто вимирює	Як оцінюється ризик	Загальний поточний бал
Автозаповнення	Випадкове розкриття даних через автозаповнення в електронній пошті	Запобігання втрати даних	Щомісячно	оперативний центр безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	4
Випадки втрати пристрою	Втрачені чи вкрадені ноутбуки чи мобільні пристрої	Фізична безпека	Щомісячно	Фізична безпека	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	2
Заражені комп'ютери	Кількість заражених комп'ютерів щомісяця через дії людини		Щомісячно	оперативний центр безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	4
Утилізація конфіденційних документів	Вимірює осіб, які безсумнівно, викидають будь-які конфіденційні документи в смітник	Перевірка сміття	Щомісячно	команда інформаційної безпеки або фізичної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	3
Порушення політики	Вимірює осіб, які порушують політику	Повідомлено керівниками служби безпеки або кадрів	Щомісячно	Відділ кадрів	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	4
Сприйняття безпеки	Вимірює сприйняття безпеки працівниками, щоб включити чи відчувають відповідальність за безпеку, чи знають вони, що вони є ціллю	Випадкові 5% робочої сили щомісяця	Щомісячно	Команда безпеки		4
Завершене навчання	Який відсоток персоналу пройшов необхідний тренінг з підвищення обізнаності	Система управління навчанням	Щомісячно	Група безпеки або навчання	98%+ завершено (1) 95%+ завершено (2) 90%+ завершено(3) 85% завершено(4) 80% завершено(5)	2

На рис. 2.4 показані загальні питання, пов'язані з конкретною організацією, які необхідно зрозуміти на початку оцінки потреб.

Рис. 2.4 Розуміння проблем, пов'язаних з конкретним підприємством

Аналіз зібраної інформації повинен дати відповіді на ключові питання:

- які знання, навчання необхідні;
- що в даний час робиться для задоволення цих потреб;
- який поточний статус щодо того, як ці потреби задовольняються;
- де розрив між потребами і тим, що робиться;
- які потреби найбільш важливі.

2.3 Розробка плану реалізації програми підвищення обізнаності персоналу з використанням методів гейміфікації

Після завершення оцінки потреб стає доступною інформація, необхідна для розробки плану підвищення обізнаності та навчання. План повинен охоплювати всю організацію і включати пріоритети, визначені оцінкою потреб. Завершення оцінки потреб дозволяє агентству розробити стратегію розробки, впровадження та підтримки своєї програми навчання і підвищення обізнаності в області IT-безпеки. План - це робочий документ, що містить елементи, складові стратегію. У плані повинні бути вказані такі елементи:

- існуюча національна і місцева політика, яка потребує підвищення обізнаності та навчання;

- обсяг програми підвищення обізнаності та навчання;

- ролі та обов'язки персоналу агентства, який повинен розробляти, впроваджувати і підтримувати інформаційні та навчальні матеріали, а також забезпечувати, щоб відповідні користувачі відвідували або переглядали застосовні матеріали;

- цілі, які повинні бути досягнуті по кожному аспекту програми (наприклад, обізнаність, навчання, освіту, професійний розвиток);

- цільові аудиторії по кожному аспекту програми;

- обов'язкові (і, у разі необхідності, факультативні) курси або матеріали для кожної цільової аудиторії;

- мета навчання по кожному аспекту програми;

- теми для обговорення на кожному занятті або курсі;

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

- локументація, відгуки та свідоцтва навчання по кожному аспекту програми;

- оцінка і оновлення матеріалу по кожному аспекту програми;

- частота, з якою кожна цільова аудиторія повинна знайомитися з матеріалом.

Програма обізнаності та навчання з IT-безпекою повинна бути реалізована тільки після того як було:

- проведено оцінку потреб;

- розроблено стратегію;

- складено план програми підвищення обізнаності та навчання для реалізації цієї стратегії;

- розроблено інформаційні та навчальні матеріали.

Здійснення програми має бути повністю пояснено компанії, щоб забезпечити підтримку в її реалізації і виділення необхідних ресурсів. Це пояснення включає очікування керівництва організації і підтримки персоналу, а також очікувані результати програми і вигоди для організації.

2.4 Введення в дію процесів моніторингу дотримання ефективності програми обізнаності та навчання персоналу

Оцінка ефективності навчання є важливим кроком для того, щоб навчання, яке проводиться, було змістовним. Навчання має сенс лише тоді, коли воно відповідає потребам як працівника, так і організації. Якщо зміст навчання є неправильним, застарілим або невідповідним для аудиторії, навчання не відповідатиме потребам працівників або організацій. Якщо метод навчання є невідповідним або щодо простоти або складності змісту, чи до типу аудиторії, навчання не відповідатиме потребам працівників і організації. Витрачання часу та ресурсів на навчання, яке не дає бажаних ефектів, може посилити, а не розвіяти сприйняття безпеки як перешкоди для продуктивності. Крім того, це може вимагати витрати набагато більше ресурсів на відновлення даних або системи після інциденту безпеки, ніж було б витрачено на заходи профілактики, такі як навчання.

Осмисленість навчання, або його ефективність, вимагає оцінювання. Оцінка ефективності навчання має чотири різні, але взаємопов'язані цілі. Необхідно оцінити:

- наскільки умови були слушними для навчання та суб'єктивне задоволення працівника;

- чому даний працінник навчився з конкретного курсу або навчального заходу (тобто цілі та ефективність навчання);

- зразок поведінки або результатів працівників після певного курсу або навчального заходу; (тобто ефективність навчання);

- цінність конкретного заняття або навчального заходу в порівнянні з іншими варіантами в контексті загальної програми навчання агенції з IT/кібербезпеки; (тобто ефективність програми).

Процес оцінки має виробляти чотири типи вимірювань, кожен з яких пов'язаний з однією з чотирьох цілей оцінки, відповідно до трьох типів користувачів оціночних даних:

- оцінки повинні допомогти самим працівникам оцінити їх подальшу роботу

продуктивність;

- оцінки повинні допомагати керівникам співробітників оцінювати подальшу продуктивність окремих працівників на робочому місці;

- оцінки повинні генерувати дані про тенденції, щоб допомогти тренерам покращити як навчання, так і викладання;

- оцінки повинні створювати статистику рентабельності інвестицій (ROI), щоб відповідальні посадові особи могли продумано та стратегічно розподіляти обмежені ресурси серед спектру обізнаності в галузі безпеки, основ кібербезпеки, навчання безпеки на основі ролей та варіантів навчання для досягнення оптимальних результатів серед робочої сили в цілому.

Після реалізації програми необхідно ввести в дію процеси моніторингу дотримання та ефективності. Автоматична система відстеження повинна бути розроблена для збору ключової інформації про діяльність програми (наприклад, курси, дати, аудиторія, витрати, джерела). Система відстеження повинна збирати ці дані на рівні компанії, щоб їх можна було використовувати для проведення аналізу і звітності в масштабах всього підприємства щодо ініціатив по підвищенню обізнаності, навчання і навчання. Вимоги до бази даних повинні включати потреби всіх можливих користувачів.

Механізми формальної оцінки та зворотного зв'язку є критично важливими компонентами будь-якої програми підвищення обізнаності, навчання і освіти в області безпеки. Безперервне поліпшення не може відбуватися без доброго розуміння того, як працює існуюча програма. Крім того, механізм зворотного зв'язку повинен бути розроблений для вирішення завдань, спочатку поставлених для програми. Після затвердження базових вимог можна розробити і впровадити стратегію зворотного зв'язку. На рисунку 2.5 показані різні механізми оцінки і зворотного зв'язку, які можна використовувати для оновлення плану програми підвищення обізнаності та навчання.

Рис. 2.5 Методи оцінки і зворотного зв'язку

Стратегія зворотного зв'язку повинна включати елементи, які будуть стосуватися якості, обсягу, способу розгортання (наприклад, веб-сайт, на місці, поза офісом), рівня складності, простоти використання, тривалості сеансу, актуальності, валюти і пропозицій щодо модифікації.

Для отримання зворотного зв'язку можна застосовувати безліч методів. До найбільш розповсюджених відносяться:

- анкети оцінки - можна використовувати різні формати;

- фокус-групи - об'єднайте учасників тренінгу на відкритих форумах, щоб обговорити їх точку зору на ефективність програми тренінгу з IT-безпеки і запросити їх ідеї щодо поліпшення;

- вибіркові інтерв'ю - цей підхід проводиться з використанням індивідуальних інтерв'ю або в невеликих однорідних групах (зазвичай десять або менше), цей підхід є більш індивідуальним і конфіденційним, ніж підхід фокус-групи, і може спонукати учасників більш відверто критикувати програму;

- незалежне спостереження, аналіз - це включення перевірки обізнаності та програми навчання в галузі IT-безпеки в якості завдання для зовнішнього підрядника або іншої третьої сторони в рамках аудиту, ініційованого агентством;

- формальні звіти про стан. Хороший спосіб зосередити увагу на вимогах до безпеки і навчання в усьому агентстві - це реалізувати вимогу регулярного надання звітів про стан функціональними менеджерами;

- порівняльний аналіз програм безпеки. Зовні орієнтована форма порівняльного аналізу безпеки порівнює ефективність організації з рядом інших організацій і надає компанії звіт про те, де вона має гірші показники, на основі спостережуваних вихідних даних у всіх організаціях з даними, доступними в даний час. Компонент цього типу порівняльного аналізу повинен включати обізнаність про безпеку і навчання.

2.5 Висновок до розділу 2

У другому розділі представлені рекомендації щодо створення та підтримки комплексної програми підвищення обізнаності та навчання у рамках програми IT-безпеки організації, починаючи від проектування, розробки та реалізації програми підвищення обізнаності та навчання до оцінки програми після впровадження. У цьому розділі також описано, як:

- вибрати теми для підвищення обізнаності та навчання;
- впровадити матеріали для підвищення обізнаності та навчання з використанням різних методів;
- оцінити ефективність програми.

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ В ПИТАННЯХ КІБЕРБЕЗПЕКИ ПЕРСОНАЛУ "КРЕДИТ-ЛЕГКО"

На основі даних викладених та проаналізованих в першому та другому розділах, розглянемо програму підвищення обізнаності персоналу в питаннях ІБ та її ефективність на прикладі ТОВ "Кредит-Легко".

3.1 Загальні відомості про підприємство

Організація ТОВ «Кредит -Легко» веде - колекторську діяльність на передсудовому і судовому етапах. Займається поверненням боргів юридичних осіб в не судовому порядку, стягненням боргів в арбітражному суді, купівлею боргів.

Форма власності: «Кредит -Легко» комерційна організація, зареєстрована як товариство з обмеженою відповідальністю, на основі приватної власності статутний капітал 500000 грн.

Діяльність організації пов'язана з взаємодією з юридичними і фізичними особами на основі договору надання послуг, пов'язаних з колекторською діяльністю. Клієнти організації надають відомості про своїх боржників, і дебіторів. ТОВ «Кредит -Легко» має справу з комерційною таємницею і персональними даними. Вищий гриф конфіденційності визначений як - строго конфіденційно.

Підприємство функціонує 5 днів на тиждень. Графік роботи з 8:00 до 18:00, з перервою на обід з 12.00 до 13.00.

На підприємстві діють наступні політики безпеки:

- політика моніторингу та контролю мережі Інтернет користувачами системи;
- політика "чистого столу";
- політика антивірусного захисту;
- політика розмежування даних;
- політика електронної пошти;
- політика утилізації технологічного обладнання.

Штат співробітників підприємства складається з 30 осіб. На рисунку 2.2 зображена організаційна структура робітників підприємства.

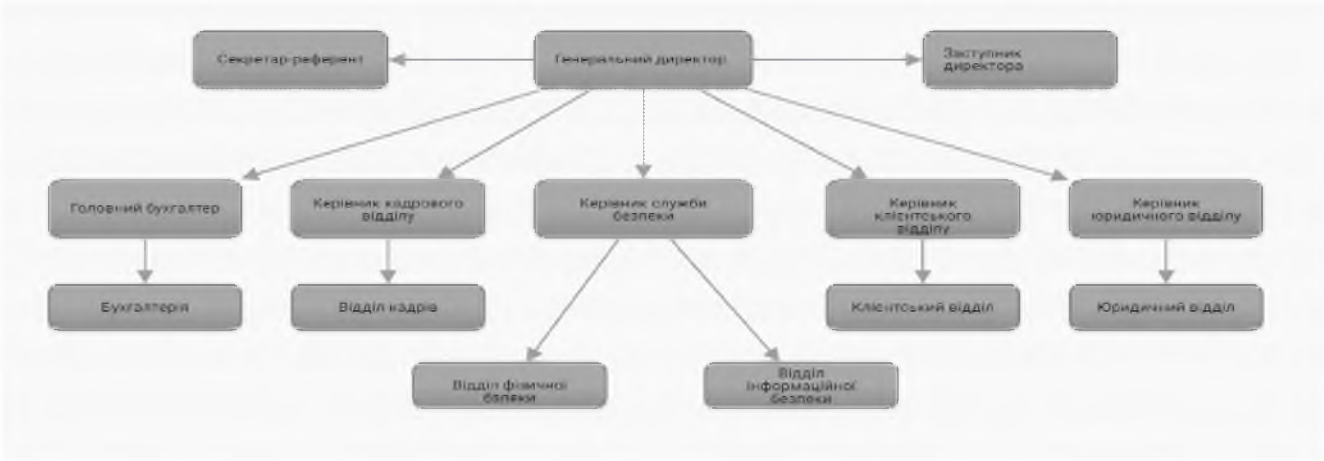

Рисунок 2.2 - Організаційна структура ТОВ «Кредит — Легко»

3.2 Модель загроз

Результатом аналізу можливих загроз є модель загроз [12] - абстрактний формалізований опис методів і засобів здійснення загроз із зазначенням рівнів гранично припустимих втрат. Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки технічного, антропогенного або стихійного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію що зберігається в ній.

Шкала оцінки загроз:

К1 – визначає ступінь доступності до об’єкта

1 – в іншій країні (для техногенних загроз) / немає доступу до об’єкта (для антропогенних загроз);

2 – в тій самій країні (для техногенних загроз) / віддалений доступ до об’єкта (для антропогенних загроз);

3 – поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних загроз) / фізичний несанкціонований доступ до об’єкта, несанкціоноване проникнення в приміщення (для антропогенних загроз);

4 – в тому ж приміщенні (для техногенних загроз) / доступ у приміщення, де знаходиться об’єкт (для антропогенних загроз);

5– сам об’єкт (для техногенних загроз) / фізичний дозволенний доступ до об’єкта (для антропогенних загроз).

К2 – присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу

1 – виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей; техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником;

2 – виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози; ПЗ та техніка оновлюється не постійно;

3 – виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загрози; ПЗ та техніка вразливі для деяких атак;

4 – виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози; відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка;

5 – мета виконавця; виконавець є експертом у методах, що реалізують загрозу (наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське ПЗ, тощо.

К3 – фатальність наслідків

1 – ОІД нічого не втратить, або наслідки будуть позитивними;

2 – Наслідками можна знехтувати;

3– Наслідки відчутні, але несуттєві;

4– Наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу;

5– Наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

К загальне для загроз розраховується за формулою:

$$(К_{оп})_i=(К1*К2*К3)/125$$

Таблиця 3.1Результати аналізу загроз та вразливостей інформації в ІТС

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
1	Здійснення атак на ОС	відсутність або неякісне антивірусне ПЗ	Зовнішнє, внутрішнє	4	3	4	0.38

Продовження таблиці 3.1

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
2	Читання залишкової інформації з оперативної та зовнішньої пам'яті ЕОМ	не реалізованість заборони повторного використання інформації	Внутрішнє	5	3	3	0.36
3	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	відсутність резервного обладнання	Внутрішнє	4	3	4	0.38
4	НСД до даних з порушенням встановлених правил розмежування внаслідок використання порушником відомих вразливостей системного та прикладного ПЗ	Недосконале ПЗ Помилки при розмежуванні доступу до системи	Зовнішнє внутрішнє	4	3	4	0.38
5	Порушення конфіденційності та цілісності інформації внаслідок навмисних дій авторизованого користувача	Відсутність резервних копій Неправильний підбір персоналу Неефективне розмежування доступу до системи	Внутрішнє	4	4	3	0.38
6	Розповсюдження і використання компютерних вірусів для порушення безпеки даних	відсутність або неефективність антивірусного ПЗ	Зовнішнє, Внутрішнє	5	3	4	0.48

Продовження таблиці 3.1

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
7	Одержання та використання атрибутів доступу системи іншим користувачем ІТС для розширення своїх повноважень або маскування під іншого зареєстрованого	відсутність/неефективність ідентифікації та автентифікації користувача	Внутрішнє	5	4	3	0.48
8	Неправомірне впровадження і забороненого політикою безпеки ПЗ(Порушення політик безпеки)	недбалість персоналу	Внутрішнє	5	3	3	0.36
9	Несанкціонований доступ до інформації через Wi-Fi	нерегулярна зміна паролів на Wi-Fi	Зовнішнє	4	3	4	0.4
10	Ненавмисне пошкодження інформації або її носіїв	- недосвідченість персоналу	Внутрішнє	5	2	3	0.24
11	Соціальна інженерія(шантаж, підкуп тощо)	- неправильний підбір персоналу	Внутрішнє	4	3	4	0.4
12	Проникнення в приміщення	неефективна система охорони; - неякісний контроль за приміщенням	Зовнішнє	3	1	4	0.1
13	Несанкціоноване копіювання інформації	- відсутність журналу подій.	Внутрішнє	2	3	4	0.2
14	Одержання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів	- передавання паролів у відкритому вигляді. - недосвідченість персоналу	Зовнішнє	5	3	4	0.48

Продовження таблиці 3.1

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
15	Випадкове зараження програмних засобів комп'ютерними вірусами	- недосвідченість персоналу; - відсутність або неякісне антивірусне ПЗ.	Внутрішнє	5	2	3	0.24
16	Несанкціонований перехват інформації на паперових або електронних носіях	неналежне зберігання документів та пристроїв з інформацією	Внутрішнє	5	3	4	0.48
17	Випадкове розкриття даних через автозаповнення в електронній пошті	- недосвідченість персоналу;	Внутрішнє	5	2	4	0.32
18	Не знання як розпізнавати фішингові посилання	- недосвідченість персоналу;	Внутрішнє	5	2	4	0.32

Згідно даних викладених в таблиці 3.1 високий рівень критичності мають наступні загрози: повязані с персоналом: випадкове розкриття даних через автозаповнення в електронній пошті, не знання як розпізнавати фішингові посилання, несанкціонований перехват інформації на паперових або електронних носіях, випадкове зараження програмних засобів комп'ютерними вірусами, одержання та використання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів, соціальна інженерія(шантаж, підкуп тощо), порушення політик безпеки, несанкціонований доступ до інформації через Wi-Fi. Реалізація цих загроз може привести до серйозних негативних наслідків.

3.3 Розробка програми навчання та підвищення обізнаності персоналу

На підприємстві проводяться планові навчання та перевірка знань персоналу:

- вступний інструктаж - проводиться при прийомі на роботу співробінника;

- первинний інструктаж на робочому місці - проводиться при виконанні. робіт, до яких пред'являються додаткові вимоги по інформаційній безпеці.

Позаплланова перевірка знань проводиться при зміні вимог по інформаційній безпеці, при порушеннях інформаційної безпеки.

Так як підприємство відносно невелике та має високий ступінь структурованості і централізованого управління більшістю IT-функцій, на підприємстві може бути використана модель централізованого управління програмою (централізована політика, стратегія і реалізація). У цій моделі відповідальність і бюджет програми навчання і підвищення обізнаності в області ІБ всієї організації покладається на центральне керівництво. Всі директиви, розробка стратегії, планування та складання графіків координуються через нього.

Під час оцінки потреб в обізнаності та навчанні шляхом метрик було визначено наступні проблеми в обізнаності персоналу:

Таблиця 3.2 Метрика до початку навчання

Метрична назва	що вимірюється	як це вимірюється	Коли це вимірюється	Хто вимірює	Як оцінюється ризик	загальний поточний бал
Час на виявлення інциденту	показник фішингових кліків	Симуляції фішингу	Щомісячно	Відділ з інформаційної безпеки	Клікабельність 0-3% дуже низька (1) 3-6% низька(2) 6-10% середня(3) 10-20% висока(4) 20%+дуже висока(5)	4
Автозаповнення	випадкове розкриття даних через автозаповнення в електронній пошті	Запобігання втрати даних	Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	5
Випадки втрати пристрою	втрачені чи вкрадені ноутбуки чи мобільні пристрої	Фізична безпека	Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1

Продовження таблиці 3.2

Метрична назва	що вимірюється	як це вимірюється	Коли це вимірюєтьс я	Хто вимірює	Як оцінюється ризик	загальний поточний бал
Утилізація конфіденційних документів	Вимірює осіб, які безсумнівно, викидають будь-які конфіденційні документи в смітник	Перевірка сміття	Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1
Порушення політики	Вимірює кількість порушень політик безпеки	Повідомлено керівниками служби безпеки або кадрів	Щомісячно	Відділ кадрів	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	3
Сприйняття безпеки	Виміряйте сприйняття безпеки працівниками, щоб включити чи відчувають відповідальність за безпеку, чи знають вони, що вони є ціллю	Випадкові 5% робочої сили щомісяця	Щомісячно	Відділ з інформаційної безпеки	Вимірюється шкалою Лікерта	4
Завершене навчання	Який відсоток персоналу пройшов необхідний тренінг з підвищення обізнаності	Система управління навчанням	Щомісячно	Відділ з інформаційної безпеки	98%+ завершено (1) 95%+ завершено (2) 90%+ завершено(3) 85% завершено(4) 80% завершено(5)	5

- незнання як виявити шпигунські програми та ПЗ(зараження компютерів) - високий;

- не знають як розпізнавати фішингові посилання(показник фішингових кліків) - високий;

- втрати даних через автозаповнення в електронній пошті - дуже високий;

- порушення політик безпеки - середній;

- працівники не допускають, що можуть стати цілями зловмисників або думають , що з хакерами боротися марно - високий;

- малий відсоток робочої сили пройшов необхідні тренінги з підвищення обізнаності - високий;

Також співробітниками відділу інформаційної безпеки були проведені організаційні опитування(ДОДАТОК Д) та тестування працівників компанії на

предмет знання в сфері інформаційної та кібербезпеки. Ці опитування вимірюють знання з предметного матеріалу до того, як буде проведено навчання. Був здійснений огляд та оцінка доступних довідкових та навчальних матеріалів,графіків навчання та списки учасників навчання.

Після аналізу даних отриманих з метрик, моделі загроз та опитувань, керівництво компанії прийняло рішення розробити та ввести політику навчання та тестування з питань безпеки та програму підвищення обізнаності персоналу.

Ціль політики навчання та тестування з питань безпеки визначає внутрішню програму навчання та обізнаності в галузі інформаційної безпеки компанії для інформування та оцінки всього персоналу щодо їх зобов'язань з інформаційної безпеки.

Ця політика застосовується до всіх співробітників компанії, які мають доступ до систем, мереж компанії, інформації компанії, закритої особистої інформації, інформації, що дозволяє встановити особу, та даним клієнтів.

Вимоги політики:

- програма підвищення обізнаності про інформаційну безпеку повинна гарантувати, що весь персонал повинен досягти базового рівня розуміння питань інформаційної безпеки, таких як загальні зобов'язання відповідно до різних політик інформаційної безпеки, стандартів, процедур, законів, нормативних актів;

- заходи з підвищення обізнаності та навчання з питань безпеки слід розпочинати якнайшвидше після приходу персоналу в організацію, як правило, шляхом проходження вступного інструктажу з інформаційної безпеки як частини процесу адаптації. Надалі діяльність з підвищення обізнаності повинна продовжуватися на безперервній основі, щоб підтримувати постійний рівень обізнаності.

- там, де це необхідно і практично здійснено, поінформованість про безпеку, а також навчальні матеріали та вправи повинні відповідати передбачуваній аудиторії з точки зору стилів, форматів, складності, технічного змісту тощо;

- компанія надасть персоналу інформацію про місце знаходження навчальних матеріалів з питань безпеки, а також політики, стандарти та рекомендації щодо безпеки для широкого кола питань інформаційної безпеки.

Відділ інформаційної безпеки компанії проводитиме періодичні імітаційні вправи з соціальної інженерії, включаючи, крім іншого: фішинг (електронна пошта), вішінг (голос), змішинг (SMS), тестування USB та фізична оцінка. Відділ ІБ компанії проводитиме ці випробування довільно протягом року без встановленого графіка або частоти. Відділ ІБ компанії може проводити цільові навчання для конкретних відділів чи окремих осіб з урахуванням визначення ризику.

Дотримання цієї політики є обов'язковим для всього персоналу. Відділ ІБ компанії контролюватиме дотримання та недотримання цієї політики та повідомлятиме керівництву про результати навчання.

Спеціалісти відділу з інформаційної безпеки компанії розробили комплексну програму підвищення обізнаності для персоналу до якої входять ігрові тренінги для підвищення обізнаності з інформаційної безпеки для співробітників всіх рівнів. Для різних категорій співробітників формуються різні навички. Вище керівництво, керівники підрозділів, IT-спеціалісти, користувачі - всі групи співробітників навчаються різним навичкам з урахуванням їх посадових обовязків. Комплексна програма підвищення обізнаності персоналу з кібербезпеки містить три основні елементи:

- навчання працівників організації
- підтримання атмосфери інформаційної безпеки
- оцінка ефективності програми.

Таблиця 3.3 Структура програми підвищення обізнаності

№	Назва	Пояснення
1	Ціль реалізації програми	Реалізація програми підвищення обізнаності співробітників направлена на вдосконалення знань та навичок з інформаційної безпеки у всіх працівників організації.

Продовження таблиці 3.3

№	Назва	Пояснення
2	Очікувані результати навчання	Кінцевою цілю реалізації програми підвищення обізнаності є зниження збитків і втрат(матеріальних, моральних і репутаційних) від загроз, пов'язаних з людським фактором при роботі з інформаційними ресурсами компанії.
3	Категорія учнів	Керівництво компанії: генеральний директор, заступник директора. Керівники структурних підрозділів: головний бухгалтер, керівник кадрового відділу, керівник юридичного відділу, керівник служби безпеки, керівник клієнтського відділу.
		Користувачі: співробітники бухгалтерії - 5 чол. співробітники кадрового відділу - 3 чол. співробітники відділу фізичної безпеки - 2 чол. співробітники юридичного відділу - 3 чол. співробітник клієнтського відділу - 4 чол. Секретар-референт
		Спеціалісти з IT-безпеки - 5 чол
4	Термін навчання , режим занять	1 місяць. 30 хвилин в день 1 раз на тиждень.
5	Форма навчань	Інтерактивні онлайн тренінги

Основними завданнями програми є:

- інформування працівників про існуючі загрози та питання безпеки, які можуть виникнути під час їх повсякденної роботи;

- забезпечення працівників основними вимогами, обмеженнями та правилами політики інформаційної безпеки компанії;

- підготовка працівників з точки зору принципів, методів і засобів протидії загрозам інформаційної безпеки;

- заохочення працівників до свідомого дотримання вимог, стосовно політик, процедур та інструкцій організації.

Програма спрямована на розвиток серед співробітників:

- здатності обгрунтовано оцінити можливі наслідки своїх дій під час роботи;

- стабільних звичок, які сприяють підтримці високого рівня інформаційної безпеки;

- здатності діяти правильно і швидко в разі виникнення інциденту інформаційної безпеки та в критичних ситуаціях.

Таблиця 3.4 Зміст програми підвищення обізнаності

№	Найменування навчального модуля	Зміст навчання	Категорія учнів	Дата проведення
1	Електрона пошта та фішинг	Теоретична частина, практичні поради, вправи що дозволяють відпрацювати практичні навички	Користувачі: співробітники бухгалтерії - 5 чол. співробітники кадрового відділу - 3 чол. співробітники відділу фізичної безпеки - 2 чол. співробітники юридичного відділу - 3 чол. співробітник клієнтського відділу - 4 чол.	щомісячно
2	Безпека паролей	Теоретична частина, практичні поради, вправи що дозволяють відпрацювати практичні навички	Користувачі: співробітники бухгалтерії - 5 чол. співробітники кадрового відділу - 3 чол. співробітники відділу фізичної безпеки - 2 чол. співробітники юридичного відділу - 3 чол. співробітник клієнтського відділу - 4 чол.	щомісячно
3	Правила безпеки для керівництва	Теоретична частина, практичні поради, вправи що дозволяють відпрацювати практичні навички	Керівництво компанії: генеральний директор, заступник директора, головний бухгалтер, керівник кадрового відділу, керівник юридичного відділу, керівник служби безпеки, керівник клієнтського відділу.	щомісячно

Продовження таблиці 3.4

№	Найменування навчального модуля	Зміст навчання	Категорія учнів	Дата проведення
4	Шпигунські програми та їх виявлення. Протидія вірусним атакам	Теоретична частина, практичні поради, вправи що дозволяють відпрацювати практичні навички	Користувачі: співробітники бухгалтерії - 5 чол. співробітники кадрового відділу - 3 чол. співробітники відділу фізичної безпеки - 2 чол. співробітники юридичного відділу - 3 чол. співробітник клієнтського відділу - 4 чол.	щомісячно
5	Корпоративна політика інформаційної безпеки	Теоретична частина, практичні поради, вправи що дозволяють відпрацювати практичні навички	Керівництво компанії: генеральний директор, заступник директора, головний бухгалтер, керівник кадрового відділу, керівник юридичного відділу, керівник служби безпеки, керівник клієнтського відділу. Користувачі: співробітники бухгалтерії - 5 чол. співробітники кадрового відділу - 3 чол. співробітники відділу фізичної безпеки - 2 чол. співробітники юридичного відділу - 3 чол. співробітник клієнтського відділу - 4 чол. Спеціалісти з IT-безпеки - 5 чол.	щомісячно
6	CTF-турніри	Командне виконання практичних завдань	Спеціалісти з IT-безпеки - 5 чол.	щомісячно

Програма підвищення обізнаності включає в себе тренінги з інформаційній безпеки для співробітників всіх рівнів. В тренінгах використовується ігровий підхід, практичні заняття, імітація атак та інші інтерактивні методи. До програми входять наступні модулі:

- Електрона пошта та фішинг;

- Безпека паролей;

- Правила безпеки для керівництва;

- Шпигунські програми та їх виявлення. Протидія вірусним атакам;

- Корпоративна політика інформаційної безпеки.

Навчальний модуль " Електрона пошта та фішинг" включає в себе інформаційні слайди на задану тему з аудіосупроводами і анімаційними додатками та навчання у вигляді ігор Rock defenders (bayside school) - навчає як розпізнавати електроні листи пов'язані з шахрайською активністю відомою як "фішинг". Anti-phishing phil - завдання гри - навчити користувачів розпізнавати фішингові посилання. Захоплююча онлайн-гра, яка вчить , як визначати фішингові URL-адреси, де шукати підказки в веб-браузерах і як використовувати пошукові системи для пошуку законних сайтів. Ціль даного модуля навчити користувачів забезпечувати:

- захист змісту листів під час їхньої передачі;

- перевірку змісту листів на наявність посилання на шкідливі сайти і спам;

- аутентифікацію і авторизацію для безпечного доступу до облікового запису;

- цілісність і функціональність поштової програми;

Модуль " Безпека паролей" включає в себе інформаційні слайди на задану тему з аудіосупроводами і анімаційними додатками та гру Password strength meter - гра показує як сила пароля може вимірюватись автоматичними веб формами і як зробити надійний пароль. В даній грі знадобиться створити паролі різної надійності відповідно зрізними факторами, такими як кількість символів, тип символів їх порядок і мінливість. Хоча це і не куленепробивний метод запобігання злому пароля при атаці методом грубої сили, це хороша стартова точка для розуміння безпеки паролів. Ціль даного модуля навчити користувачів створювати надійні паролі та надати рекомендації, яких слід дотримуватися для безпеки при користуванні паролями

Модуль " Шпигунські програми та їх виявлення. Протидія вірусним атакам" включає в себе інформаційні слайди на задану тему з аудіосупроводами і

анімаційними додатками та ігри Outbreak - гра дає можливість розвинути навики по захисту кількох офісних будівель від кібератак. Насувається хвиля кібератак і вірусів. Працівник бере на себе роль відповідального за захист всіх комп'ютерних систем розкиданих по країні. Net invaders - в цій грі потрібно захистити ЦОД, офіс і мобільне робоче місце використовуючи засоби захисту, засоби боротьби з шкідливим кодом і тп., Ця гра розрахована на вивчення різних інструментів захисту в залежності від вихідної загрози. Ціль модуля навчити користувачів:

- що таке шпигунське ПЗ та його види ;
- як виявити та видалити шпигунські програми;
- як захистити комп'ютер від вірусів;
- як працюють комп'ютерні віруси.

Модуль " Корпоративна політика інформаційної безпеки" включає в себе лекцію та семінар на задану тему. Для закріплення теми, обговорення чергуються з іграми та колективними завданнями у вигляді кросвордів, ребусів. За успішне проходження ігор та виконання завдань співробітникам видаються бейджі. Видача бейджів свідчить про виконання поставлених задач, отримання необхідних навиків. Хоч використання бейджів не є методом навчання, вони можуть послужити мотиваційним інструментом і сприяти залученню співробітників у навчальний процес. Ціль даного курсу донести до користувачів та спеціалістів важливість виконання політик інформаційної безпеки.

В основі модуля "Правила безпеки для керівництва" лежить симуляція реальних подій і значимість кібербезпеки для керівництва. Ціль даного курсу продемонструвати керівництву вплив кіберзагроз на результати бізнесу, висвітлити ризики і проблеми безпеки пов'язаних з використанням сучасних технологій. В модулі висвітлюється важливість кібербезпеки на рівні відповідальності керівництва.

Спеціалісти з відділу інформаційної безпеки компанії приймають участь у CTFтурнірах. Це змагання у формі командної гри, головна мета якої – захопити «прапор» у суперника в наближених до реальності умовах. Команди вирішують прикладні завдання, щоб одержати унікальну комбінацію символів (прапор). Далі

учасники відправляють прапор у спеціальну платформу та отримують підтвердження, що завдання вирішено правильно чи варто спробувати дати відповідь ще раз. CTF-турніри традиційно проводяться у двох форматах: у форматі Task-Based гравцям надається набір завдань, до яких потрібно знайти та надіслати відповідь. Відповідь подається у вигляді прапора, що складається з набору символів або довільної фрази. За правильне виконання кожного завдання команда отримує бали. Чим складніше завдання, тим більше очок дається за правильну відповідь. Завдання у CTF-змаганнях формату Task-Based, як правило, поділяються на наступні категорії: завдання на знаходження веб-уразливостей (web), пошук та експлуатацію вразливостей у додатках (PWN), дослідження програм без вихідного коду (reverse), розслідування інцидентів (forensic), адміністрування (admin), криптографію (crypto), стеганографію (stegano), пошук інформації з відкритих джерел (OSINT) та категорія joy, що складається з розважальних завдань.

Другий формат проведення CTF-змагань – Classic (або Attack-Defense). Команди отримують ідентичні сервери з набором вразливих сервісів, на які журі періодично надсилає приватну інформацію - прапори. Завдання кожної команди полягає в тому, щоб знайти та усунути вразливості на своєму сервері та скористатися знайденими вразливими для отримання прапорів у суперників.

Ці турніри дають можливість отримати нові знання та навички в області кибербезпеки, покращити практичні навички по розпізнаванню можливої атаки. Також мотивують IT-спеціалістів знаходитит нові ознаки кібератаки.

Для підтримання атмосфери інформаційної безпеки в компанії використовуються плакати, екрані заставки (скринсейвери), тематичні розсилки, сувенірна продукція (стікери для для запису, календарі), банери, повідомлення електронної пошти .

Таблиця 3.5 Метрика після проведення навчання

Метрична назва	Що вимірюється	Як це вимірюється	Коли це вимірюється	Хто вимірює	Як оцінюється ризик	Загальний поточний бал
Час на виявлення інцидену	показник фішингових кліків	симуляції фішингу	Щомісячно	Відділ з інформаційної безпеки	Клікабельність 0-3% дуже низька (1) 3-6% низька(2) 6-10% середня)3) 10-20% висока(4) 20%+дуже висока(5)	1
Автозаповнення	випадкове розкриття даних через автозаповнення в електронній пошті	Запобігання втрати даних	Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1
Випадки втрати пристрою	втрачені чи вкрадені ноутбуки чи мобільні пристрої	Фізична безпека	Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1
Заражені комп'ютери	Кількість заражень комп'ютерів щомісяця через дії людини		Щомісячно	Відділ з інформаційної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1
утилізація конфіденційних документів	Вимірює осіб, які безсумнівно, викидають будь-які конфіденційні документи в смітник	Перевірка сміття	Щомісячно	команда інформаційної безпеки або фізичної безпеки	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1
Порушення політики безпеки	Вимірює кількість порушень політик безпеки	Повідомлено керівниками служби безпеки або кадрів	Щомісячно	Відділ кадрів	0-2 рази на місяць (1) 3-5 разів на місяць (2) 5-10 разів на місяць (3) 10-20 разів на місяць(4) 20+(5)	1

Продовження таблиці 3.5

Метрична назва	що вимірюється	як це вимірюється	Коли це вимірюється	Хто вимірює	Як оцінюється ризик	загальний поточний бал
Сприйняття безпеки	Виміряйте сприйняття безпеки працівниками, щоб включити чи відчувають відповідальність за безпеку, чи знають вони, що вони є ціллю	Випадкові 5% робочої сили щомісяця	Щомісячно	Відділ з інформаційної безпеки	Вимірюється шкалою Лікерта	1
Завершене навчання	Який відсоток персоналу пройшов необхідний тренінг з підвищення обізнаності	Система управління навчанням	Щомісячно	Відділ з інформаційної безпеки	98%+ завершено (1) 95%+ завершено (2) 90%+ завершено(3) 85% завершено(4) 80% завершено(5)	1

Після реалізації програми підвищення обізнаності для оцінки її ефективності були проведені тестування знань працівників компанії, внутрішній аудит, а також атаки на персонал у виді відправлення провокаційних повідомлень через електронну пошту компанії, що провокує користувачів порушувати правила інформаційної безпеки, що діють в організації. Також після закінчення навчання,для аналізу ефективності програми були повторно використані метрики. Після аналізу даних можна зазначити, що рівень обізнаності персоналу значно підвищився. Після проведення порівняльного метрик проведених до навчання та після навчання персоналу було виявлено що:

- показник фішингових кліків знизився з високого(10-20% на місяць) до дуже низького(0-2% разів на місяць),

- випадкове розкриття даних через автозаповнення в електронній пошті знизилось с дуже високого(20+ разів на місяць) до дуже низького(0-2 разів на місяць)

- кількість порушень політик безпеки знизився з середнього(5-10 разів на місяць) до дуже низького(0-2 рази на місяць)

- кількість заражень компютерів через дії людини з високого (10-20 разів на місяць) до дуже низького(0-2 разів на місяць)

- показник працівників, які не допускають, що можуть стати цілями зловмисників або думають , що з хакерами боротися марно знизився до низького

- показник робітників, що пройшли необхідні тренінги з підвищення обізнаності ІБ досяг 100%.

3.4 Висновки до розділу 3

У третьому розділі було виконано обстеження ОІД, а також побудовано модель загроз та розроблено метрики для виявлення рівня обізнаності персоналу.

На основі аналізу моделі загроз та метрик було обрано найбільш актуальні загрози повязані з персоналом та для запобігання їх реалізації була розроблена програма підвищення обізнаності персоналу до якої входять наступні навчальні модулі:

- Електрона пошта та фішинг;
- Безпека паролей;
- Правила безпеки для керівництва;
- Шпигунські програми та їх виявлення. Протидія вірусним атакам;
- Корпоративна політика інформаційної безпеки.

РОЗДІЛ 4. ЕКОНОМІЧНА ЧАСТИНА

4.1 Необхідність обґрунтування витрат на реалізацію програму підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки

Метою розрахунків є економічне обґрунтування доцільності впровадження програми підвищення обізнаності персоналу у питаннях кібербезпеки. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

– витрати на розробку, впровадження та підтримку програми;

– різницю вірогідності загроз шляхом визначення рівня обізнаності персоналу у питаннях інформаційної та кібербезпеки до, та після впровадження програми підвищення обізнаності персоналу;

– економічну доцільність впровадження програми на підприємстві.

4.2 Визначення трудомісткості розробки політики безпеки інформації

Розрахунок витрат на розробку програму підвищення обізнаності персоналу у питаннях інформаційної та кібербезпеки.

Тривалість створення програми підвищення обізнаності визначається за формулою:

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку п'яти модулів 200 год.;

$t_р$– тривалість розробки анкет и метрики 16 год.;

$$t=200 \text{ год}+16 \text{ год}=216 \text{ год.}$$

Витрати на розробку програми підвищення обізнаності $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки програми підвищення обізнаності $З_{мч}$ за формулою 3.2:

$$К_{рп} = З_{зп} + З_{мч}, \text{ грн.} \qquad (3.2)$$

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

$$Ззп = t \cdot Зіб \text{ , грн} \qquad (3.3)$$

де *t* – загальна тривалість розробки програми підвищення обізнаності, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{ЗП} = 216 \cdot 405 = 22680 \text{ грн.}$$

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

$$З_{мч} = t \cdot С_{мч} \text{ , грн,} \qquad (3.4)$$

де *t* – трудомісткість розробки програми підвищення обізнаності на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + (Ф_{зал} \cdot Н_а / F_р) + (К_{лпз} \cdot Н_а / F_р), \text{ грн} \qquad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ - кількість задіяних робочих станцій при написані політики безпеки

$С_е$ – тариф на електричну енергію, грн/кВт·година;

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

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

$Н_{апз}$– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

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

Оскільки на даному підприємстві встановлена потужність *P=0,4*, а тариф на електричну енергію становить 1.91 грн/кВт·година то:

$$С_{мч} = 0.4 \cdot 1.68 \cdot 1 + (11400 \cdot 0.5/1920) + (5141 \cdot 0.5/1920) = 4.96 \text{ грн}$$

$$З_{мч} = t \cdot С_{мч} = 216 \cdot 4.96 = 1071.36 \text{грн}$$

4.3 Розрахунок капітальних та експлуатаційних витрат

Капітальні витрати розраховуються наступним чином:

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

де $К_{пр}$ - вартість розробки програми підвищення обізнаності та залучення для цього зовнішніх консультантів тис. грн. Стороння організація не наймалась, тому даний коефіцієнт не враховується при розрахунках;

$К_{зпз}$ - вартість закупівель ліцензійного основного й додаткового ПЗ, складає 2161 грн(програма Talent LMS);

$К_{рп}$ - вартість розробки програми підвищення обізнаності складає 23751.36 грн.;

$К_{аз}$ - вартість закупівлі апаратного забезпечення

$К_{дм}$ - допоміжних матеріалів: 5 плакатів(46грн/шт), банери 1 шт(37 грн), стікери 500шт(343 грн), календарі 30 шт(750 грн) - всього 1694 грн;

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, тис грн. Ввідна лекція 1000 грн.

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Оскільки підприємство не закуповує апаратне забезпечення, для розробки програми підвищення обізнаності $К_{аз}$ та $К_{н}$ не враховуються.

$$К_{рп}=З_{зп}+З_{мч}=22680+1071.36=23751.36 \text{ грн.}$$

$$К=2161+23751.36+1694+1000=29056.36 \text{ грн.}$$

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

$$С = К_{ПІ} + К_{ВП}+П_{н}+(Р\cdot t_{нал}\cdot С_{е}), \text{ тис. грн} \quad (3.7)$$

де $К_{ПІ}$ - витрати на заробітну плату співробітника за проведення інструктажу 2 рази на рік;

$К_{ВП}$ - витрати на внесення правок до модулей згідно актуальних проблем в обізнаності персоналу

$П_{н}$ - оплачувані витрати робочого часу співробітників під час проходження навчального курсу

Р – встановлена потужність ПК, кВт;

$t_{нал}$ - кількість задіяних робочих станцій

C_e – тариф на електричну енергію, грн/кВт·година;

Таблиця 3.1 – Заробітна плата робітників за місяць

Посада	Розмір заробітної плати, грн.	Всього, грн
Ген директор(1чол)	28000	28000
Заступник директора(1чол)	25000	25000
Секретар-референт(1чол)	6800	6800
Головний бухгалтер(1чол)	13000	13000
Бухгалтер(5чол)	7500	37500
Керівник кадровогу відділу(1чол)	12500	12500
Співробітник кадрового відділу(3чол)	6200	18600
Керівник клієнтського відділу(1чол)	12500	12500
Співробітник клієнтського відділу(4чол)	7500	30000
Керівник юридичного відділу(1чол)	12500	12500
Юрист(3чол)	7500	22500
Керівник служби безпеки(1чол)	12500	12500
Системний адміністратор(2чол)	11000	22000
Спеціаліст з інформаційної безпеки(3чол)	11000	33000
Начальник охорони(1чол)	12000	12000
Співробітник бюро пропусків(1чол)	6200	6200
Охоронець(1чол)	6800	6800
Всього	187500	311400

$$П_{н=(}(З_с/F) \cdot t_н, \text{ грн.} \qquad (3.8)$$

$$П_н=(311400/176) \cdot 4 = 7077.27 \text{ грн.},$$

де $З_с$ - загальна кількість витрат на заробітну плату співробітників за місяць, F - місячний фонд робочого часу, $t_н$ - час простою внаслідок навчання.

$$C = 7000+2000+7077.27+(0.4 \cdot 1.68 \cdot 30)=16107.92 \text{ грн}$$

4.4 Розрахунок вірогідності реалізації загроз до та після підвищення обізнаності

Слід зазначити, що чим нижче рівень обізнаності персоналу у питаннях інформаційної та кібербезпеки, тим вище рівень загрозі у цій сфері.

Ймовірність реалізації загрози можна розглядати як функцію трьох змінних: ймовірність існування загрози безпеки ($Й_{ІЗ}$) ймовірності існування вразливостей ($Й_{ІВ}$) і коефіцієнт наявних потенційних сил по цій загрозі на системи безпеки ($К_{НПС}$). Тоді ймовірність реалізації загрози можна розрахувати:

$$Й = Й_{ІЗ} \cdot Й_{ІВ} \cdot К_{НПС}. \quad (3.9)$$

Якщо будь-яка з цих змінних наближається до нуля, то і ймовірність реалізації загрози буде прагнути до мінімуму. Розроблена програма направлена на зменшення ймовірності існування вразивостей шляхом підвищення обізнаності співробітників у питаннях інформаційної безпеки.

Як було вказано у розділі 1за статистикою аналітичного центру Gartner Group[7], 40% збитків , пов'язаних з порушенням інформаційної безпеки, виникають через недостатню обізнаності персоналу у питаннях ікібербезпеки.

Отже:

$$Й_{вЗ} = 40\%.$$

Ймовірність існування вразливостей приймається, як відсоток обізнаності , упущений персоналом, тобто:

$$Й_{ІУ} = 100\% - О, \quad (3.10)$$

де О - рівень обізнаності персоналу у питаннях інформаційної безпеки.

Визначення рівня обізнаності персоналу у питаннях інформаційної та кібербезпеки відбувається на основі опитувань та тестувань. На основі відповідей було підраховано відсоток правильних відповідей.

Для розрахунку середнього рівня обізнаності персоналу підприємства визначається середнє арифметичне значення для усіх співробітників (30 працівників).

$$О_{ДО} = (К_1 + К_2 + К_3 + К_4 + К_5 + ... + К_{30}) / 30, \quad (3.11)$$

$О_{ДО}$=(58+34+43+27+33+40+52+37+29+25+60+31+34+62+21+26+65+60+62+29+38+47+44+22+40+30+33+28+22+39)/30 =39%

Аналогічно розрахунку рівня обізнаності персоналу у питаннях інформаційної та кібербезпеки до навчання, розраховується рівень обізнаності після її впровадження

$$О_{ПІСЛЯ} = (К_1 + К_2 + К_3 + К_4 + К_5 + ... + К_{30}) / 30, \quad (3.12)$$

$О_{ДО}$=(99+74+83+87+83+80+88+77+89+85+95+71+74+92+81+86+95+99+92+89+78+87+84+82+80+70+73+88+82+79)/30 =84%

Коефіцієнт наявності потенційних сил приймаємо $Й_{НПС}$ = 0,03%.

Отже, розрахуємо ймовірність реалізації загрози до впровадження програми:

$$Й_{ДО} = Й_{ІЗ} \cdot (100\% - О_{ДО}) \cdot К_{НПС}, \quad (3.13)$$

$Й_{ДО}$=40(100-39)0.03=73.2%

Та після впровадження:

$$Й_{ПІСЛЯ} = Й_{ІЗ} \cdot (100\% - О_{ДО}) \cdot К_{НПС}, \quad (3.14)$$

$Й_{ПІСЛЯ}$=40(100-84)0.03=19.2%

4.5 Економічна доцільність застосування програми на підприємстві

Приймаємо річний можливий збиток ТОВ "Кредит - Легко" від кібератак рівним З=100000 грн.

Отже, річний збиток до впровадження методики складав 73.2% від можливого збитку:

$З_{ДО}$=73200 грн.

Річний збиток після впровадження методики складає 19.2% від можливого збитку:

$З_{ПІСЛЯ}$=19200 грн.

Економічна доцільність застосування програми розраховується за формулою:

$$Е = З_{ПІСЛЯ} - З_{ДО} - С – К > 0, \quad (3.15)$$

Е=73200-19200-9000-29056.36=15943.64 грн.>0

Визначаємо термін окупності капітальних інвестицій за формулою:

$$Т = К / (З_{ПІСЛЯ} – З_{ДО} – С), \quad (3.16)$$

Т=15943.64/29056.36=0.54≈5 місяців

4.6 Висновки до економічної частини

В результаті розрахованих витрат на впровадження програми підвищення обізнаності у питаннях інформаційної та кібербезпеки було доведено, що застосування програми на ТОВ"Кредит - Легко" знизить ймовірність реалізації загроз інформаційної безпеки на 54%.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено теоретичну базу у сфері обізнаності персоналу в питаннях інформаційної та кібербезпеки. А саме, було проаналізовано поточний стан кібербезпеки та розглянуто основні загрози. Наступним етапом було розглянуто існуючі методи підвищення обізнаності персоналу. З методів підвищення обізнаності персоналу було виділено метод гейміфікації та проведено його аналіз. Представлені рекомендації щодо створення та підтримки комплексної програми підвищення обізнаності та навчання у рамках програми ІТ-безпеки організації, починаючи від проектування, розробки та реалізації програми підвищення обізнаності та навчання до оцінки програми після впровадження, а також описано, як:

- вибрати теми для підвищення обізнаності та навчання;
- впровадити матеріали для підвищення обізнаності та навчання з використанням різних методів;
- оцінити ефективність програми.

Виконано обстеження ОІД, а також побудовано модель загроз та розроблено метрики для виявлення рівня обізнаності персоналу.

На основі аналізу моделі загроз та метрик було обрано найбільш актуальні загрози повязані з персоналом та для запобігання їх реалізації була розроблена програма підвищення обізнаності персоналу.

Був проведений розрахунок та проаналізована доцільність впровадження політики безпеки інформації.

Отримані дані говорять про те, що впровадження програми підвищення обізнаності є доцільним.

На вимогу керівника підприємства з метою збереження конфіденційності деяка інформація про ІТС підприємства була змінена. Внесені зміни в цілому не впливають на результати розробки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кіберзлочинність в Україні. Ера цифрових технологій - ера нових злочинів. Електронний ресурс. -2021.- Режим доступу: https://uz.ligazakon.ua/ua/magazine_article/EA013606

2. Закон України "Про основні засади забезпечення кібербезпеки України". Електронний ресурс. -2021.- Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Report Covid-19 Cyberattack Analysis. Електронний ресурс. -2021.- Режим доступу: https://go.cynet.com/covid-19-cyberattack-analysis?utm_source=thn

4. Jump in cyberattack during COVID-19 confinement https://www.swissinfo.ch/eng/jump-in-cyber-attacks-during-covid-19-confinement/45818794

5. COVID-19 related scams - news and resources. Електронний ресурс. -2021.- Режим доступу: https://www.actionfraud.police.uk/covid19

6. ENISA Treat Landscape 2021. Електронний ресурс. -2021.- Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

7. Кіберзахист для CFO: 10 трендів + 10 рекомендацій -2020.- Режим доступу: https://www.bdo.ua.ru-ru/blog/consulting/march-2020/cybersecurity--for-ceo

8. Оцінка стану комунікації, координації та взаємодії між суб'єктами національної системи кібербезпеки. Електронний ресурс. -2020.- Режим доступу: https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.rnbo.gov.ua/files/2021/STRATEGIYA%2520KYBERBEZPEKI/analityka.pdf&ved=2ahUKEwjN8P6To771AhUdCRAIHdosB6YQFnoECAUQAQ&usg=AOvVaw3GO12UiyhAUW6zaRbQChcf

9. SANS institute security awareness report 2017. Електронний ресурс. -2017.- Режим доступу: https://securingthehuman.sans.org/resources/reports-and-case- studies.

10. 19 gamification trends for 2021-2025. Top stats, facts, examples. Електронний ресурс. -2021.- Режим доступу: https://www.growthengineering.co.uk/19-gamification-trends-for-2021-2025-top-stats-facts-examples/

11. NIST SP 800-50 Електронний ресурс. -2003.- Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

12. НД ТЗІ 1.1-003-99 Електронний ресурс. -1999.- Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343

13. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д. П. Пілова - Дніпро: Національний технічний університет "Дніпровська політехніка", 2019;

14. Державний стандарт України. ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання») / [На заміну ДСТУ 3008-95; чинний від 2017-07-01].- Київ: ДП «УкрНДНЦ», 2016. 31 с. URL: http://www.knmu.kharkov.ua /attachments/3659_3008-2015.PDF;

15. Державний стандарт України. ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання" URL: http://lib.npu.edu.ua/files/dstu-8302-2015.pdf (дата звернення 10. 04. 2017).

16. Стандарти з інформації, бібліотечної і видавничої справи. URL: http://wwvv.library.univ.kiev.ua/ukr/about/dstu.html (дата звернення 3. 04.2017).

17. ДСТУ ISO 5807:2016 Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів (ISO 5807:1985, IDT);

18. Положення про систему запобігання та виявлення плагіату в Національному технічному університеті «Дніпровська політехніка», затвердженого Вченою радою 13.06.2018, протокол №8.

ДОДАТОК А Перелік матеріалів на електронному носіїв

1. Кваліфікаційна робота - Тітов Дмитро 125м-20-2.docx

2. Презентація - Тітов Дмитро 125м-20-2.pptx

3. Додаток Д - Анкета.docx

ДОДАТОК Б. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	21	
6	А4	Розробка програми підвищення обізнаності персоналу у питаннях інформаційної безпеки	14	
	А4	Розробка програми підвищення обізнаності в питаннях кібербезпеки персоналу "Кредит-легко"	19	
7	А4	Економічна частина	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Перелік матеріалів на електронному носії	1	
11	А4	Додаток Б Відгук керівника кваліфікаційної роботи	1	
12	А4	Додаток В. Відомість матеріалів кваліфікаційної роботи	1	
13	А4	Додаток Г Відгук керівника економічного розділу	1	

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ доц. Пілова Д.П

ДОДАТОК Г.
Відгук керівника кваліфікаційної роботи
В І Д Г У К
на кваліфікаційну роботу магістра групи 125м-20-2
Тітова Дмитра Сергійовича
на тему: «Підвищення рівня обізнаності співробітників підприємства з питань кібербезпеки з використанням методів гейміфікації »

Пояснювальна записка складається зі вступу, чотирьох розділів і висновків, викладених на 73 сторінках.

Метою кваліфікаційної роботи є формування достатнього рівня обізнаності персоналу з питань кібербезпеки з застосуванням методів гейміфікації.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: розглянуто існуючі методи підвищення обізнаності персоналу, було виділено метод гейміфікації; представлено рекомендації щодо створення програми навчання з ІТ-безпеки організації; виконано обстеження ОІД; розроблено програму підвищення обізнаності персоналу.

Практичне значення результатів кваліфікаційної роботи полягає у формуванні достатнього рівня обізнаності персоналу з питань кібербезпеки з застосуванням методів гейміфікації, за рахунок розробки та впровадження програми навчання.

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

За час дипломування Тітов Д.С. проявив 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 виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки _80 (добре)__.

Керівник кваліфікаційної роботи **Кагадій Т.С.**

Керівник спец. розділу **Тимофєєв Д. С.**

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ доц. Пілова Д.П

ДОДАТОК Г.
Відгук керівника кваліфікаційної роботи
В І Д Г У К
на кваліфікаційну роботу магістра групи 125м-20-2
Тітова Дмитра Сергійовича
на тему: «Підвищення рівня обізнаності співробітників підприємства з питань кібербезпеки з використанням методів гейміфікації »

Пояснювальна записка складається зі вступу, чотирьох розділів і висновків, викладених на сторінках.

Метою кваліфікаційної роботи є формування достатнього рівня обізнаності персоналу з питань кібербезпеки з застосуванням методів гейміфікації.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: розглянуто існуючі методи підвищення обізнаності персоналу, було виділено метод гейміфікації; представлено рекомендації щодо створення програми навчання з ІТ-безпеки організації; виконано обстеження ОІД; розроблено програму підвищення обізнаності персоналу.

Практичне значення результатів кваліфікаційної роботи полягає у формуванні достатнього рівня обізнаності персоналу з питань кібербезпеки з застосуванням методів гейміфікації, за рахунок розробки та впровадження програми навчання.

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

За час дипломування Тітов Д.С. проявив 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 виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки _80 (добре)__.

Керівник кваліфікаційної роботи **Кагадій Т.С.**

Керівник спец. розділу **Тимофєєв Д. С.**

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ доц. Пілова Д.П