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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Середняк Катерини Олександрівни*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-комунікаційної системи закладу дистанційної освіти «GoITeens»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Корченко А.О.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	93	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Середняк Катерині Олександрівні* **академічної групи** *125-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Політика безпеки інформації інформаційно-комунікаційної системи закладу дистанційної освіти «GoITeens»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 р. № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Визначити стан питання, провести обстеження ІКС, розробити модель порушника та аналіз кіберзагроз	15.03.2024
Розділ 2	Провести оцінку існуючих елементів політики безпеки, обґрунтувати модель безпеки, розробити елементи політики безпеки та встановити заходи реалізації	10.05.2024
Розділ 3	Виконати техніко-економічне обґрунтування доцільності запровадження політики безпеки підприємства	11.06.2024

Завдання видано _____ _____
(підпис керівника) (ім'я, прізвище)

Дата видачі: 01.04.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Катерина СЕРЕДНЯК
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 82 с., 1 рис., 12 табл., 5 додатків, 13 джерел.

Об'єкт розробки: інформаційно-комунікаційна система закладу дистанційної освіти ТОВ «GoITeens».

Предмет розробки: елементи політики безпеки інформації інформаційно-комунікаційної системи закладу дистанційної освіти ТОВ «GoITeens».

Мета кваліфікаційної роботи: забезпечення достатнього рівня захисту інформації у інформаційно-комунікаційній системі підприємства.

У першому кваліфікаційної роботи розділі було визначено стан питання, розповідається про загальні відомості організації, а саме дослідження фізичного середовища, обстеження обчислювальної системи, інформаційного середовища та середовища користувачів. Розповідається про обґрунтування необхідності створення комплексної системи захисту інформації. Виконано обстеження інформаційно-комунікаційної системи, розроблено модель порушника, проведено аналіз кіберзагроз в розглянутій інформаційно-комунікаційній системі.

У другому розділі була проведена оцінка існуючих елементів політики безпеки на підприємстві та обґрунтована модель безпеки на теперішній час. Були зазначені особливості інформаційно-комунікаційної системи, розроблено порівняльний аналіз базових популярних моделей безпеки з висновком у вигляді обраної моделі. Була виконана розробка елементів політики безпеки, що включає в себе: керування обліковими записами, ідентифікація та автентифікація, розмежування доступу, антивірусний захист та використання власного обладнання. Також були розроблені заходи реалізації цієї політики.

У третьому розділі була визначена економічна ефективність та виконано техніко-економічне обґрунтування доцільності запровадження політики безпеки підприємства.

ПОЛІТИКА БЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ХМАРНІ СЕРЕДОВИЩА, ІНФОРМАЦІЙНА СИСТЕМА.

ABSTRACT

Explanatory note: 82 pp., 1 pic., 12 table, 5 app, 13 sources.

Object of development: information and communication system of distance education institution "GoITeens" LLC.

The subject of development: elements of the information security policy of the information and communication system of the distance education institution «GoITeens» LLC.

The purpose of the qualification work: ensuring a sufficient level of information protection in the information and communication system of the enterprise.

In the first section of the qualification work, the status of the issue was determined, the general information of the organization is described, namely the study of the physical environment, examination of the computer system, information environment and user environment. The rationale for the need to create a comprehensive information protection system is discussed. An inspection of the information and communication system was carried out, a model of the offender was developed, and an analysis of cyber threats in the considered information and communication system was carried out.

In the second section, an assessment of the existing elements of the company's security policy and a justified security model for the present time were carried out. Features of the information and communication system were noted, a comparative analysis of basic popular security models was developed with a conclusion in the form of the selected model. Security policy elements were developed, including: account management, identification and authentication, access restrictions, anti-virus protection, and proprietary hardware. Measures to implement this policy were also developed.

In the third section, the economic efficiency was determined and the technical and economic justification of the feasibility of introducing the company's security policy was performed.

SECURITY POLICY, INFORMATION PROTECTION, THREAT MODEL, VIOLATOR'S MODEL, CLOUD ENVIRONMENTS, INFORMATION SYSTEM.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
ДСТУ	–	державний стандарт України;
ІКС	–	інформаційно-комунікаційна система;
ІТ	–	інформаційні технології;
ІТС	–	інформаційно-комунікаційна система;
КСЗІ	–	комплексна система захисту інформації;
НД ТЗІ	–	нормативний документ технічного захисту інформації;
НСД	–	несанкціонований доступ;
ОС	–	операційна система;
ПБ	–	політика безпеки;
ПБІ	–	політика безпеки інформації;
ПЗ	–	програмне забезпечення;
ТОВ	–	товариство з обмеженою відповідальністю.

ЗМІСТ

с.

ВСТУП

У наш час сучасні технології надають неймовірні можливості для користування вебсайтами, мобільними додатками та іншими онлайн сервісами, а також для створення та ведення цілих бізнесів, які приносять значний дохід саме завдяки мережі Інтернет. Електронна комерція приваблює величезну кількість користувачів, що використовують свої особисті та фінансові дані для здійснення покупок і транзакцій. Очевидно, що такі ресурси стають справжніми магнітами для кіберзлочинців, особливо якщо не забезпечити належний захист та не впровадити ефективні стратегії безпеки. Іншими словами, без належної кібербезпеки неможливо бути впевненим у тому, що ваша особиста інформація залишиться лише вашою, а не стане здобиччю злочинців.

Особливої уваги заслуговує саме онлайн-бізнес, оскільки в ньому може циркулювати необмежена кількість як особистої, так і фінансової приватної інформації. Підприємства повинні приділяти максимальну увагу захисту даних своїх користувачів та клієнтів, щоб запобігти їх викраденню та неправильному використанню. Впровадження надійних засобів захисту та розробка стратегій кібербезпеки стають ключовими елементами успішного функціонування будь-якого онлайн-бізнесу. Без цих заходів ризики втрати інформації або фінансових ресурсів значно зростають, що може призвести до серйозних наслідків як для бізнесу, так і для його клієнтів. [2]

Це також стосується і закладів дистанційної освіти, які щороку набувають все більшої популярності. Протягом останніх п'яти років значна кількість людей обирає саме онлайн формат навчання та роботи. З розвитком цієї діяльності інформаційно-комунікаційні системи стають привабливими цілями для кіберзлочинців і потребують надійного захисту інформації. Вони обробляють великий обсяг конфіденційної інформації, включаючи персональні дані студентів і викладачів, академічні результати та фінансові дані. Захист цієї інформації є критично важливим для забезпечення конфіденційності та цілісності освітнього і робочого процесів. Дистанційна освіта, зокрема онлайн-курси, демонструє безпрецедентне зростання популярності завдяки своїй гнучкості, доступності та

можливості залучення широкої аудиторії. Проте, поряд із позитивними аспектами, виникають і нові виклики, пов'язані з безпекою інформації.

Метою кваліфікаційної роботи є розробка політики безпеки інформації у закладі дистанційної освіти. Політика безпеки інформації є критично важливою для будь-якої організації, оскільки допомагає захистити її інформаційні активи, забезпечити безперервність бізнесу та знизити ризики втрати даних або фінансових збитків унаслідок кіберзлочинів, вона необхідна для забезпечення захисту інформаційних ресурсів організації від різноманітних загроз та ризиків та служить основою для управління безпекою інформації та формує структуру, в якій організація може ефективно захищати свої дані.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство «GoITeens»

GoITeens — недержавний навчальний заклад, який спеціалізується на наданні IT-освіти дітям від 7 до 17 років. Заснований у 2015 році, GoITeens є частиною продуктової EdTech компанії GoIT, яка надає сучасні освітні послуги у сфері інформаційних технологій. Навчальний заклад використовує проектний підхід у навчанні, що дозволяє дітям отримувати практичні знання та навички. Крім технічних знань, учні також мають обов'язкові заняття з soft skills, що сприяє розвитку комунікаційних та лідерських якостей.

На початку своєї діяльності GoITeens навчав виключно дітей співробітників IT-компаній, працював офлайн на вихідних і не був окремим проектом, а входив до складу GoIT. У 2019 році було розроблено курс з програмування для дітей від 9 років, який навчає блокового програмування, що робить процес навчання більш доступним і цікавим для молодших учнів.

У 2020 році через пандемію коронавірусу були закриті всі офлайн-філіали, і заклад повністю перейшов до онлайн-формату навчання. Це дозволило продовжити навчальний процес, незалежно від обмежень, пов'язаних із пандемією, і забезпечити безпеку учнів та викладачів. Онлайн-формат також надав можливість долучити до навчання дітей з різних регіонів України та інших країн. У лютому 2022 року, попри початок повномасштабного вторгнення в Україну, GoITeens продовжив проводити заняття. Заклад заснував фонд для підтримки навчання студентів, які тимчасово не можуть платити за подальше навчання, що стало важливим кроком для забезпечення безперервності освітнього процесу в складних умовах. [4]

У лютому 2023 року GoITeens організував марафон у Roblox, де діти мали можливість побудувати Україну майбутнього. Цей захід привернув увагу понад 10 тисяч дітей і отримав підтримку від таких компаній, як monobank, robota.ua, ЛУН, Сільпо та Uklon. GoITeens також активно співпрацює з різними партнерами та проводить численні заходи, спрямовані на популяризацію IT-освіти серед молоді. [3]

1.2 Обґрунтування необхідності створення КСЗІ

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» вимагає від підприємств, що працюють з інформаційними системами, впровадження заходів для забезпечення безпеки інформації. Невиконання цих вимог може призвести до штрафів, санкцій та втрати ліцензій. [5]

Особливо важливим документом у контексті України є НД ТЗІ 3.7-003-05, що є нормативним документом з технічного захисту інформації. Цей документ визначає вимоги щодо створення, впровадження та підтримання КСЗІ на підприємствах та організаціях. Відповідність цим вимогам є обов'язковою для забезпечення надійного захисту інформації та виконання державних стандартів.

Згідно до цього нормативного документу підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Впровадження КСЗІ, відповідно до вимог НД ТЗІ 3.7-003-05, дозволяє підприємству не лише дотримуватися нормативних актів, а й створити ефективну систему захисту інформації, що відповідає найкращим міжнародним практикам. Це забезпечує комплексний підхід до захисту інформації та підтримання високого рівня безпеки у всіх аспектах діяльності підприємства.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або

забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ. [6]

У системі, що розглядається, зберігається та обробляється інформація з обмеженим доступом. Це включає конфіденційні дані, такі як персональні дані користувачів, фінансова інформація, записи відеодзвінків з клієнтами та послуги, що надаються платно у вигляді конспектів чи презентацій, які потребують підвищеного рівня захисту. Відповідно до законодавства України, зокрема Закону «Про захист інформації в інформаційно-телекомунікаційних системах» та відповідних нормативно-правових документів (НД ТЗІ), ця інформація повинна оброблятися з дотриманням спеціальних вимог безпеки.

Керівництвом системи було прийняте рішення щодо доцільності створення КСЗІ, оскільки запровадження КСЗІ дозволяє забезпечити цілісність, конфіденційність та доступність інформації, що є критично важливими аспектами для будь-якої інформаційної системи.

1.3 Обстеження ІКС

Інформаційно-комунікаційна система (ІКС) підприємства GoITeens забезпечує ефективне та безперебійне функціонування онлайн-платформи та курсів для надання високоякісних освітніх послуг у сфері програмування для підлітків. Система повинна підтримувати інтерактивне навчання, адміністрування, комунікацію між викладачами та студентами, а також забезпечувати надійність, безпеку та доступність інформаційних ресурсів.

Завдання, що виконує ІКС:

1. Забезпечення платформи для проведення онлайн-уроків у реальному часі.

2. Інтеграція з системами управління навчальним контентом (LMS) для розміщення, організації та надання доступу до навчальних матеріалів.

3. Автоматизація процесів реєстрації студентів на курси, розподілу груп та моніторингу успішності навчання, здійснення контролю за відвідуваністю, виконанням домашніх завдань та іншими навчальними активностями.

4. Забезпечення безпечного зберігання особистих даних студентів, викладачів та адміністрації.

5. Обробка та аналіз даних для підвищення якості навчального процесу та прийняття управлінських рішень.

6. Збір та аналіз статистичних даних про успішність навчання, відвідуваність та інші показники.

7. Генерація звітів для адміністрації, викладачів та інших зацікавлених сторін для покращення якості навчального процесу.

Мобільність працівників не обмежується лише можливістю працювати з дому. Співробітники можуть виконувати свої обов'язки в кафе, бібліотеках, коворкінг-просторах або будь-яких інших громадських місцях, які мають доступ до інтернету. Такий підхід сприяє створенню комфортного та продуктивного робочого середовища, що враховує індивідуальні потреби та уподобання кожного працівника.

1.3.1 Фізичне середовище

У сучасних умовах цифрової ери багато підприємств обирають моделі роботи, які не передбачають наявності традиційного фізичного офісу. Одним із таких підприємств є заклад дистанційної освіти «GoITeens», де основний акцент зроблено на гнучкість робочого графіку та мобільності працівників, які можуть виконувати свої обов'язки з будь-якого місця, маючи доступ до інтернету, та працювати зі своїх власних пристроїв. Такий спосіб використання пристроїв є важливим аспектом організації роботи підприємства. Це дозволяє співробітникам мати доступ до робочих ресурсів у будь-який час і з будь-якого місця, що значно підвищує ефективність і гнучкість бізнес-процесів. Крім того, такий підхід зменшує витрати на обладнання та обслуговування робочих місць, що є економічно вигідним для підприємства.

Незважаючи на відсутність центрального офісу, підприємство орендує невеликі офіси у великих містах країни. Ці офіси виконують роль хабів, де співробітники можуть збиратися для проведення робочих зустрічей, нарад, тренінгів та інших заходів, що вимагають фізичної присутності. Наявність таких офісів забезпечує можливість особистої взаємодії між працівниками, що є важливим елементом для підтримання корпоративної культури та командного духу. Наявність невеликих офісів та вільного фізичного перебування дозволяє уникати проблеми з відсутністю енергоживлення внаслідок воєнних дій в країні, тому працівники без труднощів можуть змінити своє фізичне положення та переміститись до пунктів незламності, де завжди присутні генератори та світло.

1.3.2 Обчислювальна система

При роботі навчального процесу ІКС на підприємстві використовуються лише хмарні сервіси, до них відносяться саме наступні: YouTube, Zoom, Slack, Google Таблиці, Kahoot, Google Диск, Notion, Telegram, Google Meet, LMS та навчальні програми.

Процес розділяється між такими робочими місцями: викладачі, менеджери, методисти та розробники, адміністратори платформи, а також студенти. З цих робочих місць можна виділити більш стабільну та варіативну частини. До стабільної можна віднести посаду менеджера, що відповідає за проведення пробних уроків із клієнтами через сервіс Zoom, за запуск нової групи студентів при її старті навчання, створення відповідного чату у соціальній мережі Telegram, також відповідає за створення зустрічей у календарі на платформі Google Meet, утворює розмежування доступу в LMS, в якому відбувається процес навчання та взаємодія між викладачем та студентом, фіксує всі зміни щодо групи у відповідних Google Таблицях, завантажує записи занять учнів до YouTube, та вирішує проблемні моменти з клієнтами стосовно оплати та інших можливих ситуацій через спеціальний чат-бот у Telegram.

Також до фіксованого робочого місця відноситься адміністратор платформи LMS, до обов'язків якого входить забезпечення та підтримка

безперебійної праці цієї платформи. Він працює над тим, щоб всі процеси між студентами та викладачами виконувались без проблем, вся циркулююча інформація не втрачала конфіденційності і не підлягала будь-якому несанкціонованому витоку. Всі учбові матеріали, що узгоджує або виправляє методист, адміністратор завантажує на платформу та контролює, щоб доступ до них мали лише ті студенти та викладачі, яким це необхідно, виходячи з обраного курсу та обов'язків.

Ще одним стабільним робочим місцем можна вважати методиста та розробників курсів, що працюють над створенням унікальних учбових матеріалів, які використовуються під час навчання студентів. Саме вони відповідають за всі навчальні матеріали з курсів на підприємстві. Розробники працюють саме з навчальними програмами, в яких навчаються студенти, тобто розробляють завдання, презентації та інші інтерактивні вправи, наприклад в середовищі Kahoot, на основі цих програм. Всі чернові варіанти уроків відправляються до спеціальної Google Таблиці, в якій методист все перевіряє, приймає рішення щодо виконаних вимог та виносить ці уроки як готові до роботи викладачам.

Менш стабільними, тобто варіативними робочими місцями, можна назвати викладачів, оскільки вони можуть постійно змінюватись. Іншими словами, кожен викладач обирає сам для себе бажані групи, які підходять під його графік. Також, вони можуть змінити курс викладання і перейти на зовсім інший, проходячи перед цим відповідну перевірку на необхідні знання. Викладач відповідає за проведення занять студентам, слідуючи відповідному курсу. В його обов'язок входить перевіряти домашні завдання студентів, починати запис заняття у середовищі Google Meet, провести урок, враховуючи всі вимоги та дотримуючись структури, під кінець провести гру-вікторину на платформі Kahoot, та після закінчення зупинити запис, відмітити відвідуваність студентів на платформі LMS і надіслати підсумки заняття до чату зі студентами у Telegram. Викладачі мають необмежений у часі доступ до курсів, що вони викладають, які знаходяться у Google Таблицях та Диску.

Останнє робоче варіативне місце – студенти. Воно вважається таким через можливу нестабільність у навчанні. В будь-який момент клієнт має можливість відмовитись від курсу, змінити напрямок, графік або навіть викладача. Також після завершення курсу вони просто залишають ІКС і дуже рідко затримуються, тому неможливо віднести таке робоче місце до стабільної частини. Студенти відвідують заняття, що проводить викладач у Google Meet, працюючи у необхідній навчальній програмі, здають домашні роботи до учбової платформи LMS, комунікують у поза учбовий час з викладачем чи менеджером у Telegram.

Як правило, типовими пристроями, з яких відбуваються процеси, є портативний комп'ютер або ноутбук, винятком для викладача та студента може бути планшет, якщо курс націлений саме на роботі з планшету. Зазвичай операційна система використовується Windows, а саме Windows 10 або 11, але також використовуватись може ОС від MacOS.

ІКС навчального процесу на підприємстві зображено на рис. 1.1.

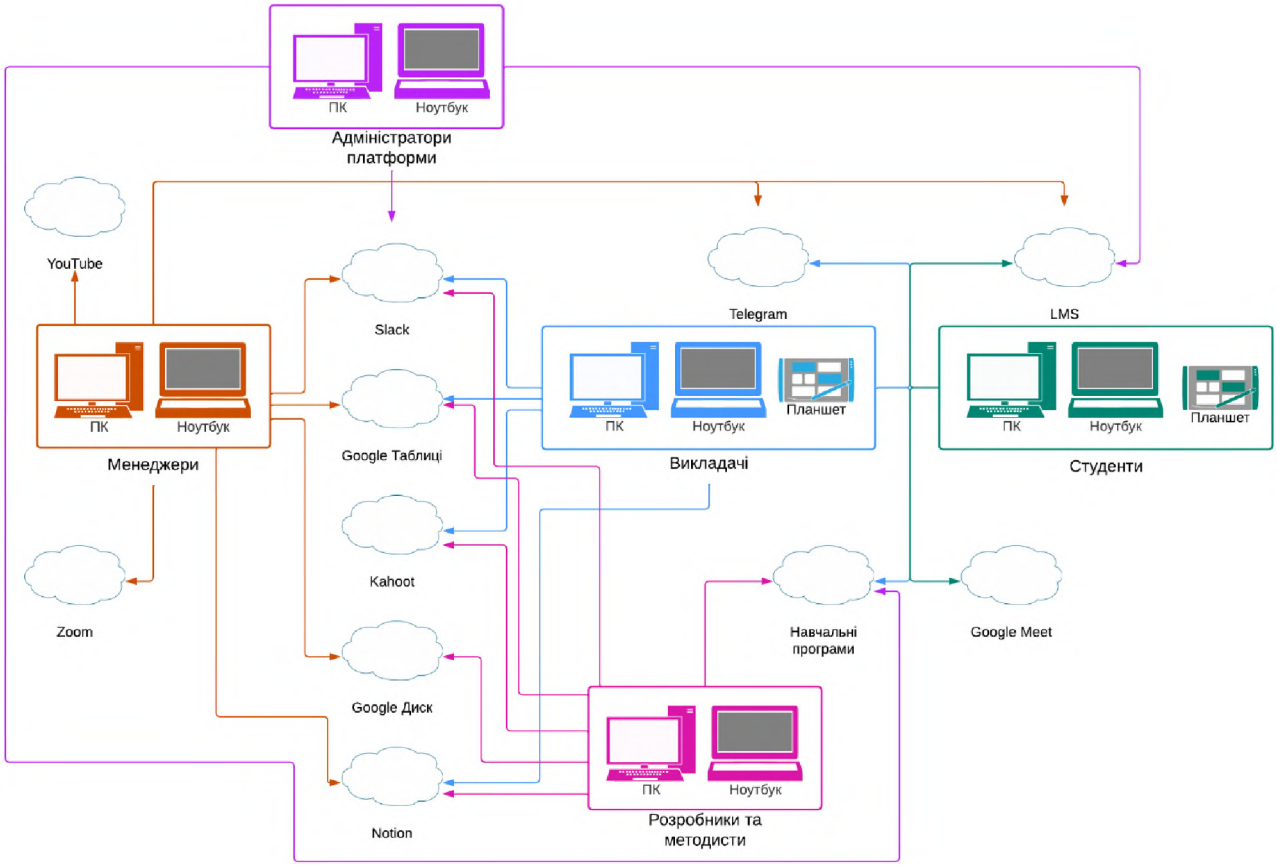

Рисунок 1.1 – Структурна схема обчислювальної системи

1.3.3 Інформаційне середовище

У ІКС циркулює та обробляється така інформація, що пов'язана з учбовим процесом: записи занять, конспекти уроків, домашні роботи, оцінки, навчальні презентації, списки груп учнів, відвідуваність, чернові варіанти курсів, методичні рекомендації. Вся інформація зберігається на хмарних платформах, а саме: LMS, Slack, Google Таблиці, Google Диск, Notion, YouTube. Доступ до всіх платформ відбувається на основі логіну та паролю. Кожен робітник має свій рівень доступу до інформації.

Всі матеріали курсів зберігаються в декількох місцях. По-перше, вони розміщені на учбовій платформі (LMS), тобто там, де працюють викладачі та навчаються студенти. Вони можуть переглядати вміст тільки свого курсу, до всіх інших доступ закритий. Цей процес ретельно контролюється менеджерами та адміністраторами, саме вони утворюють розмежування доступу та можуть вносити зміни на платформі. Також на платформі можна відстежити скільки і які учні присвоєні до групи. Процес присвоєння до групи утворюється спеціально згенерованим посиланням, яке автоматично записує на курс людину після її реєстрації. Кожен курс розділений на семестри, на платформі розмежування застосовується саме на них, тобто на кожен семестр курсу треба окремо записувати як студентів, так і викладача. Якщо один семестр підходить до кінця, то викладачу варто докласти це менеджеру, щоб він відкрив доступ до наступного всім необхідним людям. Тобто надавання доступу узгоджується заздалегідь за запитом. Також на платформі учням відкриваються конспекти поступово, з кожним пройденим заняттям стає доступним новий конспект. Це зроблено, по-перше, щоб якась дуже хитра людина не вкрала конспекти всього семестру і одразу пішла, не продовжуючи платити, а по-друге, щоб ніхто з дітей не зробив купу завдань заздалегідь, бо йому було сумно і він захотів зробити роботу наперед, а на уроці нічого не робити.

Окрім платформи, де зберігаються матеріали курсу для учнів, вони зберігаються також у хмарних середовищах. Звісно, що методист контролює свій курс і зберігає матеріали у себе в хмарі або на пристрої, але також вони

знаходяться окремо для викладачів в Google Таблиці. Приклад даної таблиці знаходиться у додатку Б. Така таблиця розділена на вкладки, в кожній вкладці зберігається по одному курсу відповідно. Доступ до вкладки мають лише ті викладачі, які ведуть курс, до інших він доступу не має. Вони можуть лише переглядати інформацію, вносити зміни вони не зможуть, лише читати та вносити коментарі. Для такого розмежування доступу використовуються власні електронні пошти робітників, які вони при вступі на роботу повідомили компанії. За допомогою такої таблички викладачі можуть ознайомитися з навчальною програмою, заздалегідь готуватись до занять та використовувати допоміжні матеріали.

Коли розробляються матеріали курсу та заняття, існує окрема Google Таблиця, доступ до якої мають лише розробники. Вони можуть редагувати таблицю, вставляючи свої розробки на перевірку. Лише після перевірок та внесення певних змін від наказів методиста, готовий матеріал групується та виставляється викладачам, голосно повідомляючи про внесення змін в таблиці. Повідомляють всю цю інформацію викладачам їх тім ліди.

Таблиця 1.1 – Класифікація інформації

№	Вид інформації	Місце зберігання	Вид представлення	Правовий режим	Режим доступу
1.	Записи занять	LMS	Відео, звуковий	Конфіденційна	Обмежений доступ
		Google Диск			
		YouTube			
2.	Конспекти уроків	LMS	Текстова, графічна, таблична, відео	Конфіденційна	Обмежений доступ
		Google Таблиці			
		Notion			

Продовження таблиці 1.1

№	Вид інформації	Місце зберігання	Вид представлення	Правовий режим	Режим доступу
3.	Домашні роботи	LMS	Текстова, графічна, звукова, відео	Конфіденційна	Обмежений доступ
4.	Оцінки	LMS	Таблична, текстова	Конфіденційна	Обмежений доступ
5.	Презентації уроків	Google Диск Google Таблиці	Текстова, графічна, відео	Конфіденційна	Обмежений доступ
6.	Списки груп учнів	LMS Google Таблиці	Таблична, текстова	Службова	Обмежений доступ
7.	Відвідуваність	LMS Google Таблиці	Таблична, текстова	Конфіденційна	Обмежений доступ
8.	Чернові варіанти курсів	Google Таблиці Notion	Текстова, таблична, графічна, відео	Службова	Обмежений доступ
9.	Методична документація	Notion	Текстова, таблична, графічна, звукова, відео	Службова	Обмежений доступ

1.3.4 Технологія обробки інформації

Для початку отримання бажаного курсу, клієнт вказує свій номер на сайті, щоб з ним могли зв'язатися для подальшої співпраці. Під час телефонної розмови клієнту пояснюється, як відбувається весь процес навчання, надається детальна інформація і задаються відповідні питання. Це дозволяє підібрати необхідний курс, враховуючи вік, інтереси та рівень клієнта, якщо він ще не визначився з вибором. У разі успішного завершення розмови та згоди клієнта на умови і ціну, його передають до відділу пробних занять. Для проведення пробного уроку обирається зручний час та день, надається вся інформація та інструкції щодо встановлення програмного забезпечення, яке буде використовуватися під час навчання. Пробний урок допомагає клієнту оцінити курс і процес навчання, а також визначити відповідний рівень знань і оптимальний формат занять. Одночасно здійснюється оцінка здібностей клієнта, щоб зрозуміти, який підтип курсу (легкий чи звичайний) йому підходить і як краще займатися – у групі чи індивідуально з викладачем. Також формується перше враження від навчання, що впливає на рішення клієнта про готовність оплатити курс.

Якщо клієнт задоволений пробним уроком і готовий почати навчання, його включають до списку на старт групи. Групи всіх курсів стартують щомісяця в певні дати. Це дозволяє набрати необхідну кількість викладачів та менеджерів, а також забезпечити точні часові проміжки для початку навчання, щоб очікування клієнтів не було занадто довгим. Перед стартом навчання відповідальний менеджер створює чат-групу в Telegram, де додає всіх учнів та викладачів. У цій групі надається вся необхідна інформація про подальший процес навчання, інструкції щодо логінів і паролів, встановлення програм, реєстрації на навчальній платформі. На платформі будуть зберігатися записи уроків, конспекти курсу і подаватися домашні завдання. Навчання стартує з основного технічного курсу, а також додатково включає уроки з розвитку софт-навичок. Ці уроки спрямовані на розвиток командної роботи та впевненості у собі. Технічні та софт-уроки проводять різні викладачі. Такий підхід забезпечує всебічний розвиток студентів і підготовку їх до майбутніх викликів у професійній діяльності.

1.3.5 Середовище користувачів

Важливою керуючою посадою, що відповідає за матеріали курсів, є *методист*. Робота методиста полягає в тому, що він проектує курс як учбовий процес. Він будує траєкторію навчання та робить все можливе для комфортного проходження курсу і досягання запланованого результату. На основі його траєкторії і планів розробники курсів чітко розуміють що саме за матеріал їм треба розробити, які умови існують та теми. Рівень кваліфікації як користувача системи – середній.

Якщо продовжувати розмову про розробників, то їх можна розділити на дві категорії, а саме це *розробники курсів* та *розробники платформи LMS (адміністратори)*, на якій ці курси проводяться та навчаються клієнти. Про перших розробників вже дізнались інформацію, вони на основі певного плану та траєкторії від методиста створюють відповідні конспекти з завданнями тощо, які потім узгоджують з ним та вносять правки до тих пір, поки не буде все ідеально для зручного навчання. Другі розробники, які відповідають за платформу, на початку створювали її, враховуючи всі побажання від співпрацівників, які будуть на цій платформі працювати, та після її створення пильно слідкують за коректною роботою кожного дня, вносячи час від часу певні зміни, такі як нові можливості або виправлення різних багів. Рівень кваліфікації розробника курсів як користувача системи – середній, а розробника платформи – високий.

Далі у переліку йдуть *викладачі курсів*. Задача викладача – знати досконально програму, яку викладає клієнтам. Він має необхідний графік, по якому проводяться заняття, тому для цього йому необхідно за півгодини до початку перевірити всі домашні роботи. Доєднатися до дзвінка, підготувати всі необхідні матеріали, впустити всіх студентів з групи, поставити запис заняття, провести урок та вимкнути запис заняття. Після цього йому необхідно в чат з групою виписати підсумки уроку та зробити звіт з проведеного уроку за допомогою спеціальної форми, щоб потім заняття зарахувалось в зарплатню. Рівень кваліфікації як користувача системи – середній.

Менеджер повинен тримати зв'язок з клієнтами, домовлятися про продовження навчання та оплати курсу, на старті навчання формує групу та надає всю інформацію та інструкції, знайомить з основними необхідними пунктами для початку навчання, кожен запис заняття менеджер завантажує на платформу, щоб у клієнтів завжди була можливість передивитися його, утворює розмежування доступу між студентами та викладачем, а також формує зустрічі в календарі. Рівень кваліфікації як користувача системи – середній.

Останнім користувачем виступає *студент*. В обов'язки студента входить відвідувати заняття за необхідним графіком, виконувати всі необхідні завдання та відправляти їх на перевірку. Якщо виникає ситуація, коли не виходить доєднатись до уроку, то необхідно проінформувати про це та потім продивитися запис заняття, щоб не відставати від учбового процесу та інших учнів, якщо навчання відбувається в групі, або попросити створити перенос заняття на інших зручний день у викладача та менеджера, якщо це індивідуальний формат навчання. Рівень кваліфікації як користувача системи – низький.

Таблиця 1.2 – Матриця розмежування доступу до інформаційних ресурсів

Користувач	Інформація									Ресурси
	1	2	3	4	5	6	7	8	9	
Методист	Ч, К	Ч, К, В, ЗБ			Ч, К, М, ЗБ	Ч, К	Ч, К	Ч, К, М, ЗБ	Ч, К, В, М, ЗБ	YouTube, Slack, Google Таблиці та Диск, Kahoot, Notion, Навчальні програми
Розробник курсів		Ч, К, ЗБ			Ч, К			Ч, К, М, ЗБ	Ч, К, ЗБ	Slack, Навчальні програми, Google Таблиці та Диск, Kahoot, Notion
Адміністратор платформи	Ч, К, В	Ч, К, ЗБ	Ч, К, В	Ч, К, М, ЗБ		Ч, К, М, ЗБ	Ч, К, М, ЗБ			Slack, Google Диск, LMS
Старший викладач	Ч, К	Ч, К	Ч, К	Ч, К, М,	Ч, К, М, ЗБ	Ч, К	Ч, К, М, ЗБ		Ч, К, ЗБ	LMS, Telegram, Google Meet, Навчальні програми, Slack, Google Таблиці та Диск, Kahoot, Notion, YouTube
Викладач	Ч, К	Ч, К	Ч, К	Ч, К, М	Ч, К, М, ЗБ	Ч, К	Ч, К, М, ЗБ		Ч, К, ЗБ	
Менеджер	Ч, К, В, ЗБ	Ч, К	Ч, К	Ч, К, М, ЗБ	Ч, К	Ч, К, М, ЗБ	Ч, К, М, ЗБ			YouTube, Zoom, Slack, LMS, Google Таблиці та Диск, Notion, Telegram

Продовження таблиці 1.2

Користувач	Інформація									Ресурси
	1	2	3	4	5	6	7	8	9	
Студент	Ч, К	Ч, К	Ч, К, В, ЗБ	Ч, К	Ч, К				Ч, К, ЗБ	Telegram, LMS, Google Meet, Навчальні програми

Ч – читання, К – копіювання, В – видалення, М – модифікація, ЗБ – зберігання

1.4 Модель порушника

Коли існує інформація, що підлягає захисту, будь-то персональні або фінансові дані – завжди знайдеться людина чи навіть група осіб, метою яких буде ознайомитись з цією інформацією, вкрасти її, модифікувати чи навіть просто видалити, щоб репутація підприємства зазнала пониження або з будь-якої іншої власної причини. Таку групу осіб можна назвати порушниками, та щоб запобігти можливому витоку інформації через їх незаконні дії, необхідно побудувати модель порушника. Ця модель буде охоплювати різні критерії, що відповідають саме розглянутій ІКС.

Загалом модель порушника описує ймовірні дії порушника, що складаються на основі аналізу категорії, специфікації за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІКС, можливостями використання засобів та методів подолання системи захисту, а також за часом ті місцем дії. Порушників можна розділити на внутрішніх та зовнішніх по відношенню до ІКС, кожній категорії буде привласнено власне позначення. До внутрішніх порушників відносяться співробітники та користувачі, що можуть наносити шкоду інформаційним ресурсам по випадковій або навмисній причині, та мають доступ до конфіденційної інформації підприємства. Зовнішні порушники навпаки, являються сторонніми особами, та не є теперішніми працівниками, тобто наприклад колишні працівники – можливі зовнішні порушники по відношенню до ІКС.

Модель порушника та всі специфікації наведено у таблицях 1.3-1.9.

Таблиця 1.3. Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІКС		
ПВ1	Клієнти	1

Продовження таблиці 1.3

Позначення	Визначення категорії	Рівень загроз
ПВ2	Співробітники компанії, які можуть мати доступ до конфіденційної інформації	2
ПВ3	Співробітники, що мають повноваження на керування КЗЗ відповідного процесу	3
Зовнішні по відношенню до ІКС		
ПЗ1	Представники організацій, що взаємодіють з питань технічного забезпечення (електропостачання, освітлення, опалення тощо)	1
ПЗ2	Колишні працівники	2
ПЗ3	Представники організацій, що взаємодіють з питань технічного ремонту пристроїв (комп'ютерів, ноутбуків)	2
ПЗ4	Хакери та кіберзлочинці	2
ПЗ5	Конкуренти	3

Таблиця 1.4. Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ5)	4

Таблиця 1.5. Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 1.6. Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може отримувати лише мінімальну інформацію на основі робочих чатів, до яких має доступ	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів)	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.7. Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	1
Ч2	Під час функціонування ІТС (або компонентів системи)	2
Ч3	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	3

Таблиця 1.8. Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Таблиця 1.9. Модель порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Внутрішні порушники по відношенню до ІТС							
Методист	ПВ3	М2	К3	З3	Ч3	Д3	18
	4	2	3	3	3	3	
Розробник курсів	ПВ2	М1	К3	З1	Ч1	Д2	10
	2	1	3	1	1	2	

Продовження таблиці 1.9

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІКС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Адміністратор	ПВ3	М2	К4	З3	Ч3	Д4	20
	4	2	4	3	3	4	
Викладач	ПВ2	М2	К2	З1	Ч3	Д2	12
	2	2	2	1	3	2	
Менеджер	ПВ2	М2	К2	З3	Ч3	Д3	15
	2	2	2	3	3	3	
Старший викладач	ПВ2	М2	К3	З1	Ч3	Д3	14
	2	2	3	1	3	3	
Клієнти	ПВ1	М1	К1	З1	Ч2	Д2	8
	1	1	1	1	2	2	
Зовнішні порушники по відношенню до ІТС							
Спеціалісти з тех. забезпеч.	ПЗ1	М1	К1	З1	Ч3	Д1	8
	1	1	1	1	3	1	
Колишні працівники	ПЗ2	М2	К3	З1	Ч2	Д1	11
	2	2	3	1	2	1	
Спеціалісти з ремонту пр.	ПЗ3	М3	К1	З2	Ч1	Д2	12
	3	3	1	2	1	2	
Хакери та кіберзлочинці	ПЗ4	М3	К2	З4	Ч3	Д3	19
	4	3	2	4	3	3	
Конкуренти	ПЗ5	М4	К4	З4	Ч3	Д4	24
	5	4	4	4	3	4	

Найбільшу загрозу несуть такі ймовірні порушники системи: методист, адміністратор платформи, хакер або кіберзлочинець, агент конкурентів.

1.5 Аналіз кіберзагроз в ІКС

Розглянемо джерела загроз, що можна розділити на: антропогенні зовнішні та внутрішні, техногенні зовнішні та внутрішні, а також стихійні.

Антропогенні зовнішні джерела загроз – це небезпеки, що виникають внаслідок діяльності людини і можуть негативно впливати на безпеку, здоров'я, навколишнє середовище або економічну стабільність об'єкта або регіону. Ці загрози мають зовнішнє походження, тобто їх джерела знаходяться поза межами об'єкта або системи, на яку вони впливають. З іншого боку, антропогенні внутрішні навпаки – виникають внаслідок діяльності людини всередині системи.

Техногенні зовнішні та внутрішні джерела загроз, на відміну від антропогенних, – це небезпеки, що виникають внаслідок технічної діяльності людини та пов'язані з використанням технологій, промислових процесів і обладнання. Розрізняються зовнішні та внутрішні джерела в залежності від того, де саме вони виникають і який об'єкт чи система піддаються ризику.

Останні, стихійні джерела загроз, з’являються внаслідок природних явищ, що негативно впливають на безпеку, здоров’я та навколишнє середовище.

На основі всіх існуючих джерел загроз, можна сформувати певний перелік можливих загроз для системи:

1. Некоректне викладання навчальних матеріалів з боку викладачів, копіювання та модифікація матеріалів без попередження, а також ймовірність нав’язування власної думки або надання сторонньої інформації, що відмінна від складу курсу.

2. Витік інформації матеріалів курсу працівниками, що мають повноваження на читання, а також конкурентами, які можуть купити курс та викрасти матеріали або записи уроків.

3. Взлом кіберзлочинцями чи хакерами працівників компанії, що мають доступ до конфіденційної інформації, що приводить до витоку інформаційних ресурсів.

4. Викладач таємно проводить заняття клієнтам, що не хочуть офіційно записуватись за курс, та за їх думкою переплачувати, через це кількість бажаючих отримувати послуги від підприємства зменшується, а також прибуток.

5. Конкуренти або студенти, що придбали та пройшли курс, що копіюють всі пройдені матеріали та записи занять, а потім діляться ними з іншими сторонніми особами, що також призводить до зменшення кількості клієнтів та прибутку.

6. Кіберзлочинець під виглядом менеджера надсилає посилання на учбову програму не з офіціального сайту, а зі шкідливим ПЗ, що призведе до витоку інформації, або просить виконувати інформаційно-небезпечні для клієнта дії.

7. Витік персональних даних клієнтів через людський фактор чи взлом.

8. Фішингові атаки на клієнтів та працівників.

9. Випадкові або навмисно утворені перебої та технічні проблеми з платформами, навчальними програмами, пристроями тощо.

10. Шахрайства фінансового характеру.

11. Збої, втрата даних або виникнення недостовірної інформації через введення невірних даних та управління системами навмисним або випадковим чином, який базується на людському факторі.

12. Втрата конфіденційної інформації та порушення цілісності даних через помилки при використанні засобів обміну інформацією.

13. Перерви у роботі, втрата даних та затримка у наданні послуг при відмові чи несправності технічних засобів.

14. Ймовірність завантаження та встановлення неофіційного ПЗ для навчального процесу з боку працівників або студентів.

15. Витік інформації з соціальної мережі Telegram, оскільки немає гарантії повного захисту інформаційних ресурсів.

1.6 Висновок першого розділу

На сьогоднішній день заклади дистанційної освіти мають велику популярність, що пов’язана із переходом багатьох учбових процесів на онлайн

формат. В ході таких дій, постає питання з приводу забезпечення безпеки інформаційних ресурсів, що циркулюють на таких підприємствах, оскільки може міститись конфіденційна, службова, персональна та навіть секретна інформація. Таким чином, в першому розділі кваліфікаційної роботи був проведений огляд одного з таких підприємств, що має назву ТОВ «GoITeens».

Перш за все було проведено з'ясовано такий факт, що фізичне середовище в організації відсутнє, тому це призводить до виникнення певних серйозних кіберзагроз, які можуть нанести велику шкоду та призвести до певних втрат та інцидентів, таких як зниження репутації, витік інформації та отримання грошових збитків. Такі кіберзагрози було можливо скласти завдяки розгляду обчислювальної системи, середовища користувачів та інформаційних ресурсів інформаційно-комунікаційної системи підприємства. Загалом кіберзагрози дуже часто пов'язані саме з витоком конфіденційної або персональної інформації, тому терміново необхідно впровадити необхідні дії, що будуть розглянуті у наступному розділі кваліфікаційної роботи.

Також дуже важливим моментом стало розроблення моделі порушника, яка базувалась на певних категоріях та відповідних коефіцієнтах, а також з'ясувала найбільш небезпечних існуючих порушників для підприємства.

Таким чином, результати першого розділу дають змогу розглянути заходи для підвищення безпеки на підприємстві, а саме розробку елементів політики безпеки інформаційно-комунікаційної системи та впровадити заходи їх реалізації.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Оцінка існуючих елементів політики безпеки

На підприємстві впроваджено різноманітні заходи безпеки та встановлено загальні принципи для захисту наших інформаційних активів. Проте, на жаль, ці існуючі елементи не оформлені у вигляді конкретних документів. Відсутність формальної документації є значним недоліком в системі безпеки, яка потребує негайної уваги. Наразі існує кілька неписаних, але практикованих заходів безпеки, таких як контроль доступу, що обмежує доступ до конфіденційних даних залежно від ролей та відповідальностей, а також захист даних та регулярних резервних копій. Однак, без офіційних документів, які б регулювали ці заходи, система безпеки на підприємстві залишається вразливою до ризиків та загроз. Формальна документація забезпечить чітке розуміння та дотримання правил безпеки всіма співробітниками, покращить ефективність заходів безпеки та підвищить загальну стійкість нашої інформаційної системи до можливих атак.

2.2 Обґрунтування моделі безпеки

При побудові системи кібербезпеки надзвичайно важливим є визначення загальних принципів, які базуються на виборі відповідної моделі безпеки. Цей процес вимагає ретельного врахування особливостей конкретної інформаційно-комунікаційної системи, що дозволить обрати найбільш ефективну модель для забезпечення захисту.

Обрана модель безпеки має враховувати унікальні загрози та вразливості, притаманні цій ІКС, а також відповідати загальним стандартам і передовим практикам в галузі кібербезпеки.

2.2.1 Особливості ІКС

1. ІКС підприємства GoITeens розрахована на надання освітніх послуг для дітей та підлітків. Система забезпечує доступ до навчальних матеріалів та ресурсів, адаптованих для юних користувачів. Основною метою є створення

безпечного, зручного та ефективного середовища для навчання, що враховує особливості сприйняття та потреби підлітків. Тобто, безпосередніми користувачами цієї системи є діти різного віку.

2. ІКС спеціалізується на дистанційному навчанні, що включає проведення онлайн-уроків, вебінарів, інтерактивних сесій та інших форм онлайн-взаємодії. Платформа підтримує різноманітні методи подачі матеріалу, включаючи відеоуроки, інтерактивні вправи, форуми для обговорення та індивідуальні консультації. Тобто, система забезпечує можливість подачі різноманітних типів інформації та матеріалів певних видів представлення, що використовує певні платформи.

3. GoITeens не має фізичних навчальних закладів або офісів для проведення занять. Усі освітні процеси відбуваються виключно онлайн через мережу Інтернет. Всі навчальні матеріали, заняття та комунікації проходять у віртуальному середовищі, що забезпечує високу доступність та зручність для учнів. Тобто немає фіксованого фізичного середовища.

4. Через велику кількість учасників навчального процесу, робітників та їхню розподіленість у різних часових зонах і місцях, централізоване управління системою є обмеженим.

5. Система не висуває строгих вимог до пристроїв та програмного забезпечення, які використовуються працівниками та студентами. Викладачі та учні можуть використовувати різноманітні пристрої, включаючи комп'ютери, планшети та смартфони, а також будь-які сучасні веб-браузери. Контролю за версіями та ліцензіями цих продуктів відсутні.

6. Курси, що пропонує GoITeens, мають визначений термін навчання, зазвичай тривалістю від одного до двох років. Однак студенти не зобов’язані залишатися до завершення курсу та можуть покинути навчання в будь-який момент без серйозних наслідків. Тобто в системі існує певна множина користувачів, що регулярно змінюється.

7. GoITeens пропонує широкий спектр освітніх матеріалів та курсів, що охоплюють різні аспекти IT-технологій. До них належать блочне програмування,

основи мов програмування (наприклад, Python, JavaScript), веб-дизайн, розробка мобільних додатків та інші сучасні напрямки.

8. Для залучення нових учнів та підтримки інтересу існуючих клієнтів, GoITeens регулярно організовує безкоштовні марафони, вебінари та інші освітні заходи. Тобто, окрім типових бізнес-процесів існують додаткові процеси, які теж при їх реалізації можуть використовувати елементи ІКС.

2.2.2 Порівняльний аналіз моделей безпеки

Для вибору моделі безпеки проведемо порівняння між такими базовими розповсюдженими моделями безпеки: VPN (віртуальна приватна мережа), SASE (Secure Access Service Edge), нульова довіра, нульове знання, повна довіра, найменш привілейований доступ, поглиблений захист.

1. VPN, virtual private network

Віртуальна приватна мережа захищає всі передачі даних між пристроєм користувача та сервером VPN за допомогою шифрування. Це встановлює захищений канал через загальнодоступний Інтернет, що дозволяє користувачам отримувати доступ до приватних мережевих ресурсів так, ніби вони безпосередньо підключені. Віддалені співробітники часто використовують VPN для доступу до ресурсів компанії та для окремих осіб, які прагнуть захистити свою конфіденційність в Інтернеті.

Слід зазначити, що VPN зазвичай базує безпеку, що орієнтована на мережу, на розташуванні та довірі мережі. Дана модель безпеки може добре підійти віддаленим працівникам, окремим особам або традиційним мережевим середовищам з локальними ресурсами більше підійде саме віртуальна приватна мережа. Очевидною перевагою віртуальної приватної мережі це те, що вона підходить для захисту мережевих периметрів, відпрацьована і широко використовувана технологія, може надавати доступ до широкого спектру мережевих ресурсів. Однак з іншого боку, VPN може знизити продуктивність, таку модель важко налаштувати та використовувати, а також може бути несумісним з усіма пристроями та програмами.

2. SASE, secure access service edge

Периферійний севріс безпечного доступу розроблено, щоб запропонувати безпеку як хмарну службу та забезпечити захист користувачам, де б вони не були. Він забезпечує повний набір компонентів безпеки, включаючи брандмауер, захист від вторгнень, захищений веб-шлюз і брокер безпеки доступу до хмари.

Якщо розглядати підхід до безпеки, то в моделі SASE використовується архітектурний підхід, який поєднує безпеку та мережу в хмарну модель. Організації з фокусом на хмарні сервіси та віддалену роботу часто можуть обирати саме цю модель безпеки, оскільки це рідна хмарна архітектура для масштабованості та гнучкості. Також є брандмауер, захист від вторгнень, безпечний веб-шлюз, CASB тощо.

3. Zero Trust, нульова довіра

Концепція найменших привілеїв передбачає надання користувачам і пристроям лише необхідного доступу, мінімізацію ризиків і запобігання несанкціонованим діям і бічним переміщенням мережі, тобто користувачі отримують доступ лише до тих даних і програм, які їм потрібні для виконання їх роботи.

Модель нульової довіри завжди буде вимагати постійної перевірки та піклуватись про безпеку мережі, саме цей підхід до безпеки використовується. Такий принцип дуже підходить сучасним організаціям з віддаленими співробітниками, хмарними сервісами та мобільними пристроями, а також підприємствам, що хочуть підвищити безпеку, адаптуватися до сучасного робочого середовища та захистити від нових загроз, та яким потрібна комплексна безпеку доступу та захист мережі. Організації обирають саме цю модель, оскільки це покращена безпека з безперервною автентифікацією та мінімальним доступом, краща адаптованість до динамічного робочого середовища, масштабована і хмарна, зменшена поверхня атаки, покращена видимість мережевого трафіку, безперервний моніторинг, доступ з найменшими привілеями, адаптація безпеки для віддалених і орієнтованих на хмару середовищ. Але не варто забувати, що таку модель також буде важко налаштувати

та керувати, може бути дорогим, може вимагати змін у процесах, може бути важко інтегруватися з існуючими системами безпеки, і може вплинути на взаємодію з користувачем, потребує постійного моніторингу.

4. Zero-knowledge, нульове знання

Підтвердження з нульовим знанням передбачає, що одна сторона доводить, що вона володіє певною інформацією, не розкриваючи її перевіряючій стороні, забезпечуючи секретність даних.

Дана модель безпеки покладається на криптографічні методи захисту даних. Обирають принцип нульового знання організації, яким необхідна автентифікація та перевірка даних із збереженням конфіденційності в різних цифрових транзакціях. Перевагою є сильна безпека даних і конфіденційність, підходить для конфіденційних даних, але може не захищати безпосередньо доступ до мережі, обмежений у додатках, крім захисту даних, потрібна криптографічна експертиза.

5. Full trust, повна довіра

Безпека повної довіри передбачає, що можна довіряти всім користувачам і пристроям всередині периметра мережі. Ця модель заснована на ідеї підходу «замок і рів», коли периметр мережі сильно укріплений, а весь трафік перевіряється перед входом або виходом з мережі. Безпека повної довіри – це традиційний підхід до безпеки, який уже не такий ефективний, як колись, через зростання хмарних обчислень, віддаленої роботи та інших сучасних загроз безпеці.

Припускається, що всім користувачам і пристроям у межах периметра мережі можна довіряти. Беруть цю модель за основу саме традиційні організації, які менше зосереджуються на динамічному робочому середовищі та сильно покладаються на мережеву довіру, оскільки саме принцип повної довіри це простота і зручність використання для користувачів і адміністраторів, знижена складність і вартість. З іншого боку, це обмежена адаптованість до сучасних робочих середовищ і віддаленої роботи, потенційна підвищена вразливість до внутрішніх загроз.

6. Least Privileged Access, найменш привілейований доступ

Принцип найменших привілеїв — це інструкція з безпеки, яка полягає в обмеженні дозволів на доступ користувачів і системи до найнеобхіднішого, необхідного для виконання конкретних завдань.

Існує обмеження прав доступу користувачів і системи до необхідного мінімуму, зменшення привілеїв для виконання завдань. Подібний принцип обирають середовища, де застосовується принцип найменших привілеїв. До переваг можна віднести зменшення ризику несанкціонованого доступу та витоку даних, покращений захист від випадкового розкриття даних, спрощений контроль доступу, узгоджений з конкретними посадовими функціями. Якщо виділяти недоліки, то використання найменш привілейованого доступу може призвести до збільшення адміністративних витрат, особливо в організаціях зі складною структурою доступу, зосередження лише на дозволах доступу може не усунути зовнішні загрози чи спроби неавторизованого доступу.

7. Defense-In-Depth, глибокий захист

Поглиблений захист , також відомий як багаторівнева безпека, передбачає використання кількох рівнів безпеки для захисту активів організації. Це забезпечує резервування, тобто якщо один рівень виходить з ладу, інший рівень вмикається, щоб захистити систему.

Глибокий захист покладається на кілька рівнів контролю безпеки, тому традиційні IT-середовища з чітко визначеними периметрами часто зупиняють свій вибір на цьому принципі. Defense-In-Depth забезпечує резервування та стійкість до окремих точок відмови, може використати наявні інвестиції в безпеку, легше реалізувати в традиційних, усталених мережевих архітектурах. З іншого боку, дана модель безпеки покладається на припущення про довіру в певних межах, що робить її сприйнятливою до внутрішніх загроз, може створити хибне відчуття безпеки, якщо не буде реалізовано комплексно на всіх рівнях, може бути неефективною проти передових цілеспрямованих атак. [7]

Об’єднані характеристики всіх моделей зображені на таблиці 2.1.

Таблиця 2.1. Порівняння базових моделей безпеки

№	Характеристика	Назва принципу						
		Zero Trust	VPN	SASE	Zero-knowledge	Full trust	Least Privileged Access	Defense-In-Depth
1.	Підхід до безпеки	Не викликає довіри, вимагає постійної перевірки, безпека мережі	Безпека, орієнтована на мережу, базується на розташуванні та довірі мережі	Поєднує безпеку та мережу в хмарну модель	Безпека даних, конфіденційність	Всім користувачам і пристроям у межах периметра мережі можна довіряти	Обмеження прав доступу користувачів і системи до необхідного мінімуму	Кілька рівнів контролю безпеки
2.	Яким організаціям підходить	З віддаленими співробітниками, хмарними сервісами та мобільними пристроями, які прагнуть захистити від нових загроз	Віддаленим працівникам, окремим особам, традиційним мережевим середовищам з локальними ресурсами	З фокусом на хмарні сервіси та віддалену роботу	Де потрібна автентифікація та перевірка даних із збереженням конфіденційності в різних цифрових транзакціях	Які менше зосереджуються на динамічному робочому середовищі та сильно покладаються на мережеву довіру	Де застосовується принцип найменших привілеїв, щоб зменшити ризик несанкціонованого доступу	Традиційним IT-середовищам з чітко визначеними периметрами або великі підприємства

Продовження таблиці 2.1

3.	Які є переваги	Безперервна автнтифікація та мінімальним доступом, краща адаптованість до динамічного робочого середовища, масштабований і хмарний, зменшена поверхня атаки, покращена видимість мережевого трафіку, суворий контроль доступу	Підходить для захисту мережевих периметрів, може надавати доступ до широкого спектру мережевих ресурсів	Рідна хмарна архітектура для масштабованості та гнучкості, брандмауер, захист від вторгнень, безпечний веб-шлюз, CASB тощо	Сильна безпека даних і конфіденційність, захищає конфіденційну інформацію, підходить для конфіденційних даних	Простота і зручність використання для користувачів і адміністраторів, знижена складність і вартість	Зменшення ризику несанкціонованого доступу та витоку даних, покращений захист від випадкового розкриття даних, спрощений контроль доступу, узгоджений з конкретними посадовими функціями	Забезпечує резервування та стійкість до окремих точок відмови, може використати наявні інвестиції в безпеку, легше реалізувати в традиційних, усталених мережевих архітектурах

Продовження таблиці 2.1

4.	Які є недоліки	Важко налаштувати та керувати, може бути дорогим, може вимагати змін у процесах, і може бути важко інтегруватися з існуючими системами безпеки, вимагає зміни мислення користувачів і організацій, потребує постій-ного моніторингу	Може знизити продуктивність, важко налаштувати та використовувати, може бути несумісним з усіма пристроями та програмам	За своєю суттю рідна хмара	Може не захищати безпосередньо доступ до мережі, обмежений у додатках, крім захисту даних, потрібна криптографічна експертиза	Обмежена адаптованість до сучасних робочих середовищ і віддаленої роботи, потенційна підвищена вразливість до внутрішніх загроз	Може призвести до збільшення адміністративних витрат, зосередження лише на дозволах доступу може не усунути зовнішні загрози чи спроби неавторизованого доступу	Покладається на припущення про довіру в певних межах, може створити хибне відчуття безпеки, якщо не буде реалізовано комплексно на всіх рівнях, може бути неефективним проти передових спрямованих атак

За результатами порівняльного аналізу, можна зробити висновок, що враховуючи всі особливості інформаційно-комунікаційної системи та елементи її обстеження, найбільш підходящою моделлю безпеки буде саме Zero Trust.

Принцип нульової довіри пропонує більш динамічний і адаптивний підхід, який краще відповідає потребам сучасних онлайн-організацій, забезпечуючи захист незалежно від місця розташування користувачів та пристроїв. За рахунок застосування принципу мінімальних привілеїв та постійної верифікації нульова довіра значно знижує ризики, пов'язані з внутрішніми загрозами. Нульова довіра забезпечує покращену видимість і контроль за трафіком мережі та діями користувачів, що дозволяє ефективніше виявляти та запобігати атакам.

2.3 Розробка елементів політики безпеки

Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації. [1]

Метою політики безпеки є впровадження та ефективна робота системи управління інформаційною безпекою та захистом мережі, яка забезпечить безпеку та надійність функціонування бізнес-процесів, захистить інформацію та ресурси компанії від зовнішніх та внутрішніх загроз та пов’язаних з ними загроз навмисно або ненавмисно утвореними співробітниками компанії. Політики забезпечують безперебійну роботу компанії, сприяють мінімізації ризиків у її операційній діяльності та створюють позитивну репутацію компанії при роботі з клієнтами. [8]

Спираючись на отримані результати аналізу моделі порушника та загроз, та розглядаючи особливості ІКС, було розроблено основні елементи політики безпеки, зокрема:

- політика керування обліковими записами;
- політика ідентифікації та автентифікації;
- політика розмежування доступу;
- політика антивірусного захисту;

- політика використання власного обладнання;
- політика проведення занять;
- політика розповсюдження та копіювання інформаційних ресурсів;
- політика захисту матеріалів за допомогою водяних знаків та інших стеганографічних засобів.

Дані політики безпеки мають наступну структуру:

1) мета;
2) область застосування;
3) зміст політики;
4) відповідальність;
5) періодичність та порядок перегляду політики.

2.3.1 Політика керування обліковими записами

Мета:

Метою політики є забезпечення контролю доступу до ресурсів, зменшення ризику несанкціонованого доступу та підвищення рівня захисту облікових записів користувачів.

Область застосування:

Ця політика поширюється на всіх співробітників та користувачів ІКС підприємства GoITeens.

Політика:

- усі нові облікові записи створюються на підставі офіційного запиту та затвердження відповідальними особами;
- кожен користувач повинен мати унікальний обліковий запис, спільне використання облікових записів заборонено;
- використання багатофакторної аутентифікації для всіх облікових записів, які мають доступ до критичних ресурсів;
- облікові записи повинні деактивуватися негайно після звільнення працівника або завершення контракту з клієнтом;

- видалення облікових записів повинно проводитися відповідно до встановлених процедур після завершення періоду зберігання даних;

- усі дії користувачів повинні логуватися для подальшого аналізу та розслідування у разі інцидентів;

- регулярне навчання користувачів з питань безпеки та правильного використання облікових записів.

Відповідальність:

Відповідні всі працівники та користувачі ІКС підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин, а користувач розривання контракту для подальшої співпраці.

Періодичність та порядок перегляду політики:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.2 Політика ідентифікації та автентифікації

Мета:

Забезпечення надійної ідентифікації та автентифікації користувачів, захист інформаційних ресурсів від несанкціонованого доступу та підвищення рівня безпеки автентифікаційних процедур.

Область застосування:

Ця політика поширюється на всіх співробітників та користувачів ІКС підприємства GoITeens.

Політика:

- кожен користувач повинен мати унікальний ідентифікатор (логін), що не використовується іншими користувачами;

- усі нові користувачі повинні проходити офіційну процедуру реєстрації з наданням необхідної інформації для створення облікового запису;

- пароль до облікового запису має складатися з мінімум 12 символів, використовуючи великі і малі літери, цифр і спеціальні символи;

- користувачі повинні змінювати паролі кожні 90 днів;

- використовувати багатофакторну автентифікація для доступу до всіх критичних ресурсів. Така автентифікація повинна включати в себе щонайменше два фактори, наприклад пароль та код;

- облікові записи повинні автоматично блокуватися після 5 невдалих спроб входу з подальшою процедурою розблокування через службу підтримки;

- користувач повинен отримувати повідомлення на зареєстровану ним електронну пошту або мобільний телефон при зміні пароля або інших критичних діях;

- всі дії, пов'язані з автентифікацією та доступом, повинні логуватися для подальшого аналізу.

Відповідальність:

Відповідні всі працівники та користувачі ІКС підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин, а користувач розривання контракту для подальшої співпраці.

Періодичність та порядок перегляду політики:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.3 Політика розмежування доступу

Мета:

Забезпечення контрольованого доступу до інформаційних ресурсів, мінімізування ризиків несанкціонованого доступу та потенційних загроз, підвищення рівню захисту конфіденційних даних та систем.

Область застосування:

Ця політика поширюється на всіх співробітників підприємства GoITeens.

Політика:

- користувачі повинні мати доступ лише до тих ресурсів і даних, які необхідні для виконання їхніх обов'язків;

- доступ до ресурсів розподіляється відповідно до ролей та обов'язків користувачів, забезпечуючи мінімально необхідний доступ;

- всі користувачі повинні бути асоційовані з певними ролями, які визначають рівень доступу до ресурсів;

- користувачі з однаковими ролями об'єднуються в групи, для яких налаштовуються відповідні права доступу;

- доступ надається на підставі офіційного запиту та затвердження відповідальними особами. Процедура надання доступу повинна бути задокументована;

- доступ відкликається негайно після зміни ролі, завершення контракту або звільнення працівника. Відповідальна особа повинна повідомити про необхідність відкликання доступу;

- всі дії, пов'язані з доступом до критичних ресурсів, повинні логуватися для подальшого аналізу;

- періодичні перевірки та аудити прав доступу для забезпечення відповідності актуальним вимогам та ролям користувачів.

Відповідальність:

Відповідні всі працівники підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.4 Політика антивірусного захисту

Мета:

Захист інформаційних систем організації від вірусів, шкідливого ПЗ та інших загроз.

Область застосування:

Ця політика поширюється на всіх співробітників підприємства GoITeens.

Політика:

- на всіх комп'ютерах, серверах та інших пристроях організації повинно бути встановлене і налаштоване антивірусне програмне забезпечення;
- антивірусне програмне забезпечення повинно підтримуватися у актуальному стані, з встановленням усіх доступних оновлень;
- файли, що завантажуються з Інтернету або отримуються через електронну пошту, повинні автоматично скануватися перед відкриттям.
- антивірусне програмне забезпечення повинно автоматично повідомляти користувача про виявлення шкідливого програмного забезпечення.

Відповідальність:

Відповідні всі працівники підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.5 Політика використання власного обладнання

Мета:

Забезпечення безпечного використання власного обладнання для доступу до корпоративних ресурсів, захист конфіденційних даних від витоків та несанкціонованого доступу.

Область застосування:

Ця політика поширюється на всіх співробітників підприємства GoITeens.

Політика:

- усі власні пристрої, що використовуються для роботи з корпоративними ресурсами, повинні бути зареєстровані в системі управління мобільними пристроями (MDM);
- власні пристрої повинні проходити перевірку на відповідність політикам безпеки організації, включаючи наявність антивірусного програмного забезпечення;
- всі дані на власних пристроях, які використовуються для роботи з корпоративними ресурсами, повинні бути зашифровані;
- пристрої повинні мати налаштоване автоматичне блокування екрану та вимагати пароль або інший метод автентифікації для розблокування;
- особисті та корпоративні дані на власних пристроях повинні бути розмежовані;
- у разі втрати або крадіжки пристрою повинна бути можливість віддаленого видалення корпоративних даних.

Відповідальність:

Відповідні всі працівники підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.6 Політика проведення занять

Мета:

Захист від поширення неправдивої інформації та запобігання соціальній інженерії.

Область застосування:

Ця політика поширюється на всіх співробітників підприємства GoITeens, що пов'язані з навчальним процесом.

Політика:

- всі онлайн заняття повинні записуватися для можливості подальшого перегляду та перевірки;

- записи зберігаються на захищених серверах протягом визначеного періоду часу, що встановлюється керівництвом;

- учні повинні мати можливість анонімно повідомляти про підозрілі або неправдиві дані, які вони виявили під час занять. Всі повідомлення учнів повинні бути розглянуті відділом контролю якості в найкоротші терміни;

- відділ контролю якості здійснює постійний моніторинг всіх записів занять та використовує алгоритми машинного навчання та штучного інтелекту для автоматичного виявлення підозрілої поведінки або неправдивої інформації під час занять;

- всі викладачі повинні проходити регулярне навчання з питань інформаційної безпеки, включаючи принципи запобігання соціальній інженерії та відповідальність за надання достовірної інформації.

Відповідальність:

Відповідні всі працівники підприємства. У разі порушення даної політики працівник передбачає дисциплінарну відповідальність та повинен понести стягнення, навіть припинення трудових відносин.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.7 Політика розповсюдження та копіювання інформаційних ресурсів

Мета:

Встановлення правил та процедур для захисту конфіденційної та службової інформації від несанкціонованого розповсюдження або копіювання.

Область застосування:

Ця політика поширюється на всіх співробітників та користувачів ІКС підприємства GoITeens.

Політика:

- вся інформація підприємства повинна бути класифікована на конфіденційну, службову та загальнодоступну;

- конфіденційна та службова інформація не повинна передаватися стороннім особам або організаціям без письмового дозволу керівництва;

- всі електронні повідомлення, що містять конфіденційну інформацію, повинні бути зашифровані;

- копіювання конфіденційної інформації на зовнішні носії даних забороняється без письмового дозволу керівництва;

- конфіденційна інформація повинна зберігатися в захищених місцях з обмеженим доступом;

- конфіденційна інформація повинна бути безпечно видалена після закінчення терміну її зберігання або після втрати актуальності.

Відповідальність:

Відповідні всі працівники та користувачі ІКС підприємства. У разі порушення даної політики працівник передбачає припинення трудових відносин, а користувач розривання контракту для подальшої співпраці.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.3.8 Політика захисту матеріалів за допомогою водяних знаків та інших стеганографічних засобів

Мета:

Забезпечення належності інформації підприємстві в разі її викрадення чи несанкціонованого розповсюдження.

Область застосування:

Ця політика поширюється на всіх співробітників та користувачів ІКС підприємства GoITeens.

Політика:

- всі цифрові документи, графічні матеріали, відео та інші цифрові контенти підприємства повинні містити водяні знаки, які ідентифікують належність матеріалів підприємству;

- водяні знаки повинні містити логотип підприємства, назву та інші ідентифікуючі деталі;

- всі цифрові файли повинні містити метадані, які вказують на їх належність підприємству, включаючи автора, дату створення та іншу важливу інформацію;

- метадані повинні бути захищені від редагування;

- всі важливі документи та контракти повинні бути підписані за допомогою цифрового підпису, який підтверджує їх автентичність.

Відповідальність:

Відповідні всі працівники та користувачі ІКС підприємства. У разі порушення даної політики працівник передбачає припинення трудових відносин, а користувач розривання контракту для подальшої співпраці.

Періодичність та порядок перегляду безпеки:

Політика повинна переглядатись щороку радою директорів. У разі необхідності корективи можуть бути внесені раніше необхідному терміну перегляду.

2.4 Заходи реалізації моделі безпеки Zero Trust

Як було зазначено в обстеженні ІКС, типові робочі місця зазвичай базуються на Microsoft Windows 10 або 11 версії. На основі документацій, рекомендованих для реалізації принципу Zero Trust, можна розробити певні заходи реалізації цієї моделі безпеки.

Zero Trust – це комплексна стратегія безпеки, яка відстежує та контролює шість стовпів безпеки: посвідчення, кінцеві точки, програми, мережу, інфраструктуру та дані.

1. Посвідчення

Посвідчення у підході «Нікому не довіряй» визначається як користувачі, служби та облікові дані, які застосовуються додатками та пристроями Інтернету речей. Посвідчення контролюють та адмініструють доступ до важливих даних та ресурсів. Це означає, що коли посвідчення намагається отримати доступ до ресурсу, організація повинна перевірити його за допомогою методів суворої автентифікації та переконатися, що доступ відповідає вимогам і є типовим для цього посвідчення із застосуванням принципів мінімальних прав доступу.

2. Кінцева точка

Кінцева точка — це будь-який пристрій, який підключається до мережі в хмарі, локально або віддалено. До них відносяться пристрої працівників, пристрої Інтернету речей, смартфони, а також гостьові пристрої. У підході «Нікому не довіряй» безпекові політики застосовуються однаково для всіх кінцевих точок. При наданні посвідчення доступу до ресурсу дані можуть передаватися з різних кінцевих точок. Якщо кінцеві точки не захищені, це може спричинити великий ризик.

3. Програми

Програми – це засоби підвищення продуктивності, за допомогою яких користувачі отримують доступ до своїх даних. Знання принципів роботи цих додатків та їх програмних інтерфейсів дуже важливе для розуміння потоку даних та управління ним. Усі програми, що використовуються у цифровій інфраструктурі, повинні отримувати строго контрольовані дозволи в програмі з відстеженням їхньої аномальної поведінки.

4. Мережа

Мережі являють собою засоби для доступу до наших даних. Використання елементів керування доступом до мережі та моніторинг поведінки користувачів і пристроїв у режимі реального часу можуть надавати аналітику та забезпечувати

видимість загроз, а також допомагають кіберзлочинцям переміщатися по мережі в бічному напрямку. Сегментація мережі, використання засобів виявлення та запобігання загрозам, а також шифрування мережного трафіку знижують ймовірність атаки та зменшують наслідки пролому в системі безпеки.

5. Інфраструктура

Інфраструктура охоплює всі аспекти цифрової області – від локальних серверів до хмарних віртуальних машин. Основна увага в інфраструктурі приділяється управлінню конфігурацією та оновленню програмного забезпечення. Надійний підхід до управління конфігурацією гарантує, що всі розгорнуті пристрої відповідають мінімальним вимогам щодо безпеки та політики.

6. Дані

Розуміння своїх даних та застосування правильного рівня керування доступом дуже важливе, якщо ви хочете захистити їх. Але це далеко ще не все. Обмежуючи доступ та реалізуючи надійні політики використання даних, а також застосовуючи моніторинг у режимі реального часу, ви можете обмежити або заблокувати загальний доступ до конфіденційних даних та файлів. [9]

Хоча реалізація «Нульова довіра» продовжує розвиватися, кожна організація є унікальною і часто починається з посвідчення користувача та додатку. Нижче наведено політики та елементи управління, які багато організацій пріоритетують у міру розгортання нульової довіри:

- реалізуйте політики гігієни облікових даних та змін додатків та служб. Коли зловмисники компрометують такі секрети, як сертифікати або паролі, вони можуть досягти глибини системного доступу для отримання маркерів під виглядом посвідчення програми. Потім вони отримують доступ до конфіденційних даних, переміщуються пізніше і встановлюють збереження;

- розгортання суворої автентифікації. IT-адміністратори налаштовують політики, що вимагають багатофакторної автентифікації;

- обмежте згоду користувачів з дозволами з низьким ризиком для перевірених програм видавця. Організації та клієнти оцінюють запити на

дозволи та надійність додатка перед наданням згоди. IT-адміністратори ухвалюють принцип явної перевірки, вимагаючи перевірки видавця. Вони застосовують принцип найменшого привілею, дозволяючи згоду користувача лише для дозволів з низьким ризиком;

- блокування застарілих протоколів та API. IT-адміністратори блокують старі протоколи автентифікації, такі як «Звичайна автентифікація» і вимагають сучасних протоколів, таких як OpenID Підключення та OAuth2.

Документації Microsoft рекомендують використовувати довірені бібліотеки автентифікації на основі стандартів. Замість використання протоколів з відомими вразливостями та великою документацією для розробки програми, рекомендується використання таких бібліотек, як бібліотека автентифікації Майкрософт (MSAL), бібліотека автентифікації Microsoft Identity Web і комплекти засобів розробників програмного забезпечення Azure Software Developer Kits (SDK).

Також важливим моментом є планування та проектування мінімального доступу до привілеїв. Ключовим принципом нульової довіри є найменш привілейований доступ. Достатньо розробити та задокументувати програму, щоб клієнти могли успішно налаштувати політики найменших привілеїв.

Ще одним важливим моментом є підтримка безперервної оцінки доступу. Це дозволяє Microsoft Graph швидко заборонити доступ у відповідь на події безпеки. Приклади включають такі дії адміністратора клієнта: видалення або вимкнення облікового запису користувача, увімкнення багатофакторної автентифікації для користувача, явне скасування виданих користувачем маркерів, виявлення користувача, що переміщується у стан високого ризику. [10]

2.6 Криптографічні засоби захисту авторських прав

Враховуючи політику захисту матеріалів підприємства, що наведена у п. 2.3.8, варто обрати необхідний засіб, який зможе захистити авторські права інформаційних ресурсів, що циркулюють у ІКС.

Розберемо існуючі доступні способи захисту [11] та визначимо, чи підходять вони для розглянутого підприємства:

1. Обмеження функціональності

За такого підходу, власник авторського права надає користувачеві примірник твору, який має функціональні обмеження. Тобто, це щось на кшталт пробної версії продукту чи інформації. В даному випадку такий засіб не підходить, оскільки працівники повинні постійно мати доступ до необхідної їм інформації, тому що вони її використовують.

2. Використання кодових слів

Полягає у введенні у текст рідкісних та екзотичних слів за якими можна відстежити використання власного твору. Такий засіб не є ефективним, оскільки компанія основується на курсах програмування для підлітків, тобто рідкісні або екзотичні слова не можуть бути використані для навчання.

3. Встановлення таймеру

Власник авторських прав розповсюджує об'єкт інтелектуальної власності, але встановлює дату, після якої доступ до нього буде неможливим. Такий підхід дійсно може використовуватись на клієнтів підприємства, але даний засіб не забезпечує уникнення загрози з боку працівників.

4. Криптографічні конверти

Зашифрування інформації таким чином, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру. Знову ж таки, засіб не може бути ефективним, оскільки після розшифрування працівники можуть використовувати цю інформацію без обмежень.

5. Стеганографічні цифрові водяні знаки

Такий підхід дозволяє вбудовувати інформацію у файли з метою її прихованої передачі та захистити інформацію від викрадення та подальшого незаконного використовування. Даний засіб може влучно підійти для такого особливого випадку, що існує на підприємстві.

Оскільки цифрові водяні знаки є найбільш підходящим методом захисту авторських прав інформаційних ресурсів підприємства, проведемо аналіз

популярних та доступних інструментів для зображення водяних знаків. До таких інструментів можна віднести: Adobe Photoshop, iLoveIMG, Batch Picture Protector, iWatermark Pro, uMark. [12]

1. Adobe Photoshop

Комплексний інструмент, що вважається галузевим стандартом для редагування та обробки зображень, і вимагає встановлення. Він дозволяє вставляти текст або графічні зображення в якості водяних знаків. Можна налаштовувати всі необхідні вимоги відповідно розміру, прозорості або позиції. Даний інструмент також дозволяє наносити водяні знаки на кілька зображень одночасно, що є перевагою. З іншого боку, даний інструмент не має можливості створення водяного знаку на основі метаданих. Також, Adobe Photoshop – платний продукт.

2. iLoveIMG

Пропонує інтуїтивно зрозумілу платформу для застосування водяних знаків до зображень. Він підтримує можливість використовувати онлайн інтерфейс, тому встановлення окремої програми не потрібно. Значною перевагою інструменту є простота у розумінні інтерфейсу та безкоштовні можливості, які звісно можна розширити за допомогою платної версії. Налічує в собі багато шрифтів, кольорів і налаштувань для водяних знаків, проте відсутнє створення водяного знаку на основі метаданих також, як і в минулому розглянутому інструменті.

3. Batch Picture Protector

Інструмент, призначений для одночасного застосування водяних знаків до кількох зображень. Пропонує широкий спектр настроюваних функцій для нанесення водяних знаків, включаючи налаштування непрозорості, розміру та положення. Доволі інтуїтивний у використанні, але вимагає попереднього встановлення. Також вважається платним інструментом.

4. iWatermark Pro

Даний інструмент задовольняє потреби водяних знаків високого класу, створений для ідеального балансу функціональності та зручності користувача.

Він пропонує налаштування параметрів водяних знаків, включаючи текст, логотипи, підписи, QR-коди та навіть водяні знаки на основі метаданих. Існує також встановлення прозорості, масштабу, обертання та розташування водяного знаку, що добре підходить для професійного використання. Дозволяє оброблювати одночасно одразу велику кількість зображень. Потребує попереднього встановлення та купівлі, має складний інтерфейс користування через величезний набір функцій.

5. uMark

Універсальний інструмент для водяних знаків, яке пропонує користувачам можливість захистити свої графічні матеріали від несанкціонованого використання ефективним і зручним способом. Дозволяє створювати власні водні знаки у вигляді тексту, зображень, форм чи навіть опцію вбудовування метаданих. Також існує можливість групового нанесення водяних знаків. Через такий список можливостей інструмент звичайно ж є платним, але має пробну безкоштовну версію, та потребує встановлення.

Зібрані характеристики кожного інструмента захисту авторських прав та інші факти зображені на таблиці 2.2.

Таблиця 2.2. Характеристики інструментів захисту авторських прав

Назва інструменту	Можливості	Простота інтерфейсу	Ціна	Підтримка клієнтів
Adobe Photoshop	Можливість налаштування ВЗ, одночасна робота з кількома зображеннями, вимагає встановлення	Може бути важко через велику кількість функцій	Висока	Висока

Продовження таблиці 2.2

iLoveIMG	Можливість налаштування, текстові або графічні ВЗ, не вимагає встановлення	Дуже простий	Безкоштовно, з платними додатковими можливостями	Середня
Batch Picture Protector	Одночасна робота, різні типи знаків, збереження якості, вимагає встановлення	Доволі простий	Від середньої до високої	Висока
iWatermark Pro	Різні типи знаків, одночасна робота, збереження якості вбудовування метаданих, вимагає встановлення	Середня складність	Висока	Висока
uMark	Гнучкі параметри, одночасна робота, вбудовування метаданих, вимагає встановлення, має пробну версію	Середня складність	Від середньої до високої	Висока

Враховуючи всі характеристики та правила розробленої політики безпеки, можна дійти висновку, що інструмент для захисту авторських прав для зручності роботи повинен містити в собі вбудовування метаданих, а не просто накладення водяного знаку. Таким чином, підходять лише два інструменти з перерахованих, а саме iWatermark Pro та uMark. Розглядаючи їх можливості та ціну, найбільш підходящим інструментом стає uMark. Цей інструмент має пробну версію, яку

можна використати в якості тестування та точно зупинити свій вибір на ньому. Також ціна може бути не настільки висока в порівнянні з другим інструментом.

2.7 Висновок спеціального розділу

У другому розділі кваліфікаційної роботи було проведено оцінку існуючих елементів політики безпеки в закладі дистанційної освіти та обґрунтовано вибір моделі безпеки. Обстеження особливостей інформаційно-комунікаційної системи та порівняльний аналіз базових популярних моделей безпеки дозволили вибрати найбільш підходящу модель – «Zero Trust».

На основі цієї оцінки та обґрунтування були розроблені елементи політики безпеки, які охоплюють такі важливі аспекти, як керування обліковими записами, ідентифікація та автентифікація користувачів, розмежування доступу, антивірусний захист, використання власного обладнання, проведення занять, розповсюдження та копіювання інформаційних ресурсів, а також захист матеріалів за допомогою водяних знаків та інших стеганографічних засобів.

Окрім розробки політики, були також розглянуті заходи реалізації моделі безпеки, що базуються на документаціях від Microsoft, та проведено аналіз і вибір криптографічного засобу захисту авторських прав. Ці заходи спрямовані на забезпечення цілісності, конфіденційності та доступності інформації в закладі дистанційної освіти, що є ключовими елементами ефективного захисту даних і підтримки надійної роботи інформаційно-комунікаційної системи.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Мета економічного розділу

Метою виконання економічного розділу кваліфікаційної роботи є техніко-економічне обґрунтування доцільності запровадження політики безпеки інформації інформаційно-комунікаційної системи закладу дистанційної освіти «GoITeens».

Впровадження політики безпеки інформації є важливим аспектом діяльності будь-якого підприємства, включаючи заклади дистанційної освіти. Це є інвестицією в довгострокову стабільність, безпеку та репутацію закладу та допомагає уникнути багатьох потенційних проблем та забезпечити надійну основу для подальшого розвитку. Попередження кіберінцидентів може зекономити значні фінансові ресурси, оскільки відновлення після кібератаки може бути дуже витратним.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це вкладення коштів у придбання, створення або модернізацію довгострокових активів підприємства. Капітальні інвестиції спрямовані на забезпечення стійкого розвитку підприємства, підвищення його конкурентоспроможності та ефективності.

За методикою Gartner Group до фіксованих витрат підприємства GoITeens варто віднести наступні витрати:

- ліцензії на платформи для проведення процесу навчання;
- системи управління навчанням (LMS);
- оптимізація та підтримка веб-сайту закладу;
- розробка та придбання мультимедійних матеріалів;
- витрати на залучення клієнтів;
- розробка політики безпеки інформації;
- інтеграція системи інформативної безпеки у вже існуючу систему;
- навчання працівників.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Трудомісткість у даному випадку буде розраховуватися за формулою 3.1:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Показники часу, визначеного на розробку політики інформаційної безпеки наведені у таблиці 3.1.

Таблиця 3.1 – Показники трудомісткості розробки політики безпеки

Показник	Значення, год
$t_{тз}$	5
$t_{в}$	5
$t_{а}$	6
$t_{вз}$	4
$t_{озб}$	3
$t_{овр}$	3
$t_{д}$	4

Згідно з формулою 3.1, трудомісткість розробки ПБ становить:

$$t = 5 \text{ год} + 5 \text{ год} + 6 \text{ год} + 4 \text{ год} + 3 \text{ год} + 3 \text{ год} + 4 \text{ год} = 30 \text{ год.}$$

Надалі потрібно розрахувати витрати на створення політики безпеки інформації ($К_{рп}$), використовуючи наступні показники: витрати на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) та вартість витрат машинного часу, що необхідний для розробки політики безпеки інформації ($З_{мч}$).

Розрахунок проводиться за формулою 3.2:

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

У свою чергу, витрати на основну і додаткову заробітну плату спеціаліста ІБ, а також відрахування на соціальні потреби, розраховуються за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, год;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуванням, грн/годину. Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, в загальному випадку, становить – 150 грн/год.

Також, вартість витрат машинного часу, що необхідний для розробки політики безпеки інформації, розраховується за формулою 3.4:

$$З_{мч} = t \cdot C_{мч} \text{ грн,} \quad (3.4)$$

де t – трудомісткість розробки політики безпеки інформації на ПК, год;

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

Відповідно вартість години машинного часу ПК розраховується за формулою 3.5:

$$С_{мч} = Р \cdot t_{нал} \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}} \text{ грн,} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$С_{е}$ – тариф на електричну енергію, 4,32 грн/кВт · год;

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

$Н_{а}$ – річна норма амортизації на ПК, частки одиниці;

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

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

$F_р$ – річний фонд робочого часу.

Вартість ПК – 10000 грн, строк корисної служби – 32 місяці. Мінімальний строк корисної служби – 24 місяці. Накопичена амортизація в такому випадку складає 10 000 : 32 · 12 = 3 750 грн. Таким чином, залишкова вартість складає: 10000 – 3 750 = 6 250 грн.

Ліцензійне програмне забезпечення складається із: Windows 10 Pro – 7 960 грн, Microsoft Office 365 2021 – 3 900 грн, тобто 7 960 + 3 900 = 11 860 грн.

Згідно з формулою 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 30 \cdot 150 \text{ грн/год} = 4\,500 \text{ грн.}$$

Далі, згідно з формулою 3.5, вартість 1 години машинного часу ПК, становить:

$$С_{мч} = 0{,}085 \cdot 1 \cdot 4{,}32 + \frac{6250 \cdot 0{,}5}{1920} + \frac{11860 \cdot 0{,}5}{1920} = 0{,}37 + 1{,}63 + 3{,}09 = 5{,}09 \text{ грн,}$$

а значить, що вартість витрат машинного часу, що необхідний для розробки політики безпеки інформації, за формулою 3.4 становить:

$$З_{мч} = 30 \cdot 5{,}09 = 152{,}7 \text{ грн.}$$

Тож, витрати на створення ПБ за формулою 3.2 становлять:

$$К_{рп} = 4\,500 + 152{,}7 = 4\,652{,}7 \text{ грн.}$$

У результаті розрахунків, маємо вартість розробки ПБ – 4 500 гривень.

У даному випадку повну вартість капітальних витрат можна розрахувати за формулою 3.6:

$$K = K_{пр} + K_{аз} + K_{рп} + K_{навч} + K_{зпз} + K_{н} \text{ грн.} \qquad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, грн. Оскільки не планується наймання зовнішніх консультантів, то даний коефіцієнт не враховується та вважається за 0;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, грн. Оскільки всі процеси інформаційно-комунікаційної системи на підприємстві відбуваються за допомогою хмарних сервісів та кожен працює з власного пристрою, то апаратне забезпечення не планується використовуватись. В такому випадку даний коефіцієнт враховуємо за 0;

$К_{рп}$ – вартість розробки політики безпеки інформації, грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн. В даному випадку буде проведений одноразовий кваліфікаційний захід для співробітників з питань ознайомлення з редакцією політики безпеки, що буде коштувати 1000 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, грн. В даному випадку закупівлі ПЗ відсутні, тому вартість сприймаємо за 0;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, грн. Оскільки встановлення обладнання не планується, то будемо вважати ці витрати за 0.

Враховуючи всі нульові показники, фінальною формулою, що розраховує повну вартість капітальних витрат являється формула 3.7:

$$К = К_{рп} + К_{навч} \text{ грн.} \quad (3.7)$$

Згідно цієї формули проведемо розрахунок:

$$К = 4\,652{,}7 + 1000 = 5\,652{,}7 \text{ грн}$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об’єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі. [13]

За методикою Gartner Group до поточних (експлуатаційних) витрат даного підприємства можна відвести наступні:

- заробітна плата обслуговуючого персоналу;
- навчання адміністративного персоналу й кінцевих користувачів;
- кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки.

Методи захисту, передбачені політикою безпеки, мають більш організаційних характер та несуть в собі перелік правил та вимог, тому поточними витратами можна вважати лише заробітну платню системного адміністратора, що буде найнятий для забезпечення безпеки та контролю системи в майбутньому. Її можна розрахувати за формулою 3.8:

$$C = З_{зп} + З_{кз} + З_{дод} \text{ грн}, \quad (3.8)$$

де $З_{зп}$ – заробітна платня системного адміністратора, що в середньому складає 20 000 грн;

$З_{кз}$ – виплати системному адміністратору за проведення кваліфікаційних заходів та перевірку знань та навичок персоналу стосовно правил, регламентованих політикою безпеки. В цьому випадку вартість такої послуги буде становити 900 грн та проводитиметься раз квартал, тобто умовно оплата за один місяць – 300 грн;

$З_{дод}$ – додаткові виплати системному адміністратору за відповідальність за виконання певних розділів політики безпеки інформації. Таким чином, розмір таких додаткових виплат становитиме 1000 грн на місяць.

За формулою 3.8 зробимо розрахунок поточних витрат:

$$C = 20\,000 + 300 + 1000 = 21\,300 \text{ грн}$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою оцінки є визначення обсягів матеріальних збитків, виходячи з ймовірності реалізації конкретної загрози та можливих матеріальних втрат від

неї. Нижче будуть вказані загрози, які можуть нести економічних вплив на підприємство:

1. Взлом кіберзлочинцями чи хакерами працівників компанії, що мають доступ до конфіденційної інформації, що приводить до витоку інформаційних ресурсів. Така загроза може спричинити втрату частини запланованого заробітку, а також використання додаткових коштів для усунення наслідків;

2. Шахрайства фінансового характеру. Конкуренти або кіберзлочинці можуть видати себе за менеджера з питань оплати та обманути клієнтів. Така загроза призведе втрату запланованого заробітку.

3. Перерви у роботі, втрата даних та затримка у наданні послуг при відмові чи несправності технічних засобів. Призведе до додаткових витрат у вигляді компенсації клієнтам.

4. Збої, втрата даних або виникнення недостовірної інформації через введення невірних даних та управління системами навмисним або випадковим чином, який базується на людському факторі. Така загроза також може спричинити втрату частини запланованого заробітку.

Для розрахунку збитків від реалізації даних загроз використовується формула 3.9:

$$U = П_п + П_в + V \text{ грн}, \tag{3.9}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників активного вузла, грн;

$П_в$ – вартість відновлення працездатності вузла, грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу для розрахунку цих трьох показників використовуються формули 3.10 – 3.12 відповідно:

$$П_п = \frac{\sum З_с}{F} \cdot t_n \text{ грн}, \tag{3.10}$$

де $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

F – місячний фонд робочого часу;

t_n – час простою вузла або сегмента корпоративної мережі внаслідок атаки, год.

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн}, \quad (3.11)$$

де $П_п$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

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

$$V = \frac{O}{F} \cdot (t_п + t_в + t_{ви}) \text{ грн}, \quad (3.12)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн/місяць;

F – місячний фонд робочого часу;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, год;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, год;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, год.

У свою чергу, $П_{ви}$ та $П_{пв}$ розраховуються за формулами 3.13 та 3.14 відповідно.

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} \text{ грн}, \quad (3.13)$$

де $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць;

F – місячний фонд робочого часу;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, год.

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в \text{ грн}, \quad (3.14)$$

де $З_о$ – заробітна плата обслуговуючого персоналу, грн/місяць;

F – місячний фонд робочого часу;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, год.

Відповідно до пронумерованого списку загроз, можна розрахувати ймовірні збитки. Враховуючи той факт, що деяка загрози мають схожі наслідки, розрахунки будуть проводитись для одного випадку з групи подібних, але надалі буде враховуватись кількість можливих подій на рік та ймовірність їх виникнення.

Загрози 1 (взлом працівників), 3 (відмова чи несправність технічних засобів) та 4 (введення невірних даних та управління системами) мають схожі наслідки, тому розмір збитку від реалізації однієї з них буде таким самим і для інших, та буде розраховуватись за формулами 3.9 – 3.14:

$$П_п = 15000 \text{ грн} \cdot \frac{50 \text{ чол}}{176 \text{ год}} \cdot 10 \text{ год} = 42\,614 \text{ грн}$$

$$П_{ви} = 0 \text{ грн}$$

$$П_{зч} = 0 \text{ грн}$$

$$П_{пв} = 20\,000 \text{ грн} \cdot \frac{1 \text{ чол}}{176 \text{ год}} \cdot 5 \text{ год} = 568 \text{ грн}$$

$$П_в = 0 + 568 + 0 = 568 \text{ грн}$$

$$V = 2\,250\,000 \cdot \frac{1}{176} \cdot (10 + 5 + 0) = 191\,761 \text{ грн}$$

Маючи всі необхідні показники, розрахуємо розрахунок збитків:

$$U = 42\,614 + 568 + 191\,761 = 234\,943 \text{ грн}$$

Тобто, збиток після реалізації однієї з загроз 1, 3 або 8 становитиме – 234 943 грн.

Остання загроза, що відмінна від всіх інших та має певний наслідок від її реалізації – загроза під номером 2 (шахрайство). В середньому оплата за курс за місяць складає 3000 грн, тому шахраї мають можливість обманути клієнта та вкрасти цю суму, а підприємство відповідно втратить ці кошти.

Підводячи підсумок, маючи дані про можливі збитки від реалізації загроз можна провести розрахунок загального збитку від кожної з них за формулою 3.15.

$$\text{B} = \sum_{\text{i}} \cdot \sum_{n} \cdot \text{U} \qquad (3.15)$$

де i – число атакованих вузлів;

n – середнє число атак на рік.

Проведемо розрахунок для кожної з атак:

1) $\text{B}_1 = 1 \cdot 2 \cdot 234\,943 = 469\,886$ грн;

2) $\text{B}_2 = 1 \cdot 1 \cdot 3\,000 = 3\,000$ грн;

3) $\text{B}_3 = 1 \cdot 1 \cdot 234\,943 = 234\,943$ грн;

4) $\text{B}_4 = 1 \cdot 1 \cdot 234\,943 = 234\,943$ грн.

Загальний збиток від всіх можливих атак можна розрахувати за формулою 3.16:

$$\text{B} = R_1 \cdot B_1 + R_2 \cdot B_2 + R_3 \cdot B_3 + R_4 \cdot B_4 \text{ грн}, \qquad (3.16)$$

де R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці.

Тому, загальний збиток складає:

$$\text{B} = 0{,}05 \cdot 469\,886 + 0{,}02 \cdot 3000 + 0{,}01 \cdot 234\,943 + 0{,}08 \cdot 234\,943 =$$
$$= 23\,494{,}3 + 60 + 2\,349{,}43 + 18\,795{,}44 = 44\,699{,}17 \text{ грн}$$

3.3 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою 3.17:

$$\text{E} = \text{B} - \text{C} \text{ грн} \qquad (3.17)$$

де В – загальний збиток від атаки на вузол корпоративної мережі, грн;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Економічний ефект становить:

$$E = 44\,699{,}17 - 21\,300 = 23\,399{,}17 \text{ грн}$$

В загальному вигляді, оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій (ROSI);
- термін окупності капітальних інвестицій $T_о$.

У даному випадку ТСО не використовується, оскільки було визначено величину відверненого збитку.

ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.18.

$$ROSI = \frac{E}{K}, \tag{3.18}$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

Тому,

$$ROSI = \frac{23\,399{,}17}{5\,652} = 4{,}14.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $E_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, та розраховується за формулою 3.19.

$$ROSI > (N_{\text{ден}} - N_{\text{інф}})/100 \quad (3.19)$$

де $N_{\text{ден}} = 19$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{\text{інф}} = 8$ – річний рівень інфляції, %.

4,14 > (19-8)/100 → 4,14 > 0,11.

Отже, проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.20:

$$T_o = \frac{E}{K} = \frac{1}{ROSI} = \frac{1}{4,14} = 0,24 \text{ року.} \quad (3.20)$$

3.4 Висновок економічного розділу

У третьому розділі кваліфікаційної роботи було детально проаналізовано витрати на розробку політики безпеки інформації для закладу дистанційної освіти. Цей аналіз включав розрахунок капітальних (фіксованих) витрат та експлуатаційних (поточних) витрат, необхідних для впровадження заходів безпеки.

Окрім цього, була проведена оцінка потенційних збитків у разі реалізації загроз, що дозволило визначити та проаналізувати показники економічної ефективності запропонованих проектних рішень. Результати розрахунків показали, що введення в експлуатацію засобів та заходів захисту є економічно вигідним для закладу. Термін окупності складає всього 0,24 року, а коефіцієнт ефективності значно перевищує річний рівень прибутковості альтернативних варіантів (4,14 > 0,11).

Ці дані свідчать про повну доцільність впровадження та використання обраних проектних рішень, оскільки вони забезпечують не лише надійний захист інформації, але й високу економічну ефективність. Впровадження таких заходів сприятиме підвищенню безпеки та стабільності роботи закладу дистанційної освіти, знижуючи ризики втрат та підвищуючи довіру користувачів.

ВИСНОВКИ

З розвитком технологій та збільшенням популярності дистанційної освіти питання забезпечення інформаційної безпеки стає все більш актуальним. Проведене дослідження дозволило глибоко проаналізувати сучасні виклики та загрози, з якими стикаються заклади дистанційної освіти, і запропонувати ефективні рішення для їх подолання.

У ході роботи було вивчено інформаційно-комунікаційну систему обраного закладу дистанційної освіти. Детальний аналіз фізичного, обчислювального та інформаційного середовища дозволив виявити потенційні уразливості та ризики. На основі цих даних було обґрунтовано необхідність створення комплексної системи захисту інформації, яка включає як технічні, так і організаційні заходи.

Особлива увага була приділена вибору оптимальної моделі безпеки. Проведений порівняльний аналіз базових популярних моделей безпеки дозволив вибрати модель «Zero Trust», що передбачає недовіру до будь-яких елементів системи за замовчуванням і вимагає постійної перевірки та підтвердження автентичності.

Розроблені політики безпеки охоплюють ключові аспекти захисту даних та забезпечують чітке керування доступом до інформаційних ресурсів. Це включає політики щодо керування обліковими записами, ідентифікації та автентифікації, антивірусного захисту, використання власного обладнання, проведення занять, розповсюдження та копіювання інформаційних ресурсів, а також захисту матеріалів за допомогою водяних знаків та інших стеганографічних засобів.

Економічний аналіз витрат та ефективності запропонованих заходів показав, що впровадження системи захисту є не лише необхідним, але й економічно вигідним. Швидка окупність інвестицій та високий коефіцієнт ефективності (4,14) у порівнянні з річним рівнем прибутковості альтернативних варіантів (0,11) підтверджують доцільність запропонованих рішень.

Результати дослідження свідчать про те, що впровадження комплексних заходів з інформаційної безпеки у закладах дистанційної освіти є критично

важливим для забезпечення їхньої стабільної та безпечної роботи. Це сприятиме підвищенню довіри користувачів, захисту конфіденційних даних та покращенню якості освітніх послуг, відповідаючи сучасним вимогам та викликам у сфері кібербезпеки. Таким чином, проведена робота не лише демонструє ефективність запропонованих рішень, але й встановлює фундамент для подальшого вдосконалення систем захисту інформації у сфері дистанційної освіти.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-003-99 – Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - №22 – (Нормативний документ системи технічного захисту інформації).

2. Wezom.com.ua – Електронний ресурс – https://wezom.com.ua/blog/kiberbezopasnost-v-proektah-ecommerce-kompleksnyy-gayd

3. Speka.media – Електронний ресурс – https://speka.media/yak-diti-buduvali-ukrayinu-maibutnyogo-u-metavsesviti-keis-vm8o7p

4. Uk.wikipedia.org – Електронний ресурс – https://uk.wikipedia.org/wiki/GoITeens

5. Закон України про захист інформації в інформаційно-комунікаційних системах – Електронний ресурс – https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

6. НД ТЗІ 3.7-003 -2005 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Чинний від 08.11.2005]- К. : ДССЗЗІ, 2005. - №125 – (Нормативний документ системи технічного захисту інформації).

7. Humanize.security – Електронний ресурс –https://www.humanize.security/blog/cyber-strategy/zero-trust-model-explained#What-differentiates-Zero-Trust-from-other-security-models

8. Kitsoft.ua – Електронний ресурс – https://kitsoft.ua/ua/politika-informacijnoyi-bezpeki

9. Learn.microsoft.com – Електронний ресурс – https://learn.microsoft.com/en-us/training/modules/zero-trust-introduction/zero-trust-components?ns-enrollment-type=learningpath&ns-enrollment-id=learn-m365.principles-zero-trust

10. Learn.microsoft.com – Електронний ресурс – https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-iam-development-best-practices

11. Intellect21.cdu.edu.ua – Електронний ресурс – http://intellect21.

cdu.edu.ua/?p=281

12. Datanumen.com – Електронний ресурс – http://surl.li/ojuosh

13. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	22	
6	А4	2 Розділ	27	
7	А4	3 Розділ	13	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Б. Вигляд таблиці з матеріалами курсу для викладачів

№	Тема	Опис	Матеріал теми (PDF-файл або презентація)	Посилання на код з конспекту	Посилання на Кахут*	Додаткові матеріали
1 семестр. Назва семестру.						
1.						
2.						
…						
2 семестр. Назва.						
1.						
…						

**Кахут (Kahoot) – ігрова навчальна платформа, що використовується в класі в школах та інших навчальних закладах.*

ДОДАТОК В. Перелік документів на оптичному носії

Пояснювальна_записка_Середняк.docx

Презентація_Середняк.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 93 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ім'я, прізвище)

ДОДАТОК Ґ.

ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
«Політика безпеки інформації інформаційно-комунікаційної системи закладу дистанційної освіти «GoITeens»
студентки групи 125-20-1
Середняк Катерини Олександрівни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 82 сторінках та містить 1 рисунок, 12 таблиць, 13 джерел та 5 додатків.

Метою кваліфікаційної роботи є забезпечення даного рівня безпеки інформації, яка обробляється в ІКС закладу дистанційної освіти «GoITeens».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІКС, розробка моделі порушника, аналіз кіберзагроз в ІКС, оцінка існуючих елементів політики безпеки, вибір моделі безпеки, розробка елементів політики безпеки та обґрунтування засобів їх реалізації.

Розроблені положення політики безпеки щодо: керування обліковими записами, ідентифікації та автентифікації, розмежування доступу, антивірусного захисту, використання власного обладнання, розповсюдження та копіювання інформаційних ресурсів та застосування водяних знаків.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей структури та організації інформаційної діяльності закладу дистанційної освіти «GoITeens».

До недоліків відноситься недостатньо обґрунтований перелік кіберзагроз.

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

За час дипломування Середняк К.О. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра 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 «_____».

Керівник кваліфікаційної роботи, професор **Корченко А.О.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**