МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ"

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Надія Святська
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-41

Надія Святська
Ім'я, ПРІЗВИЩЕ

Керівник: Тетяна Мужанова
к.держ.упр., доцент Ім'я, ПРІЗВИЩЕ

Рецензент:
Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Святській Надії Андріївні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к.держ.упр., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека, інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки, гейміфікація*.

4. Перелік питань, які мають бути розроблені:

4.1. Дослідити кращі практики формування обізнаності й навчання персоналу з інформаційної безпеки від NIST, ISO, ENISA.

4.2. Проаналізувати інноваційні технології навчання з інформаційної безпеки.

4.3. З’ясувати особливості гейміфікації у навчанні й підвищенні обізнаності персоналу з інформаційної безпеки й розробити програму курсу за напрямом.

Перелік ілюстративного матеріалу: *презентація PowerPoint*

5. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Дослідження кращих практик формування обізнаності й навчання персоналу з інформаційної безпеки.	08.04.2024	
4.	Аналіз інноваційних технологій навчання з інформаційної безпеки.	22.04.2024	
5.	Вивчення особливості гейміфікації у навчанні й підвищенні обізнаності персоналу з інформаційної безпеки й розробка програми курсу за напрямом.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Святська Н.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувачка СВЯТСЬКА Надія у кваліфікаційній роботі дослідила кращі практики формування обізнаності й навчання персоналу з інформаційної безпеки від провідних експертних організацій NIST, ISO, ENISA; проаналізувала інноваційні технології навчання з інформаційної безпеки; з'ясувала особливості гейміфікації у навчанні й підвищенні обізнаності персоналу з інформаційної безпеки й розробила програму курсу за напрямом.

СВЯТСЬКА Надія показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження, проявила себе як організований, самостійний дослідник і виконавець. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки СВЯТСЬКОЇ Надії на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Святська Н.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти СВЯТСЬКОЇ Надії
на тему “Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки”

Актуальність. Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки є надзвичайно важливими в сучасних умовах, коли кіберзагрози постійно еволюціонують. Ефективне навчання з інформаційної безпеки забезпечує персонал необхідними знаннями і навичками для розпізнавання та реагування на різноманітні кіберзагрози. Використання інноваційних методів та технологій дозволяє не тільки підвищити рівень обізнаності, але й забезпечити інтерактивне та практичне засвоєння матеріалу, що сприяє швидшому реагуванню на потенційні інциденти та зменшенню ризиків для організації.

З огляду на зазначене дослідження інноваційних технологій формування обізнаності й навчання персоналу з інформаційної безпеки є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено кращі практики формування обізнаності й навчання персоналу з інформаційної безпеки; проаналізовано інноваційні технології навчання з інформаційної безпеки.

2. Оформлення кваліфікаційної роботи відповідає встановленим вимогам. Виклад матеріалу здійснено логічно й послідовно, згідно з планом, зроблено змістовні висновки. Основні положення роботи представлено у вигляді рисунків.

3. Автор опрацювала значну джерельну базу, переважно англомовну, детально проаналізувала рекомендації щодо навчання й формування обізнаності від NIST, ISO, ENISA.

4. За результатами дослідження розроблено програму курсу підвищення обізнаності з інформаційної безпеки .

Недоліки.

Доцільно було б приділити більше уваги вивченню впливу конкретних інноваційних технологій на рівень обізнаності та навчання персоналу з інформаційної безпеки, а також порівнянню ефективності різних методів навчання.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувачка СВЯТСЬКА Надія заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню інноваційних технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 23 рисунка, висновків і списку використаних джерел із 54 найменувань. Загальний обсяг роботи становить 78 аркушів, з яких 5 аркушів займає список використаних джерел.

Метою роботи є дослідження інноваційних технологій формування обізнаності й навчання персоналу з інформаційної безпеки.

Об'єктом дослідження є управління персоналом у сфері інформаційної безпеки.

Предмет дослідження – інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, класифікації та порівняння, оцінки ефективності інноваційних технологій навчання, моделювання навчальних процесів, а також методи функціонального аналізу інструментів підвищення обізнаності персоналу з інформаційної безпеки.

Як результат у роботі досліджено кращі практики формування обізнаності й навчання персоналу з інформаційної безпеки від провідних експертних організацій NIST, ISO, ENISA; проаналізовано інноваційні технології навчання з інформаційної безпеки; з'ясовано особливості гейміфікації у навчанні й підвищенні обізнаності персоналу з інформаційної безпеки й розроблено програму курсу за напрямом.

Галузь застосування. Розроблені підходи можуть бути використані в управлінні інформаційною безпекою підприємства для підвищення ефективності процесів формування обізнаності й навчання персоналу з інформаційної безпеки, що сприятиме кращому розпізнаванню та реагуванню на актуальні й потенційні кіберзагрози.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ГЕЙМІФІКАЦІЯ.

ABSTRACT

The qualification work is devoted to the study of innovative technologies for creating awareness and training of information security personnel. The work consists of an introduction, three chapters containing 23 figures, conclusions and a list of 54 references. The total volume of the work is 78 pages, of which 5 pages are taken up by the list of references.

The purpose of the study is to investigate innovative technologies for creating awareness and training of information security personnel.

The object of the study is personnel management in the field of information security.

The subject of the study is innovative technologies for creating awareness and training of information security personnel.

Research methods. To solve the above scientific task, the methods of analysis, classification and comparison, evaluation of the effectiveness of innovative training technologies, modeling of educational processes, as well as methods of functional analysis of information security awareness tools were used.

As a result, the best practices of information security awareness and training from leading expert organizations NIST, ISO, ENISA were studied; innovative information security training technologies were analyzed; the features of gamification in training and raising awareness of information security personnel were found out and a course program in this area was developed.

Field of application. The developed approaches can be used in the management of enterprise information security to improve the efficiency of the processes of awareness raising and training of information security personnel, which will contribute to better recognition and response to current and potential cyber threats.

Keywords: INFORMATION SECURITY, INNOVATIVE TECHNOLOGIES FOR CREATING AWARENESS AND TRAINING OF INFORMATION SECURITY PERSONNEL, GAMIFICATION.

ЗМІСТ

ВСТУП

Актуальність теми. Інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки є важливим аспектом сучасного управління інформаційною безпекою. Впровадження цих технологій є ключовим елементом, оскільки вони дозволяють: ефективніше навчати працівників розпізнавати та реагувати на потенційні кіберзагрози, адаптувати методи навчання до нових загроз, зменшувати ризики, підвищувати загальний рівень безпеки організації та забезпечувати відповідність нормативним вимогам.

З огляду на зазначене дослідження значення розвідки загроз в управлінні інформаційною безпекою підприємства є актуальним науковим завданням.

Мета роботи полягає у дослідженні інноваційних технологій формування обізнаності й навчання персоналу з інформаційної безпеки.

Об'єкт дослідження **–** управління персоналом у сфері інформаційної безпеки.

Предмет дослідження – інноваційні технології формування обізнаності й навчання персоналу з інформаційної безпеки.

Для досягнення цієї мети в роботі необхідно виконати такі **завдання**:

1. Дослідити кращі практики формування обізнаності й навчання персоналу з інформаційної безпеки від NIST, ISO, ENISA.

2. Проаналізувати інноваційні технології навчання з інформаційної безпеки.

3. З'ясувати особливості гейміфікації у навчанні й підвищенні обізнаності персоналу з інформаційної безпеки й розробити програму курсу за напрямом.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та оцінки загроз і ризиків, моніторингу безпеки, інформаційної розвідки, моделювання навчальних процесів, а також функціонального аналізу інструментів підвищення обізнаності персоналу.

Практичне значення одержаних результатів. Впровадження розробки

дозволить зробити обґрунтований вибір методів та інструментів для формування обізнаності й навчання персоналу з інформаційної безпеки, що стане ключовим елементом управління інформаційною безпекою відповідно до бізнес-цілей, можливостей та ресурсів підприємства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 КРАЩІ ПРАКТИКИ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Важливим елементом управління персоналом організації є формування обізнаності й навчання у сфері інформаційної безпеки, завдяки чому забезпечується набуття працівниками необхідних знань і навичок щодо захисту інформації, виховання свідомого й відповідального ставлення до питань безпеки, розвиток корпоративної культури інформаційної безпеки, а, отже зростання ефективності запобігання і протидії загрозам безпеки.

Впровадження комплексу заходів із формування обізнаності й навчання у сфері інформаційної безпеки є обов'язковим завданням у рамках управління інформаційною безпекою організації. Для цього доцільно використовувати зразки кращих практик, які представлені у публікаціях і стандартах провідних експертних організацій, зокрема Міжнародної організації зі стандартизації ISO, Національного інституту стандартів і технологій США NIST, Європейського агентства з мережевої та інформаційної безпеки ENISA та інших.

1.1 Концепція NIST щодо розробки програми інформування й навчання з безпеки ІТ

Національний інститут стандартів і технологій (NIST) є наріжним каменем науково-технічного прогресу в Міністерстві торгівлі США. Заснований у 1901 році, NIST перетворився на всесвітньо визнану установу, яка сприяє інноваціям, промисловій конкурентоспроможності та економічному зростанню завдяки своїй місії розвитку науки про вимірювання, стандарти і технології. Завдяки різноманітному портфоліо, що охоплює фундаментальні дослідження в галузі фізики, інженерії та матеріалознавства, а також розробку передових технологій і стандартів, NIST відіграє ключову роль у формуванні майбутнього різних галузей і секторів.

У сфері інформаційної безпеки вплив і значення NIST особливо помітні. Усвідомлюючи гостру потребу у вирішенні нових викликів кібербезпеки та захисті цифрових активів і систем, NIST перебуває в лідерах з розробки всеосяжних і авторитетних стандартів, керівних принципів і найкращих практик у сфері кібербезпеки. Ці ресурси, які часто разом називають Рамковою основою кібербезпеки NIST, надають організаціям системний підхід до управління ризиками кібербезпеки, підвищення стійкості та забезпечення конфіденційності, цілісності та доступності інформації та інформаційних систем [1].

Значення стандартів NIST для інформаційної безпеки полягає в їхньому суворому та науково обґрунтованому підході до усунення загроз та вразливостей кібербезпеки. Залучаючи експертів галузі, урядові установи, наукові кола та міжнародних партнерів, стандарти NIST проходять ретельну розробку, перевірку та валідацію, щоб забезпечити їх точність, актуальність та застосовність до різних організаційних контекстів та викликів у сфері кібербезпеки.

Дотримуючись стандартів NIST, організації можуть створити надійну систему кібербезпеки, адаптовану до їхніх конкретних потреб і профілів ризиків. Ці рамки забезпечують структурований підхід до виявлення, оцінки та зменшення ризиків кібербезпеки, а також сприяють дотриманню регуляторних вимог та найкращих галузевих практик. Крім того, стандарти NIST слугують спільною мовою та орієнтиром для фахівців з кібербезпеки, політиків і зацікавлених сторін у всьому світі, сприяючи співпраці, сумісності та обміну інформацією в глобальній боротьбі з кіберзагрозами [2].

Отже, NIST відіграє ключову роль у формуванні інформаційної безпеки завдяки розробці та поширенню стандартів, керівних принципів і передового досвіду. Оскільки організації борються з дедалі складнішими кіберзагрозами, стандарти NIST забезпечують надійну та авторитетну основу для побудови стійкого захисту кібербезпеки, охорони критичної інфраструктури та захисту конфіденційної інформації у взаємопов'язаному та цифровому світі.

Спеціальна публікація NIST 800-50 «Розробка програми формування обізнаності й навчання з безпеки IT» 2003 року

Спеціальна публікація NIST 800-50, оприлюднена в 2003 році, містить вичерпні рекомендації щодо створення та підтримки ефективних програм підвищення обізнаності та навчання з питань безпеки в організаціях. Основні положення NIST SP 800-50 версії 2003 року показані на рис. 1.1.

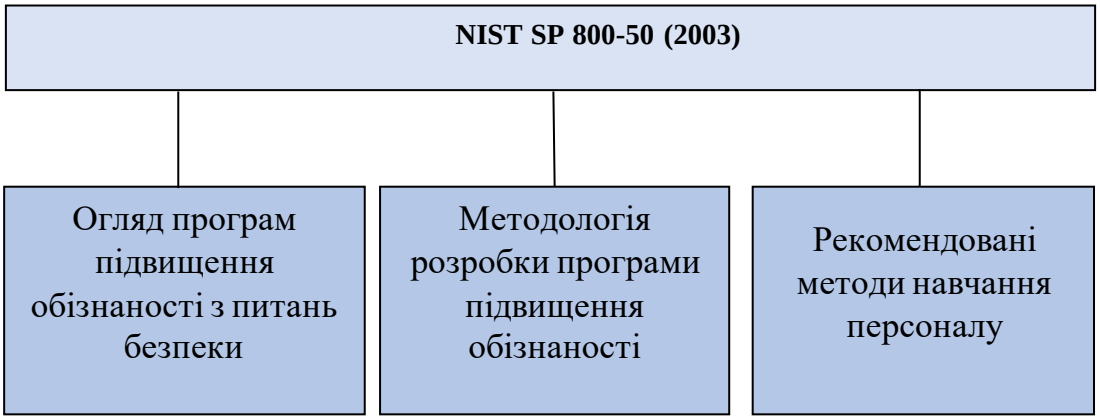


Рис. 1.1. Основні положення NIST SP 800-50 (2003)

1. *Огляд програм підвищення обізнаності з питань безпеки*:

стандарт окреслює важливість підвищення обізнаності та навчання з питань безпеки для зменшення ризиків кібербезпеки та формування культури безпеки в організаціях. Вона підкреслює роль програм підвищення обізнаності в навчанні персоналу щодо політик, процедур і найкращих практик безпеки для зменшення ймовірності інцидентів і порушень безпеки [3].

2. Методологія створення програми підвищення обізнаності:

NIST SP 800-50 пропонує структуровану методологію для розробки та впровадження програми підвищення обізнаності з питань безпеки. Ця методологія включає оцінку потреб і завдань організації, визначення цільової аудиторії, визначення цілей і завдань програми, вибір відповідних методів навчання і матеріалів, а також встановлення показників для оцінки ефективності програми.

3. Рекомендовані методи навчання персоналу:

стандарт рекомендує різноманітні методи та прийоми навчання для ефективного ознайомлення персоналу з темами, пов'язаними з безпекою. Ці методи можуть включати навчальні заняття в класі, онлайн-курси, інтерактивні семінари, імітаційні вправи з фішингу та рольові ігри. NIST SP 800-50

підкреслює важливість адаптації навчальних програм до конкретних потреб і навчальних уподобань різних груп аудиторії в організації [4].

Спеціальна публікація NIST 800-50 «Створення навчальної програми з кібербезпеки та конфіденційності» 2023 року

Спеціальна публікація NIST 800-50, оприлюднена у 2023 році, містить оновлені та вичерпні рекомендації щодо створення та підтримки ефективних програм підвищення обізнаності та навчання з питань кібербезпеки та конфіденційності в організаціях. Основні положення NIST SP 800-50 версії 2023 року включають інтеграцію конфіденційності з кібербезпекою, впровадження моделі життєвого циклу для постійних ітераційних поліпшень, використання сучасних рекомендацій і термінології NIST, розробку навчальних програм, що відповідають організаційним цілям з управління ризиками, створення культури кібербезпеки та конфіденційності, а також застосування метрик та методів оцінювання для регулярного вдосконалення програм [5]. Основні положення NIST SP 800-50 версії 2023 року показані на Рис. 1.2.

Рис. 1.2. Основні положення NIST SP 800-50 (2023)

1. *Огляд програм підвищення обізнаності про безпеку:*

Програми підвищення обізнаності з питань безпеки мають важливе значення для забезпечення того, щоб працівники організації були добре поінформовані та підготовлені до реагування на ризики кібербезпеки та конфіденційності. Ці програми, такі як Навчальна програма з кібербезпеки та конфіденційності (CPLP), розроблені для надання комплексних рекомендацій щодо заходів з підвищення обізнаності, рольових тренінгів та освітніх програм [6].

Основна мета цих програм - сформувати глибоке розуміння ризиків кібербезпеки та навчити персонал розуміти свою роль у виявленні, управлінні та пом'якшенні цих ризиків. Інтеграція цих програм у стратегічне планування організації має вирішальне значення для формування культури безперервного навчання та управління ризиками, гарантуючи, що всі співробітники, від загального персоналу до спеціалізованих ролей, мають необхідні знання та навички.

2. *Методологія створення програми підвищення обізнаності:*

Створення ефективної програми підвищення обізнаності з питань безпеки передбачає кілька важливих кроків, починаючи з ретельного аналізу конкретних потреб і ризиків організації. Це включає визначення ключових ролей в організації, які потребують спеціалізованої підготовки, та визначення цілей навчання для кожної ролі. Програма повинна включати різноманітні методи навчання, такі як практичні вправи, симуляції та безперервні заходи з підвищення обізнаності, адаптовані до різних рівнів робочої сили. Важливо узгодити програму з цілями організації та розробити чітку стратегію, яка включає вимірювані цілі і тактику. Регулярна оцінка та механізми зворотного зв'язку необхідні для того, щоб програма залишалася актуальною та ефективною, дозволяючи вносити постійні корективи та вдосконалення на основі зворотного зв'язку та еволюції загроз [7].

3. *Рекомендовані методи навчання персоналу:*

Навчання персоналу в рамках програми підвищення обізнаності з питань безпеки має бути багатогранним, спрямованим на задоволення як загальних, так і спеціальних потреб. Для загального персоналу навчання часто включає щорічні тренінги з кібербезпеки та конфіденційності, інформаційні кампанії та практичні вправи, такі як симуляції фішингу. Для тих, хто має значні обов'язки з кібербезпеки, вирішальне значення має рольова підготовка, яка зосереджується на конкретних завданнях та обов'язках, пов'язаних з їхніми ролями. Рекомендуються такі методи, як практичні лабораторні роботи, вправи на основі сценаріїв, а також постійний професійний розвиток через курси підвищення кваліфікації та сертифікацію. Навчання також повинно включати регулярні оновлення та курси підвищення кваліфікації, щоб весь персонал був в курсі новітніх практик безпеки та нових загроз, що сприятиме проактивному підходу до кібербезпеки в організації [8].

Спеціальна публікація NIST 800-50 слугує цінним ресурсом для організацій, які прагнуть розробити, впровадити та вдосконалити програми підвищення обізнаності та навчання з питань безпеки. Дотримуючись рекомендацій, наведених у публікації, організації можуть посилити свою кібербезпеку, зменшити ризик інцидентів безпеки та надати персоналу можливість відігравати активну роль у захисті конфіденційної інформації та активів [9].

1.2 Настанови щодо інформування, освіти й навчання з інформаційної безпеки відповідно до стандартів ISO 27к

Міжнародна організація зі стандартизації (ISO) – це всесвітньо визнана організація, яка розробляє та публікує міжнародні стандарти в різних галузях і секторах. Заснована в 1947 році, ISO об'єднує країни-члени з усього світу, кожна з яких робить свій внесок у розробку стандартів на основі консенсусу, що сприяють інноваціям, ефективності та сумісності в глобальному масштабі.

Стандарти ISO охоплюють широкий спектр тем, включаючи управління якістю, екологічний менеджмент, інформаційні технології та кібербезпеку.

У сфері інформаційної безпеки ISO розробила кілька стандартів, які відіграють вирішальну роль у забезпеченні конфіденційності, цілісності та доступності інформаційних активів в організаціях. Одним з найбільш відомих стандартів є ISO/IEC 27001, який забезпечує всеосяжну основу для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). ISO/IEC 27001 визначає вимоги та найкращі практики для виявлення ризиків безпеки, впровадження засобів контролю для зменшення цих ризиків, а також моніторингу й оцінки ефективності заходів безпеки.

Загалом, роль стандартів ISO у забезпеченні інформаційної безпеки є першорядною, оскільки вони надають організаціям міжнародно визнані рамки та настанови для ефективного управління ризиками кібербезпеки та захисту чутливих інформаційних активів. Прийнявши стандарти ISO, організації можуть підвищити свою стійкість до кіберзагроз, побудувати довіру з клієнтами та зацікавленими сторонами, а також продемонструвати свою прихильність до захисту інформації у все більш взаємопов'язаному та цифровому світі [10].

Центральне місце у впровадженні ISO/IEC 27002 займає акцент на навчанні та підвищенні обізнаності всередині організації.

Навчання та інформування відіграють життєво важливу роль у забезпеченні успіху СУІБ, надаючи персоналу знання, навички та обізнаність, необхідні для захисту конфіденційних інформаційних активів та зменшення ризиків безпеки. Це включає в себе навчання співробітників політикам, процедурам та найкращим практикам безпеки, а також проведення спеціальних тренінгів щодо засобів контролю безпеки та процедур реагування на інциденти. Розвиваючи культуру обізнаності в питаннях безпеки, організації можуть навчити своїх співробітників розпізнавати загрози безпеці та реагувати на них на випередження, зменшуючи ймовірність інцидентів і порушень безпеки.

Основні властивості інформаційної безпеки, на яких наголошується в стандарті ISO/IEC 27002, включають конфіденційність, цілісність і доступність. Ці властивості формують основний принцип інформаційної безпеки, гарантуючи, що дані захищені від несанкціонованого доступу, залишаються точними і незмінними, а також доступні в разі потреби.

Концепції кібербезпеки в цих рамках зосереджені на принципі захисту. Це передбачає захист інформаційних систем від загроз і вразливостей, які можуть поставити під загрозу їхню безпеку. Захист даних і систем є фундаментальним елементом кібербезпеки, що вимагає постійного моніторингу та проактивних механізмів захисту для зменшення ризиків.

Операційні можливості також розглядаються в стандарті, зокрема, безпека людських ресурсів. Це стосується забезпечення того, щоб персонал був належним чином підготовлений і усвідомлював свої ролі та обов'язки щодо інформаційної безпеки. Безпека людських ресурсів охоплює такі заходи, як перевірка документів, контроль доступу та постійні навчальні програми для підтримання безпечного організаційного середовища [11].

Розглянуті безпекові напрямки охоплюють управління та функціонування інфраструктури. Управління відноситься до політик, процедур і рамок, які визначають підхід організації до інформаційної безпеки. Воно передбачає встановлення чітких положень і стандартів для управління інформаційними активами та їх захисту. Принцип функціонування інфраструктури визнає взаємопов'язану сутність сучасних інформаційних систем і необхідність цілісного підходу до безпеки, що враховує всі компоненти та зацікавлені сторони в системі.

Підхід з точки зору управління підкреслює, що персонал і зацікавлені сторони повинні регулярно отримувати оновлення щодо політики інформаційної безпеки організації, а також специфічних політик і процедур, що стосуються їхніх посадових обов'язків. Таке безперервне навчання гарантує, що всі особи будуть поінформовані про найновіші технології безпеки, загрози та стратегії їх усунення.

Мета цих заходів полягає в тому, щоб персонал і відповідні зацікавлені сторони повністю усвідомлювали та виконували свої обов'язки з інформаційної безпеки. Розвиваючи культуру обізнаності з питань безпеки та безперервної освіти, організації можуть краще захистити свої інформаційні активи, зменшити ризик порушень безпеки та забезпечити дотримання відповідних норм і стандартів.

У рекомендаціях щодо створення програми інформування, навчання та підготовки з інформаційної безпеки підкреслюється необхідність її узгодження з загальною політикою інформаційної безпеки організації, а також з конкретними політиками та процедурами, що стосуються інформаційної безпеки. Таке узгодження має вирішальне значення для забезпечення того, щоб навчальна програма відповідала унікальним потребам і ризикам, пов'язаним з інформаційними активами організації. Програма повинна бути розроблена з повним розумінням особливостей інформації, яка потребує захисту, а також засобів управління безпекою, що вже існують для захисту цієї інформації.

Ще одним важливим фактором є особиста відповідальність. Працівники повинні усвідомлювати свою відповідальність за свої дії та бездіяльність щодо інформаційної безпеки. Це включає в себе розуміння своєї ролі в забезпеченні або захисті інформації, яка належить організації та її зацікавленим сторонам. Виховання почуття особистої відповідальності заохочує проактивну поведінку та пильність у дотриманні протоколів безпеки. Особисту відповідальність можна підвищити шляхом чіткого інформування про індивідуальні обов'язки та наслідки невиконання вимог безпеки.

Новий персонал повинен пройти початковий тренінг для ознайомлення з політикою безпеки організації та своїми конкретними обов'язками. Крім того, особи, які переходять на нові посади з суттєво відмінними вимогами до безпеки, повинні пройти цільову підготовку для вирішення нових завдань та очікувань, пов'язаних з їхніми посадами.

Оцінка розуміння персоналу по завершенню кожного навчального заходу має важливе значення для оцінки ефективності навчальної програми. Таке

оцінювання може відбуватися у різних формах, наприклад, у вигляді тестів, практичних вправ або дискусій, і має на меті виміряти передачу знань і переконатися, що учасники засвоїли ключові концепції та практики. Результати такого оцінювання дають цінний зворотний зв'язок, який можна використати для вдосконалення майбутніх навчальних сесій, щоб вони залишалися актуальними та ефективними [12].

Крім того, програма повинна бути динамічною, здатною розвиватися у відповідь на нові виклики інформаційній безпеці та технологічні досягнення. Така адаптивність гарантує, що система безпеки організації залишатиметься надійною та реагуватиме на мінливий характер загроз. Необхідно регулярно оновлювати навчальний контент, щоб враховувати останні тенденції в галузі інформаційної безпеки, регуляторні зміни та найкращі практики.

Плануючи програму підвищення обізнаності, важливо враховувати різноманітні ролі персоналу в організації, включаючи як внутрішній персонал, так і зовнішній, наприклад, консультантів і постачальників. Програма має бути систематично розписана в часі, з регулярними заходами, які закріплюють ключові концепції та практики безпеки.

Ефективна комунікація є ще одним важливим елементом навчальної програми. Навчання має бути цікавим і доступним, з використанням різноманітних форматів, таких як лекції, інтерактивні семінари, онлайн-курси та практичні вправи. Така різноманітність допомагає пристосуватися до різних стилів навчання і гарантує, що всі учасники зможуть ефективно засвоїти матеріал.

Кінцевою метою програми підвищення обізнаності, навчання та тренінгів з інформаційної безпеки є створення культури безпеки в організації. Переконавшись, що весь персонал розуміє свої ролі та обов'язки щодо інформаційної безпеки, організація може значно знизити ризик порушень безпеки та забезпечити дотримання відповідних стандартів і правил. Добре впроваджена програма навчання сприяє проактивному підходу до інформаційної

безпеки, коли працівники не лише усвідомлюють потенційні ризики, але й володіють знаннями та навичками для їх ефективного зменшення.

При розробці програми підвищення обізнаності про інформаційну безпеку важливо враховувати не тільки "що" і "як", але й "чому", що стоять за ініціативами. Розуміння мети та важливості інформаційної безпеки має важливе значення для того, щоб персонал повністю усвідомив її вплив на організацію. Таке розуміння має включати як позитивні результати ретельних практик безпеки, так і потенційні негативні наслідки порушень або недотримання вимог безпеки. Наголошуючи на обґрунтуванні заходів безпеки, працівники з більшою ймовірністю будуть цінувати свої ролі та обов'язки, тим самим сприяючи формуванню культури проактивної обізнаності щодо безпеки.

1.3 Структурований підхід до розробки навчальних програм з кібербезпеки ENISA

Європейське агентство з мережевої та інформаційної безпеки (ENISA) є важливою установою в Європейському Союзі, що зосереджує свою діяльність на зміцненні кібербезпеки в державах-членах. Створене у 2004 році під наглядом Європейської Комісії, ENISA є центральним агентством ЄС з питань експертизи, співробітництва та обміну інформацією у сфері кібербезпеки.

Місія ENISA полягає у створенні надійного середовища кібербезпеки в ЄС, що сприяє загальній цифровій стійкості Союзу. Для виконання цієї місії ENISA переслідує кілька ключових цілей, включаючи підтримку країн-членів ЄС шляхом надання експертних консультацій та технічної допомоги. Крім того, ENISA сприяє співпраці та обміну інформацією між країнами-членами та іншими інституціями, агентствами та міжнародними партнерами ЄС. ENISA також намагається підвищити обізнаність про загрози та ризики кібербезпеки серед громадян ЄС, бізнесу та органів державної влади за допомогою різних інформаційно-просвітницьких заходів та освітніх ініціатив. Крім того, ENISA підтримує розробку політики та законодавства ЄС у сфері кібербезпеки,

пропонуючи технічну експертизу та консультації. Нарешті, ENISA сприяє дослідженням та інноваціям у сфері кібербезпеки, сприяючи співпраці між промисловістю, науковими колами та науково-дослідними установами, тим самим сприяючи розвитку технологій та рішень у сфері кібербезпеки. Загалом, ENISA відіграє життєво важливу роль у просуванні кібербезпеки в ЄС, прагнучи побудувати більш безпечне і надійне цифрове середовище для всіх зацікавлених сторін [13].

ENISA, агентство Європейського Союзу з кібербезпеки, пропонує вичерпні рекомендації щодо ініціатив з підвищення обізнаності та навчання, спрямованих на посилення стійкості до кібербезпеки в країнах-членах. Ці настанови містять цінні рекомендації для організацій, які прагнуть розробити ефективні програми з підвищення обізнаності та навчання.

Основні рекомендації ENISA підкреслюють важливість адаптації зусиль з підвищення обізнаності та навчання до конкретних потреб і особливостей організації. Вони пропагують проактивний підхід, який інтегрує кібербезпеку в організаційну культуру та сприяє спільній відповідальності за безпеку серед усього персоналу. Крім того, ENISA підкреслює важливість безперервної освіти та взаємодії для ефективної протидії кіберзагрозам, що еволюціонують.

З точки зору методології ENISA пропонує структурований підхід до розробки навчальних програм, показаний на рис. 1.3.

Ця методологія передбачає проведення ретельної оцінки потреб у навчанні, визначення цілей програми та цільової аудиторії, вибір відповідних методів навчання та матеріалів, а також оцінку ефективності програми. Дотримуючись цієї методології, організації можуть гарантувати, що їхні навчальні програми відповідають їхнім цілям безпеки та адаптовані до потреб їхнього персоналу.

Рис. 1.3. Етапи розробки навчальних програм

ENISA також пропонує ряд інструментів і ресурсів для підтримки програм підвищення обізнаності та навчання. До них відносяться навчальні онлайн-курси, матеріали для підвищення обізнаності, посібники з найкращих практик та набори інструментів, які організації можуть використовувати для розробки своїх навчальних ініціатив. Крім того, ENISA надає доступ до експертних порад та допомоги через семінари, вебінари та платформи для співпраці, що дозволяє організаціям скористатися досвідом та рекомендаціями агентства [14].

Загалом, керівні принципи ENISA щодо підвищення обізнаності та навчання надають цінну інформацію та ресурси для організацій, які прагнуть посилити свої позиції в галузі кібербезпеки. Використовуючи рекомендації, методологію та інструменти ENISA, організації можуть розробити ефективні програми підвищення обізнаності та навчання, які дозволять персоналу розпізнавати кіберзагрози й проактивно реагувати на них, тим самим зміцнюючи загальну стійкість до кіберзагроз.

ENISA пропонує практичні приклади та ідеї, почерпнуті з успішних програм підвищення обізнаності й навчання, реалізованих різними організаціями. Ці приклади демонструють найкращі практики й інноваційні підходи, які довели свою ефективність у підвищенні обізнаності та стійкості до кіберзагроз.

Вивчаючи ці тематичні дослідження, організації можуть отримати цінну інформацію про стратегії, методології та інструменти, що використовуються в успішних програмах підвищення обізнаності та навчання. Наприклад, вони можуть дізнатися про важливість залучення підтримки керівництва, адаптації навчального контенту до різних груп аудиторії, використання інтерактивних та цікавих методів навчання, а також формування культури безперервного навчання та вдосконалення.

Крім того, ENISA робить висновки та рекомендації на основі свого досвіду та спостережень, отриманих під час аналізу цих тематичних досліджень. Ці висновки висвітлюють ключові фактори успіху, загальні виклики та уроки, отримані в результаті реалізації ініціатив з підвищення обізнаності та навчання. Рекомендації ENISA є практичним керівництвом для організацій, які прагнуть розробити або вдосконалити власні програми підвищення обізнаності та навчання, пропонуючи дієві ідеї та стратегії для підвищення стійкості до кібербезпеки [15].

Загалом, практичні приклади, тематичні дослідження, висновки та рекомендації ENISA пропонують цінну інформацію та рекомендації для організацій, які прагнуть посилити свої зусилля з підвищення обізнаності та навчання з питань кібербезпеки. Використовуючи експертизу ENISA та навчаючись на реальному досвіді, організації можуть розробити ефективні стратегії та підходи для розбудови культури безпеки та стійкості у власному середовищі.

Висновки до розділу 1

Встановлено, що формування обізнаності й навчання персоналу з питань інформаційної безпеки є важливим елементом управління інформаційною безпекою організації. Завдяки впровадженню комплексних заходів навчання та підвищення обізнаності, працівники набувають необхідних знань і навичок для

захисту інформації, що сприяє вихованню свідомого та відповідального ставлення до питань безпеки.

Дослідження показало, що використання кращих практик, представлених у публікаціях і стандартах провідних експертних організацій, таких як ISO, NIST та ENISA, забезпечує ефективність програм навчання та обізнаності. Зокрема, концепція NIST щодо розробки програм підвищення обізнаності та навчання з кібербезпеки та конфіденційності, а також рекомендації ENISA пропонують структурований підхід до створення ефективних програм, що включає оцінку потреб, визначення цілей, вибір методів навчання та матеріалів, а також оцінку ефективності програм. Важливим аспектом є також постійне оновлення навчального контенту та інтеграція новітніх тенденцій і технологій у програми навчання, що забезпечує проактивний підхід до кібербезпеки.

Таким чином, формування обізнаності й навчання персоналу з інформаційної безпеки сприяє підвищенню загальної стійкості організації до кіберзагроз, зниженню ризику порушень безпеки та забезпеченню дотримання відповідних стандартів і норм.

Розділ 2 ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сфері інформаційної безпеки, як і в багатьох інших галузях, освіта відіграє ключову роль у формуванні компетентних фахівців, здатних протидіяти загрозам та забезпечувати захист інформаційних систем. Протягом багатьох десятиліть основними засобами передачі знань залишалися традиційні методи навчання, які включають лекції, семінари, практичні заняття та використання підручників. Ці методи забезпечували базову теоретичну підготовку та ознайомлення студентів з основами інформаційної безпеки.

Однак, з розвитком технологій і зростанням складності інформаційних загроз, традиційні методи навчання виявилися недостатніми для повноцінної підготовки спеціалістів. Сучасний світ вимагає від фахівців не лише глибоких теоретичних знань, але й практичних навичок, швидкої адаптації до нових викликів та здатності до постійного навчання. Саме ці виклики зумовлюють необхідність впровадження інноваційних технологій навчання, які можуть забезпечити ефективнішу та комплекснішу підготовку майбутніх фахівців з інформаційної безпеки.

2.1 Традиційні методи навчання та їх обмеження

У традиційних методах навчання процес орієнтований переважно на викладача, який є суб'єктом навчання, тоді як студенти виступають об'єктами його викладацького впливу. Основні етапи традиційних методів навчання можна охарактеризувати як викладання, засвоєння та відтворення матеріалу. Вважається, що результатом такого навчання є стійка сукупність знань. Ефективність навчання залежить в основному від методів та прийомів викладача. Тому основна увага приділяється пошуку та обґрунтуванню ефективних методів викладання, тоді як особливості пізнавальної активності студентів зазвичай не враховуються [16].

Традиційні засоби навчання можна класифікувати на шість основних категорій (Рис. 2.1).

Рис. 2.1. Види традиційних засобів навчання

Перша категорія включає підручники та інші друковані матеріали, такі як навчальні посібники, довідники, спеціальна література і методичні рекомендації. Ці засоби є фундаментальними для теоретичного навчання, забезпечуючи студентів необхідною базою знань.

Друга категорія складається з простих візуальних засобів, до яких належать моделі, діаграми, графіки тощо. Вони сприяють візуалізації складних концепцій та покращують розуміння навчального матеріалу. Третя категорія охоплює механічні візуальні засоби, такі як діаскопи та телескопи, які використовуються для детального вивчення об'єктів і явищ, що сприяє глибшому засвоєнню матеріалу.

Четверта категорія включає аудіозасоби, як-от магнітофони та інші пристрої для відтворення звуку. Вони дозволяють студентам слухати лекції, аудіокниги або інші навчальні матеріали, що може бути особливо корисним для тих, хто краще сприймає інформацію на слух. П'ята категорія складається з аудіовізуальних засобів, таких як відеокамери та інші пристрої для запису і

відтворення відео. Ці засоби поєднують візуальну та аудіоінформацію, що робить навчання більш інтерактивним і динамічним [17].

Шоста категорія включає засоби, які автоматизують процес навчання, наприклад, тренажери та комп'ютери. Вони дозволяють студентам виконувати практичні завдання, моделювати різні ситуації та отримувати миттєвий зворотний зв'язок, що значно покращує якість навчання. Кожна з цих категорій має свої переваги і недоліки, і їх ефективне використання залежить від контексту навчання та конкретних навчальних цілей.

За характером подання інформації засоби навчання можна розділити на словесні та візуальні, або наочні. Словесні засоби включають підручники, навчальні посібники, довідники та інші друковані матеріали. Вони передають інформацію через текст і вербальні пояснення, що допомагає студентам розвивати теоретичні знання та мовні навички.

Візуальні (наочні) засоби, до яких належать діаграми, графіки, моделі, діаскопи, відеокамери та інші візуалізаційні інструменти, сприяють кращому розумінню та запам'ятовуванню інформації шляхом візуального сприйняття. Вони допомагають студентам краще уявити абстрактні концепції та складні процеси, що робить навчання більш інтерактивним та захоплюючим.

Етапи пояснювально-ілюстративного навчання включають кілька ключових кроків, які забезпечують ефективне засвоєння матеріалу (Рис. 2.2).

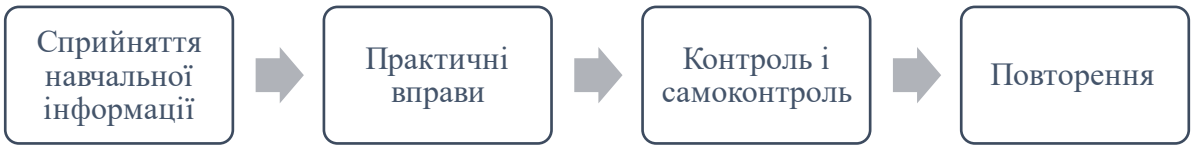


Рис. 2.2. Етапи пояснювально-ілюстративного навчання

Спершу студенти отримують та узагальнюють нову інформацію, засвоюючи основні поняття, закони та теорії. Викладач пояснює матеріал, використовуючи різноманітні ілюстрації та приклади для кращого розуміння. Далі слідують практичні вправи, що сприяють поглибленню знань, їх закріпленню, а

також формуванню умінь і навичок. Студенти вчаться застосовувати отримані знання в нових ситуаціях, що розвиває їх практичні навички.

Наступний крок включає контроль і самоконтроль ефективності засвоєння знань, умінь і навичок. Викладач проводить контрольні роботи, тести або інші форми оцінювання, а студенти мають можливість здійснити самоконтроль своєї роботи та визначити, наскільки добре вони засвоїли матеріал. Завершується процес повторенням вивченого матеріалу для його закріплення та кращого запам'ятовування. Це допомагає студентам систематизувати знання та підготуватися до подальшого навчання [18].

Традиційні методи навчання, хоча й широко застосовуються, мають певні обмеження, які можуть перешкоджати ефективному засвоєнню знань. Одним із головних недоліків є брак інтерактивності. Лекції та письмові матеріали часто сприяють пасивному навчанню, коли учні отримують інформацію без активної взаємодії з її змістом. Така пасивність може знижувати мотивацію і якість запам'ятовування, оскільки учням важко встановити зв'язок з матеріалом на глибшому рівні.

Традиційні методи викладання зазвичай застосовують однаковий підхід до всіх учнів, незалежно від їхніх індивідуальних стилів навчання, вподобань чи рівня володіння мовою. Відсутність індивідуального підходу може призводити до розсіювання уваги та неефективного засвоєння матеріалу для тих учнів, які потребують інших стратегій викладання для кращого розуміння складних концепцій. Це може негативно вплинути на результати навчання, оскільки кожен учень має свої унікальні потреби та спосіб сприйняття інформації.

Іншим важливим обмеженням традиційних методів є обмежена можливість ефективно відстежувати прогрес учнів. Традиційні методи часто бракують надійних механізмів для моніторингу успішності учнів у часі. Без своєчасного зворотного зв'язку та даних оцінювання викладачам важко визначити, в яких саме сферах учні потребують додаткової підтримки або втручання. Це може затримувати навчальний процес і призводити до того, що учні не отримують необхідної допомоги вчасно.

Традиційні методи навчання також часто фокусуються на передачі фактологічного матеріалу, що може перевантажувати пам'ять учнів і не сприяє розвитку критичного мислення і творчого підходу. Вони здебільшого не враховують індивідуальні особливості студентів, що може знижувати ефективність навчання. Крім того, застосування однотипних, переважно репродуктивних методів навчання обмежує можливості для самостійної творчої пізнавальної діяльності учнів [19].

Отже, традиційні технології навчання характеризуються кількома ключовими рисами:

– Засвоєння знань у вигляді фактологічного матеріалу та понятійного апарату чітко регламентується навчальними програмами.

– Формування умінь здійснюється на репродуктивному рівні і доводиться до автоматизму.

– У спілкуванні між викладачем і студентами переважає авторитарний стиль, де провідна роль у подачі навчального матеріалу належить викладачу.

– Обов’язком студентів є навчання, хоча мотивація в таких умовах відходить на другий план, а єдиним стимулом залишається оцінка.

– Основною формою навчання є фронтальна, коли вся група студентів під безпосереднім керівництвом викладача виконує спільне завдання.

Традиційні технології навчання мають і свої недоліки, серед яких:

– Пам’ять студентів перевантажується фактологічним матеріалом, обсяг якого постійно зростає.

– Обмаль можливостей для самостійної творчої пізнавальної діяльності.

– Індивідуальні особливості студентів не враховуються, а методи навчання є однотипними, головним чином репродуктивними.

2.2 Особливості інноваційних методів навчання

Інноваційні технології навчання – це систематичне і послідовне практичне втілення заздалегідь спроектованого навчально-виховного процесу, що являє собою проект певної педагогічної системи, реалізованої на практиці. Вони охоплюють сферу практичних взаємодій студента та викладача у різноманітних видах діяльності, зорганізованих на засадах чіткого цілепокладання, систематизації та алгоритмізації прийомів навчання.

Інноваційні технології представляють собою системну сукупність і порядок функціювання всіх особистісних, інструментальних та методологічних засобів, що використовуються для досягнення викладацької мети. Це також технологічно розроблені навчальні системи, що включають систему методів та прийомів професійної роботи викладача, методики та окремі методи виховання. Вони є частиною педагогічної науки, яка вивчає і розробляє мету, зміст та методи навчання, проектує педагогічні процеси та забезпечує їх ефективне функціювання. Інноваційні технології передбачають послідовну взаємозалежну систему дій педагога, спрямовану на розв’язання педагогічних завдань, та планомірне і послідовне втілення на практиці заздалегідь спроектованого педагогічного процесу [20].

Підходи інноваційного навчання показані на рис. 2.3.

Електронне навчання, або е-навчання, стало популярною альтернативою традиційним методам навчання, пропонуючи численні переваги для організацій. Однією з ключових особливостей електронного навчання є використання онлайн-курсів і вебінарів, які дозволяють учням отримувати доступ до навчальних матеріалів і лекцій дистанційно через Інтернет. Це забезпечує значну гнучкість, оскільки працівники можуть брати участь у навчальних сесіях з будь-якого місця, де є доступ до Інтернету, усуваючи необхідність фізичної присутності в аудиторії та зменшуючи логістичні обмеження.

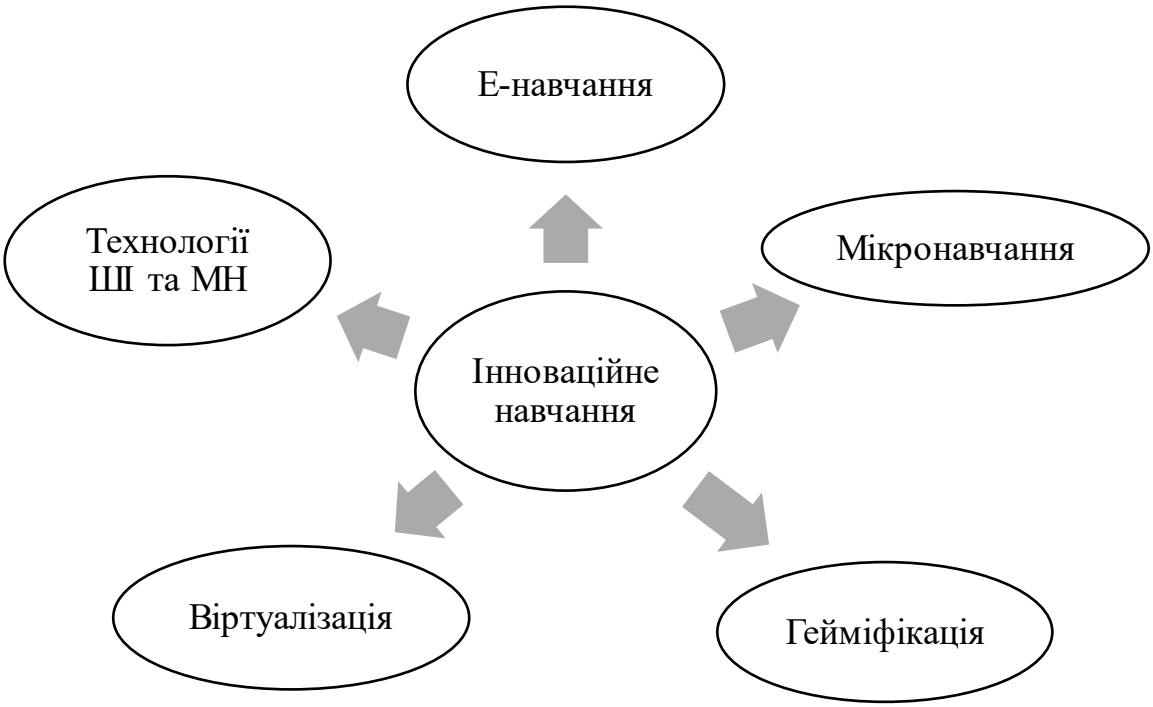


Рис. 2.3. Підходи інноваційного навчання

Інтерактивні навчальні платформи є ще однією відмінною рисою електронного навчання, надаючи учням цікавий і захоплюючий навчальний досвід. Ці платформи часто містять мультимедійний контент, такий як відео, анімації та інтерактивні симуляції, а також інструменти для спільної роботи, такі як дискусійні форуми та віртуальні класи. Активно залучаючи учнів до навчального процесу, інтерактивні платформи покращують запам'ятовування і засвоєння знань.

Крім того, електронне навчання значно полегшує дистанційне навчання, роблячи навчальні матеріали доступними для учнів у будь-який час. Ця асинхронна модель навчання дозволяє працівникам навчатися у власному темпі та за власним графіком, враховуючи різноманітні стилі навчання та вподобання. Учні мають можливість отримати доступ до матеріалів курсів, лекцій та оцінок у зручний для них час, що дозволяє поєднувати навчання з іншими робочими та особистими зобов'язаннями [21].

Загалом, електронне навчання пропонує організаціям гнучкий, економічно ефективний і масштабований підхід до навчання та професійного розвитку.

Використання онлайн-курсів, вебінарів, інтерактивних платформ та можливостей дистанційного навчання дозволяє організаціям надавати працівникам високоякісний навчальний досвід, який покращує їхні навички, знання та продуктивність. Це також дозволяє враховувати індивідуальні потреби та уподобання кожного працівника, що робить процес навчання більш персоналізованим і ефективним.

Електронне навчання також сприяє значному зниженню витрат, пов'язаних із навчанням. Відсутність необхідності фізичної присутності зменшує витрати на транспорт, проживання та оренду навчальних приміщень. Крім того, електронні ресурси можна легко оновлювати та розповсюджувати, що забезпечує актуальність і своєчасність навчальних матеріалів. Риси електронного навчання показані на рис. 2.4.

Рис. 2.4. Риси електронного навчання

Таким чином, електронне навчання є сучасним рішенням для організацій, що прагнуть забезпечити своїм працівникам високоякісну, гнучку та доступну освіту. Використовуючи сучасні технології, організації можуть ефективно підвищувати рівень знань і навичок своїх працівників, сприяючи їх професійному зростанню та підвищенню продуктивності [22].

Мікронавчання є сучасним підходом до освіти, який передбачає надання коротких, цілеспрямованих навчальних модулів, спеціально розроблених для вирішення конкретних завдань або тем. Ці модулі є стислими та легко

адаптованими до робочого графіку і навчальних уподобань працівників, що робить їх особливо зручними для інтеграції в щоденний розпорядок. Однією з ключових особливостей мікронавчання є його акцент на ефективності та стислій подачі інформації. Розбиваючи складні теми на невеликі порції, мікронавчання дозволяє учням ефективніше засвоювати і зберігати знання. Цей підхід є ідеальним для працівників із напруженим графіком або обмеженою концентрацією уваги, оскільки дозволяє їм опрацьовувати навчальний контент короткими, керованими кроками.

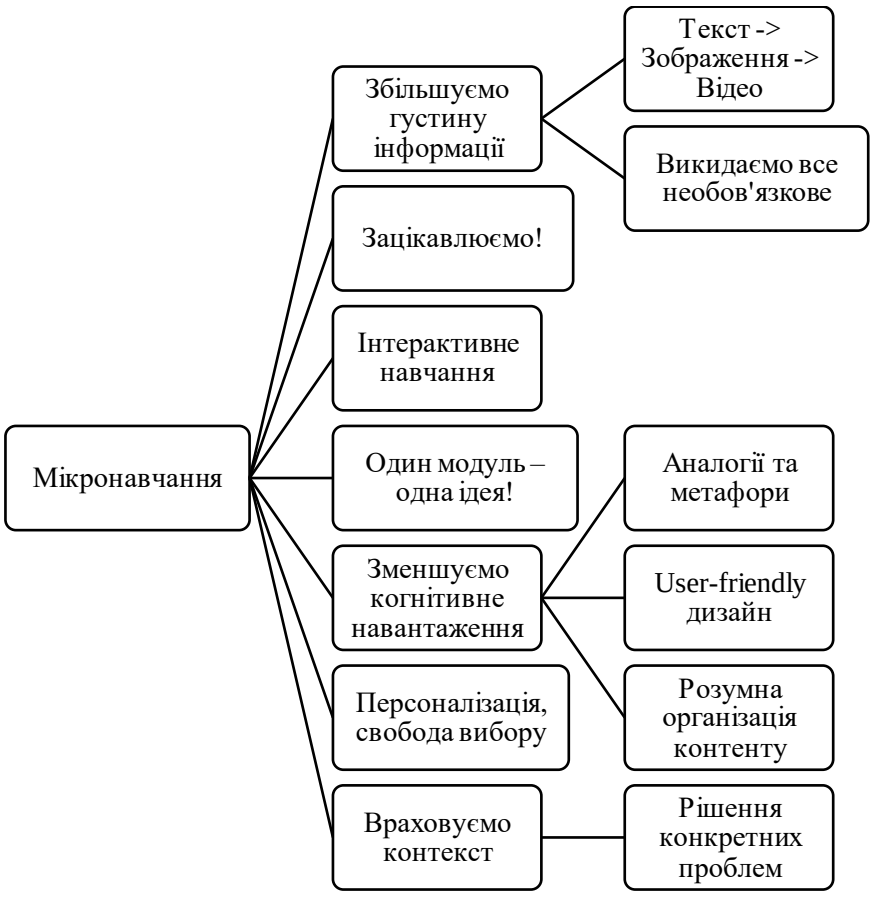


Рис. 2.5. Характеристики мікронавчання [23]

Мікронавчальні модулі часто включають мультимедійні елементи, такі як відео, інфографіку та інтерактивні компоненти, щоб підвищити зацікавленість і полегшити навчання. Відео забезпечують візуальну та слухову стимуляцію, що сприяє кращому розумінню і запам'ятовуванню матеріалу, тоді як інфографіка конденсує інформацію у візуально привабливі формати, які легко сприймаються. Інтерактивні елементи, такі як вікторини, симуляції та розгалужені сценарії, заохочують активну участь і допомагають закріпити отримані знання.

Додатковою перевагою мікронавчання є можливість доступу до навчальних модулів у будь-який час і в будь-якому місці за допомогою різноманітних пристроїв, включаючи смартфони, планшети та ноутбуки. Така гнучкість дозволяє працівникам навчатися у зручний для них час, наприклад, під час перерв, поїздок на роботу або простою на роботі. Інтегруючи мікронавчання у свої навчальні програми, організації надають працівникам можливість контролювати власне навчання і розвивати навички та знання в умовах, які органічно вписуються у їхнє зайняте життя.

Мікронавчання не лише сприяє більш ефективному засвоєнню знань, але й стимулює мотивацію до навчання завдяки інтерактивному та мультимедійному підходу. Завдяки цьому, організації можуть підвищити загальний рівень кваліфікації своїх працівників, забезпечуючи їм можливість постійного професійного розвитку без відриву від основної діяльності. Цей підхід дозволяє працівникам залишатися конкурентоспроможними на ринку праці, постійно вдосконалюючи свої знання та навички у зручний та ефективний спосіб.

Навчання за допомогою ігор, також відоме як гейміфікація, передбачає інтеграцію ігрових елементів і принципів у навчальний процес для підвищення зацікавленості та мотивації учнів. Цей підхід використовує притаманну іграм привабливість для створення захоплюючого та інтерактивного навчального процесу, який є одночасно приємним та ефективним. Одним із ключових аспектів гейміфікації є впровадження ігрових елементів, таких як бали, значки, рівні та таблиці лідерів, для стимулювання участі та прогресу. Учні заробляють бали та значки за виконання завдань, оволодіння навичками чи досягнення проміжних результатів, що дає їм відчутну винагороду та визнання за їхні зусилля. Таблиці лідерів дозволяють учням бачити, як їхні результати порівнюються з результатами їхніх однолітків, що сприяє формуванню почуття конкуренції та заохочує дружнє суперництво [24].

Крім того, гейміфікація часто включає сценарії, симуляції та інтерактивні вправи, щоб надати учням практичний досвід та практичне застосування знань і навичок. Сценарії представляють учням реальні життєві ситуації або виклики, які

вони повинні вирішити, використовуючи критичне мислення та навички розв'язання проблем. Симуляції дозволяють учням досліджувати складні концепції або процеси в безпечному віртуальному середовищі, даючи їм змогу експериментувати і вчитися на своїх помилках без наслідків у реальному світі. Інтерактивні вікторини, головоломки та ігри посилюють навчальні цілі та заохочують учнів до активної участі.

Впроваджуючи ігрові елементи та принципи в навчальний процес, гейміфікація підвищує мотивацію та залученість учнів. Ігри використовують внутрішні мотиватори, такі як допитливість, самостійність і майстерність, надаючи учням відчуття мети і задоволення, що заохочує їх інвестувати час і зусилля в навчальну діяльність. Крім того, гейміфікація сприяє підвищенню почуття досягнення і прогресу, оскільки учні працюють над досягненням цілей і проходженням етапів, підвищуючи їхню впевненість і самооцінку.

Загалом, навчання через ігри пропонує організаціям цікавий та ефективний спосіб залучити працівників до навчання та професійного розвитку. Інтегруючи ігрові елементи, сценарії, симуляції та інтерактивні вправи в навчальний процес, організації можуть створити цікавий і захоплюючий навчальний досвід, який викликає цікавість, стимулює мотивацію та покращує запам'ятовування і передачу знань. Таким чином, гейміфікація не лише підвищує залученість і мотивацію учнів, але й сприяє кращому засвоєнню матеріалу, забезпечуючи всебічний і ефективний підхід до навчання.

На рис. 2.6 показано, які ігрові елементи навчання активують певні моделі поведінки учнів.

Технології віртуальної реальності (VR) і доповненої реальності (AR) зробили революцію в навчанні та освіті, забезпечивши інтерактивний досвід навчання з ефектом занурення. Одним із ключових застосувань VR і AR у навчанні є створення реалістичних сценаріїв, які імітують реальні середовища і ситуації. VR-середовища дозволяють учням досліджувати і взаємодіяти з віртуальними об'єктами, тоді як AR накладає цифрову інформацію на фізичний світ, покращуючи сприйняття учнями свого оточення. Завдяки цьому учні

можуть брати участь у практичних заняттях, не ризикуючи своєю безпекою або цілісністю фізичного обладнання, що особливо важливо при відтворенні складних або небезпечних сценаріїв.

Рис. 2.6. Співвідношення ігрових елементів та моделей поведінки, які вони активують [25]

Більше того, VR і AR дозволяють проводити практичні заняття в безпечному і контрольованому середовищі. Учні можуть маніпулювати віртуальними об'єктами, виконувати завдання та відпрацьовувати навички у реалістичних, але безпечних умовах. Такий підхід дозволяє отримати практичний досвід і розвинути м'язову пам'ять у спосіб, який неможливий за допомогою традиційних методів навчання.

Інтерактивність та занурення є центральними елементами навчального процесу у VR та AR-середовищах. Учні можуть взаємодіяти з контентом за допомогою жестів, голосових команд та інтерактивних симуляцій, що робить процес навчання більш захоплюючим і партисипативним. Імерсивні технології переносять учнів у віртуальні світи, де вони можуть досліджувати та взаємодіяти

з цифровим контентом у природний та інтуїтивний спосіб. Це сприяє глибокому залученню та концентрації, що покращує результати навчання та збереження знань [26].

Технології віртуальної і доповненої реальності пропонують захоплюючі можливості для трансформації навчання і освіти, забезпечуючи реалістичний, практичний і захоплюючий навчальний досвід. Використовуючи ці технології, організації можуть підвищити ефективність навчання, знизити витрати, пов'язані з традиційними методами навчання, і дати можливість учням набувати і застосовувати нові навички в безпечний і цікавий спосіб. Це відкриває нові горизонти для освітніх програм, роблячи навчання більш доступним і ефективним, дозволяючи учням глибше зануритися у вивчення матеріалу і краще засвоювати нові знання та навички.

Рис. 2.7. Технології VR і AR

Загалом, впровадження VR і AR у навчальний процес значно підвищує залученість учнів, покращує результати навчання та створює умови для безпечного і практичного набуття досвіду. Ці технології надають учням унікальні можливості для взаємодії з навчальним контентом, сприяючи більш глибокому розумінню матеріалу і ефективнішому засвоєнню знань.

Технології штучного інтелекту (ШІ) та машинного навчання (МН) змінюють навчальний ландшафт, пропонуючи персоналізовані підходи до

освіти, що ґрунтуються на даних. Одним із важливих застосувань ШІ є його здатність адаптувати навчальний процес до індивідуальних потреб учнів. Алгоритми ШІ аналізують взаємодію учнів з навчальним контентом, визначаючи їхні сильні та слабкі сторони, а також навчальні вподобання. На основі цього аналізу ШІ може адаптувати навчальний процес у режимі реального часу, представляючи контент відповідно до темпу, стилю та рівня розуміння кожного учня. Такий адаптивний підхід гарантує, що студенти отримують індивідуальну підтримку і настанови, максимізуючи результати навчання і залученість.

Штучний інтелект також полегшує аналіз даних для оцінки ефективності навчання. Збираючи й аналізуючи величезні обсяги даних про учнів, алгоритми ШІ можуть виявляти тенденції, закономірності та кореляції, які дають уявлення про результати навчання та показники ефективності. Такий підхід, заснований на даних, дає змогу освітянам оцінювати ефективність навчальних матеріалів, методів викладання та стратегій навчання, дозволяючи їм приймати рішення, що ґрунтуються на фактах, для покращення якості освіти.

Крім того, системи на основі штучного інтелекту можуть надавати учням персоналізовані рекомендації та навчальні траєкторії. Використовуючи предиктивну аналітику та механізми рекомендацій, алгоритми ШІ можуть пропонувати відповідні навчальні ресурси, види діяльності та курси на основі інтересів, цілей та попередньої взаємодії учнів. Ці персоналізовані рекомендації допомагають учням відкривати нові теми, поглиблювати розуміння існуючих концепцій, а також залишатися мотивованими та залученими протягом усього навчального процесу [27].

Машинне навчання, підрозділ ШІ, зосереджується на розробці алгоритмів, які дозволяють комп'ютерам вчитися і робити прогнози на основі даних. Технології МН можна віднести до категорії штучного інтелекту, і в багатьох контекстах ці поняття використовуються як тотожні. Машинне навчання (Machine Learning, МН) сьогодні найчастіше визначають як напрямок розвитку технологій ШІ зі створення гнучких алгоритмів, здатних до навчання та розвитку на основі отримуваних даних. Завдяки МН машини отримали змогу виявляти

закономірності у великих наборах даних та ухвалювати на основі цього аналізу правильні рішення. На відміну від звичайних запрограмованих алгоритмів, моделі МН поступово покращуються під час використання. Їх точність залежить від об’єму та якості доступних даних.

Відмінності між технологіями ШІ й МН показані на рис. 2.8.

Рис. 2.8. Відмінності між ШІ і МН

На відміну від традиційного програмування, яке спирається на чітко визначені правила та логіку, системи МН використовують статистичні методи, що дозволяють комп'ютерам покращувати свою роботу над завданням на основі досвіду. Основна ідея полягає в побудові моделей, які можуть узагальнювати набір навчальних даних на невидимі дані, тим самим приймаючи обґрунтовані рішення або прогнози.

Загалом, штучний інтелект і машинне навчання пропонують трансформаційні можливості для вдосконалення освіти, забезпечуючи адаптивний, керований даними і персоналізований навчальний досвід. Використовуючи ці технології, освітяни можуть створювати індивідуальні навчальні програми, які відповідають унікальним потребам і вподобанням кожного учня. Це призводить до покращення результатів навчання, підвищення рівня залученості та ефективності освіти. У майбутньому, інтеграція ШІ в освітні

процеси може стати ключовим фактором у підготовці учнів до вимогливих викликів сучасного світу, роблячи навчання більш доступним, ефективним та орієнтованим на потреби кожного індивіда.

2.3 Адаптивна система навчання

Адаптивне навчання є освітнім підходом, що використовує технології для персоналізації навчального процесу для кожного учня. Цей підхід динамічно коригує зміст, темп і методи навчання на основі унікальних потреб, уподобань і успішності учня, спрямований на оптимізацію результатів шляхом надання індивідуального навчання та підтримки.

Адаптивне навчання пропонує значні переваги завдяки персоналізації та адаптивності, гнучкості та масштабованості, а також завдяки особливим характеристикам адаптивних систем. Основною перевагою адаптивного навчання є його здатність пристосовуватися до різних стилів навчання та здібностей учнів, забезпечуючи кожного з них належною підтримкою. Системи адаптивного навчання динамічно коригують зміст і методи викладання, враховуючи індивідуальні вподобання та рівень підготовки кожного учня. Це гарантує, що навчальний процес максимально відповідає потребам кожного учасника, сприяючи ефективнішому засвоєнню знань і навичок.

Крім того, адаптивне навчання вирізняється своєю гнучкістю і масштабованістю. Учні можуть отримувати доступ до систем адаптивного навчання в будь-який час і з будь-якого місця, використовуючи різноманітні пристрої, що робить навчання більш доступним і зручним. Такі системи також здатні масштабуватися, щоб вміщати велику кількість учнів, забезпечуючи при цьому персоналізоване навчання та підтримку, що є особливо корисним у великих навчальних закладах або організаціях [28].

Основні характеристики адаптивних систем навчання включають персоналізацію, адаптивність, зворотний зв'язок, інтерактивність та прийняття рішень на основі даних (Рис. 2.9).

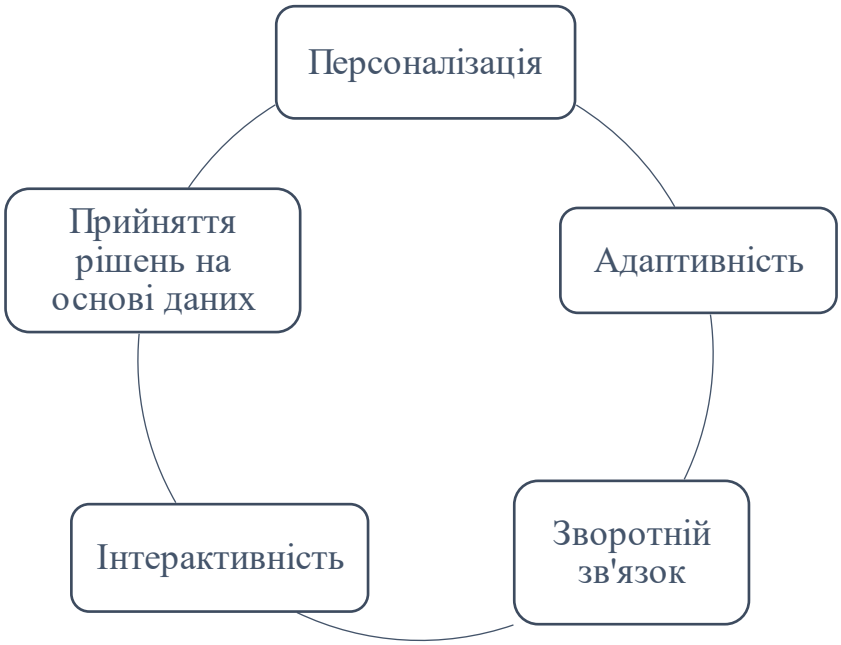


Рис. 2.9. Характеристики адаптивних систем

Персоналізація дозволяє адаптувати навчальний процес до потреб кожного учня, тоді як адаптивність забезпечує динамічне коригування змісту і темпу навчання. Своєчасний зворотний зв'язок надає учням інформацію щодо їхньої успішності, допомагаючи їм розуміти свої сильні та слабкі сторони. Інтерактивність включає в себе використання інтерактивних елементів, які залучають учнів до активної участі в навчальному процесі, роблячи його більш цікавим і захоплюючим. Нарешті, прийняття рішень на основі даних передбачає використання аналізу даних для вдосконалення навчального процесу, що дозволяє ефективніше вирішувати проблеми і поліпшувати результати навчання.

Оцінка ефективності адаптивного навчання передбачає кілька ключових аспектів, що дозволяють оцінити прогрес у навчанні, отримати зворотний зв'язок і стимулювати постійне вдосконалення. Першим важливим кроком є визначення ключових показників ефективності (КПЕ). Ці показники можуть включати відсоток завершення курсу, результати тестів та показники зворотного зв'язку з користувачами. Відсоток завершення курсу показує, яка частка учнів успішно завершила курс, що відображає рівень їхньої залученості та прихильності до навчання. Результати тестів оцінюють рівень засвоєння учнями змісту курсу, а

зворотний зв'язок від користувачів надає інформацію про задоволеність, розуміння та загальний досвід навчання.

Аналіз відгуків працівників є ще одним важливим аспектом оцінки ефективності адаптивного навчання. Регулярні опитування й анкетування збирають відгуки про різні аспекти навчального процесу, зокрема про актуальність, зрозумілість і залученість контенту. Цей зворотний зв'язок використовується для визначення сфер, що потребують вдосконалення, і для внесення коректив у навчальні програми. Інструменти аналізу даних дозволяють глибше аналізувати отримані дані, отримуючи дієві висновки, які допомагають підвищити ефективність навчання [29].

Пріоритезація постійного вдосконалення є ще одним ключовим елементом оцінки ефективності адаптивного навчання. Аналізуючи результати навчання і показники ефективності, організації можуть виявити сильні і слабкі сторони своїх навчальних програм. На основі цього аналізу вони приймають рішення щодо оптимізації навчального процесу, коригуючи контент, регулюючи темп навчання або інтегруючи нові технології для покращення залученості та розуміння. Автоматизація процесу вдосконалення за допомогою алгоритмів на основі штучного інтелекту дозволяє безперервно вдосконалювати навчальні матеріали, динамічно коригуючи їх у режимі реального часу, щоб краще відповідати індивідуальним потребам учнів.

Загалом, оцінка ефективності адаптивного навчання включає багатогранний підхід, що охоплює визначення ключових показників ефективності, збір зворотного зв'язку від учнів і постійне вдосконалення навчальних програм на основі зібраних даних. Використовуючи метрики, механізми зворотного зв'язку та аналітику даних, організації можуть забезпечити позитивні результати навчання та сприяти постійному підвищенню ефективності освітнього процесу.

SC Training (раніше EdApp) – це адаптивна навчальна платформа, оснащена такими функціями, як авторський інструмент, шаблони електронного навчання, елементи гейміфікації та набір аналітики. Вона включає функцію

створення курсів зі штучним інтелектом "Створюй зі штучним інтелектом", яка дозволяє швидко створювати уроки, просто ввівши тему курсу. Система автоматично інтегрує підтеми з відповідними текстами, зображеннями та вікторинами, а також дозволяє кастомізувати їх за допомогою вбудованого авторського інструменту та понад 80 шаблонів. Платформа використовує елементи гейміфікації, такі як ігри та вікторини, щоб підвищити залученість учнів. Комплексний набір звітів та аналітики дозволяє виявити прогалини в навчанні як для окремих осіб, так і для команд. Розроблена з урахуванням мобільного підходу, SC Training (раніше EdApp) забезпечує сумісність з пристроями Android і Apple та підтримує безперебійне форматування в комп'ютерних веб-браузерах, пропонуючи гнучкість у проведенні уроків.

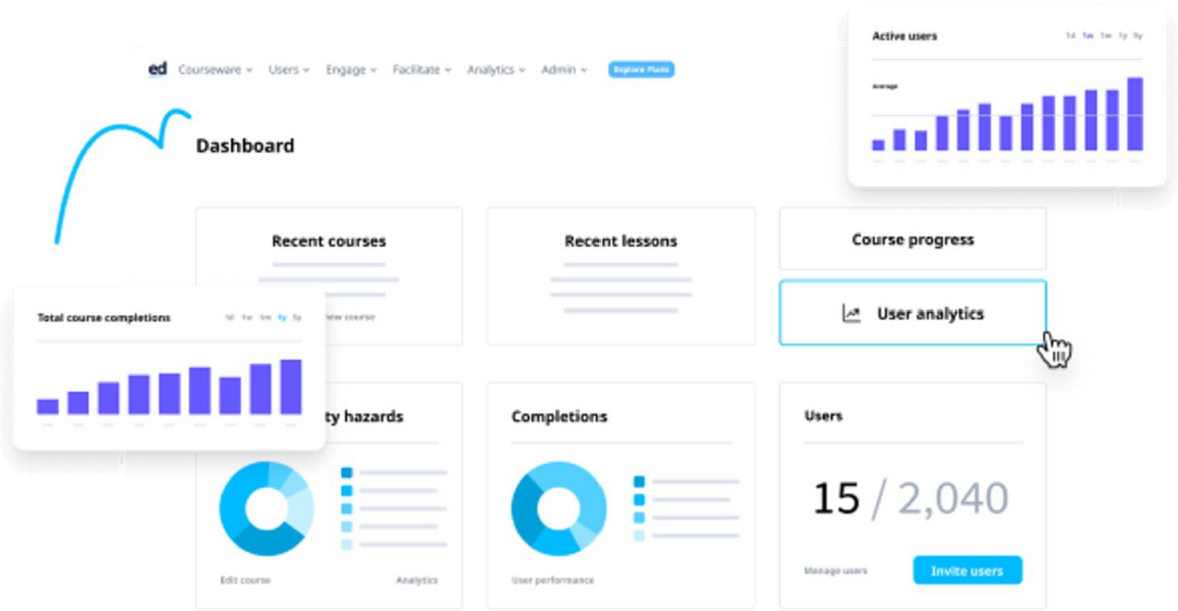


Рис. 2.10. Інтерфейс SC Training [30]

Whatfix – це цифрова платформа для адаптивного навчання за допомогою персоналізованих, контекстно-чутливих рекомендацій. Вона забезпечує аналіз взаємодії користувачів з додатками чи програмним забезпеченням у режимі реального часу, надаючи відповідну інформацію, покрокові інструкції та підказки, щоб допомогти користувачам розібратися зі складними процесами. Такий підхід гарантує, що користувачі отримують належний рівень підтримки саме тоді, коли це потрібно, підвищуючи ефективність та результативність

процесу навчання. Whatfix адаптує свої рекомендації до рівня кваліфікації користувачів, пропонуючи фундаментальну підтримку для початківців та поглиблену допомогу для досвідчених користувачів. Ця персоналізована стратегія підвищує залученість користувачів, зменшує ймовірність невдач і прискорює процес навчання, що в кінцевому підсумку підвищує кваліфікацію та продуктивність користувачів.

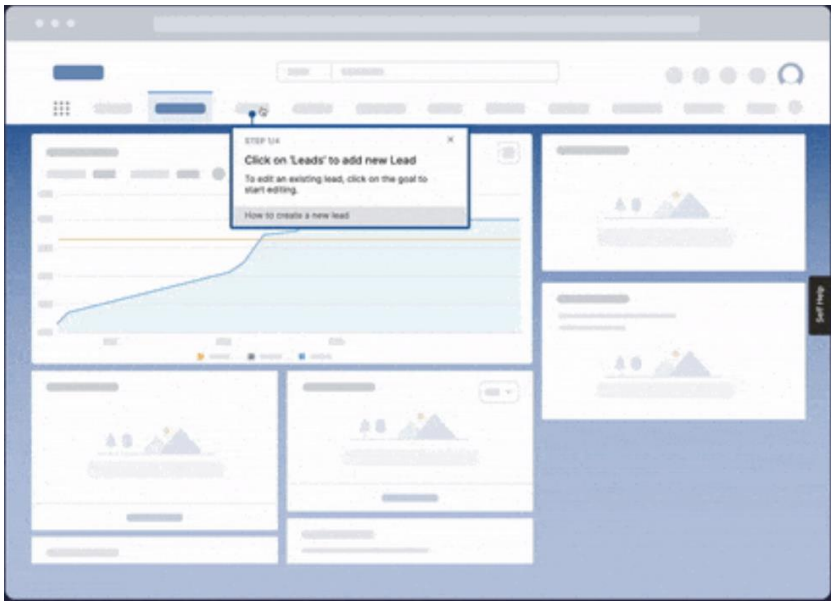


Рис. 2.11. Інтерфейс Whatfix [31]

Висновки до розділу 2

Впровадження інноваційних технологій навчання є необхідним для підвищення ефективності підготовки фахівців з інформаційної безпеки. Традиційні методи навчання, хоча й забезпечують базову теоретичну підготовку, виявляються недостатніми для повноцінного розвитку практичних навичок та адаптації до нових викликів сучасного світу. Інноваційні технології, такі як електронне навчання, мікронавчання, гейміфікація, віртуальна та доповнена реальність, а також штучний інтелект і машинне навчання, пропонують більш гнучкий, інтерактивний і персоналізований підхід до освіти. Вони дозволяють організаціям надавати працівникам доступ до навчальних матеріалів будь-де і будь-коли, враховуючи їх індивідуальні потреби та стилі навчання.

Електронне навчання, завдяки використанню онлайн-курсів і вебінарів, забезпечує значну гнучкість та знижує витрати на навчання, дозволяючи працівникам поєднувати навчання з іншими зобов'язаннями. Інтерактивні платформи з мультимедійним контентом та інструментами для спільної роботи підвищують зацікавленість і ефективність навчального процесу. Мікронавчання, яке передбачає надання коротких цілеспрямованих модулів, дозволяє ефективніше засвоювати знання в умовах напруженого графіка. Гейміфікація, інтегруючи ігрові елементи у навчальний процес, підвищує мотивацію та залученість учнів. Технології віртуальної і доповненої реальності створюють реалістичні сценарії для практичного навчання, забезпечуючи безпечне середовище для відпрацювання навичок. Штучний інтелект і машинне навчання надають персоналізовані рекомендації та адаптують навчальний процес до потреб кожного учня, що значно підвищує ефективність освіти.

Таким чином, інтеграція інноваційних технологій у навчальний процес з інформаційної безпеки сприяє підвищенню якості підготовки фахівців, забезпечуючи їх актуальними знаннями і практичними навичками. Це дозволяє організаціям ефективно протидіяти сучасним загрозам та забезпечувати захист інформаційних систем.

Розділ 3 ОСОБЛИВОСТІ ГЕЙМІФІКАЦІЇ У НАВЧАННІ Й ПІДВИЩЕННІ ОБІЗНАНОСТІ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Переваги й механізми ігрового навчання

Гейміфікація в навчанні – це впровадження елементів і принципів ігрового дизайну в освітнє середовище для підвищення залученості, мотивації та загальних результатів навчання. Цей підхід використовує внутрішні стимули, такі як конкуренція, досягнення та співпраця, інтегруючи в навчальний процес такі елементи, як бали, значки, таблиці лідерів та виклики. Трансформуючи традиційні освітні заходи в інтерактивний і динамічний досвід, гейміфікація має на меті сприяти більш захоплюючій і приємній атмосфері навчання. Теоретичне підґрунтя гейміфікації в навчанні спирається на поведінкові, когнітивні та конструктивістські теорії навчання, які наголошують на активній участі, негайному зворотному зв'язку та застосуванні знань у контекстно-релевантних сценаріях.

Гейміфікація може привести до покращення показників засвоєння матеріалу, посилення мотивації та вищого рівня участі слухачів. Однак її ефективність залежить від ретельної розробки та узгодження з освітніми цілями, гарантуючи, що ігрові елементи підтримують навчальні цілі, а не відволікають від них [32].

Вона також сприяє персоналізованому навчанню, зменшує повторювану негативну поведінку і професіоналізує використання інформаційно-комунікаційних технологій (ІКТ), які стають важливими ресурсами. Важливо відрізняти гейміфікацію від простого впровадження ігор або відеоігор для розвитку теми, оскільки гейміфікація передбачає стратегічне застосування елементів ігрового дизайну в освітньому контексті, створюючи таким чином більш цікавий та ефективний навчальний досвід. Переваги гейміфікації показані на рис. 3.1.

Рис. 3.1. Переваги гейміфікації

Використання різноманітних завдань, соціальної взаємодії, персоналізації навчання та мотивуючих елементів допомагає формувати компетентності й навички, необхідні для успішного засвоєння матеріалу та подальшого професійного розвитку. Навчальний контент має бути інтерактивним, захоплюючим і багатим на мультимедійні елементи. Навчальні вправи мають бути розроблені з урахуванням навчальних цілей і можливостей:

- Багаторазове виконання – навчальна діяльність має бути розроблена таким чином, щоб слухачі могли повторити її у разі невдалої спроби. Дуже важливо створити умови та можливості для досягнення кінцевої мети. В результаті повторень слухачі будуть вдосконалювати свої навички.

- Реалістичність – навчальні завдання мають бути посильними для виконання. Вони мають бути адаптовані до потенціалу та рівня навичок слухачів.

- Різноманітність завдань – навчальні завдання мають бути різноманітними за формою та змістом, щоб підтримувати інтерес та мотивацію слухачів. Це може включати різні типи вправ, від тестів до інтерактивних симуляцій.

- Соціальна взаємодія – впровадження елементів, що сприяють співпраці та конкуренції серед слухачів, може стимулювати їхню участь та залученість. Це може бути досягнуто через групові проекти, форуми для обговорень і змагальні завдання.

Щоб зрозуміти гейміфікацію, важливо ознайомитися з фундаментальними компонентами, які роблять ігри цікавими. До них належать ігрова механіка, механіка навчання та ігрова естетика [33].

Механізми навчання стосуються основних моделей взаємодії або інтерактивних структурних блоків, з якими взаємодіє учасник навчання (рис. 3.2). Вони можуть бути сформульовані або як окремі заходи, або як взаємопов'язані між собою, причому обидва ці варіанти складають основну навчальну діяльність, яка часто відтворюється в грі. Кожна навчальна гра має механіку навчання, яка визначає правила та способи взаємодії, що використовуються для мотивації та залучення гравців до проходження гри і, зрештою, розширення їхніх знань та/або розвитку їхніх навичок. Схематичне зображення всіх основних ігрових механізмів зображено на рис. 3.2.

Рис. 3.2. Механізми навчання

У навчальних програмах цифрового навчання від слухачів очікується виконання низки послідовних дій, щоб виконати поставлені завдання. Навчальні ігри в цьому контексті насамперед використовують принципи проблемно-орієнтованого навчання або навчання, заснованого на виконанні завдань. Коли студенти повинні співпрацювати для досягнення спільної мети, ці сценарії також включають елементи навчання у співпраці [34].

Залежно від характеру навчального завдання, слухачі можуть розвивати широкий спектр когнітивних навичок, таких як планування, критичне мислення та розв'язання проблем, технічних навичок, що передбачають розвиток знань за допомогою нових методів або практичне застосування існуючих методів, а також соціальних навичок, включаючи обмін знаннями, інформацією та думками. Навчальні заходи, пов'язані з цими механізмами, включають рольові ігри, парні або групові дискусії, дослідження, спостереження та інші практичні вправи.

Навчальна програма - це діяльність під керівництвом викладача та/або самостійна робота, покликана дати можливість студентам здобути теоретичні знання або закріпити практичні навички. Як механізм навчання, вони ґрунтуються на принципах конструктивістської та когнітивної моделей і можуть іноді передбачати співпрацю студентів, наприклад, під час виконання курсових завдань. Залежно від навчального предмету, підручники для здобуття теоретичних знань або навичок можуть бути дискусійними, зосередженими на глибшому вивченні змісту курсу через дискусії та дебати, або ж практичними, з акцентом на розвиток практичних навичок. Незалежно від формату, додатковою перевагою такого підходу є можливість для слухачів брати участь у подальших сесіях запитань і відповідей. Ефективна інтеграція цього навчального механізму посилюється завдяки використанню різних мультимедійних ресурсів, зокрема презентацій.

Віртуальні навчальні середовища дають змогу викладачам демонструвати абстрактні теми та концепції, які можуть бути складними або непридатними для вивчення в традиційних класах. Освітні ігри цієї категорії в першу чергу спираються на принципи поведінкового підходу, моделюючи сценарії, що

підкреслюють причинно-наслідкові зв'язки, або на підхід експериментального навчання, коли слухачі спостерігають і повторюють дії спікера. Коли навчальна діяльність передбачає зв’язки між учнями, наприклад, конкуренцію, взаємодію чи співпрацю, цей підхід також можна пов'язати з теорією соціального навчання. Освітні заходи, пов'язані з цим механізмом, включають симуляції, 3D-моделювання та програмування, віртуальні екскурсії на основі сценаріїв та дослідження під керівництвом викладача через розповідь історій [35].

Окрім сприяння навчальній діяльності, розробники та практики можуть інтегрувати завдання, пов'язані з оцінюванням, щоб дати слухачам уявлення про їхній навчальний прогрес і просування в навчанні. У серйозних іграх оцінювання співробітників може бути безперервним, з переходом від одного рівня до іншого, що супроводжується зростанням складності, або прихованим, інтегрованим у гейміфіковану діяльність. Ці елементи забезпечують безперервність процесу навчання, дозволяючи викладачам збирати цінну інформацію про розвиток знань і навичок працівників.

Загальний підхід до полегшення оцінювання в цифровому навчальному середовищі передбачає фіксацію, запис та аналіз поведінки слухачів за допомогою цифрових журналів користувачів. Після завершення завдання дуже важливо забезпечити зворотний зв'язок. У контексті гейміфікованих вправ зворотний зв'язок може надаватися як під час гри, наприклад, за допомогою підказок про невдачу/повторення, так і після гри, через моменти роздумів, спостереження за іншими та перегляд нещодавніх вправ. Зворотній зв'язок може мати різні форми, включаючи текстові та аудіовізуальні формати, і може надаватися як ізольовано, так і в поєднанні.

Після завершення навчальних завдань викладачі повинні забезпечити можливості для критичного осмислення та обговорення. Цей процес, який може відбуватися поза ігровим контекстом шляхом підбиття підсумків, може включати ведення журналів спостережень, наставництво та критику гри.

Окрім безпосередньої користі для учасників, аналіз і обговорення також дають змогу розробникам навчальної програми оцінити, чи відповідає вибір ігор

мотивації та інтересу учасників, визначити елементи, яким вони надають перевагу, виклики, з якими вони стикаються, і як їм вдається долати ці виклики. Для більш підготовлених слухачів можна організувати обговорення, орієнтоване на групу, або обговорення в колі студентів на основі попередньо визначених рекомендацій. Така практика не лише покращує розуміння та запам'ятовування матеріалу, але й надає цінний зворотній зв'язок для вдосконалення освітніх стратегій та ігрових підходів до навчання.

Ігрова механіка - це набір правил і механізмів зворотного зв'язку, покликаних сприяти захопливому ігровому процесу. Вони часто вважаються основоположними елементами і можуть бути адаптовані та інтегровані для впровадження ігрових функцій у неігрове середовище. Різні ігрові механіки використовуються для того, щоб використовувати мотиваційні стимули гравців та їхню готовність до взаємодії. Наприклад, мотивація колекціонерів може бути вирішена за допомогою цифрових товарів, тоді як мисливців за досягненнями можна мотивувати за допомогою таблиць лідерів або значків. Аналогічно, механіки невдач використовуються для того, щоб в ігровій формі повідомити про дії, які гравці повинні і не повинні виконувати. У цілісному гейміфікованому дизайні можна використовувати комбінацію різних мотиваційних чинників; однак, коли працівники стикаються з численними елементами ігрової механіки, їм може бути складно зосередитися на навчальних цілях. Основні механіки зображені на рис. 3.3.

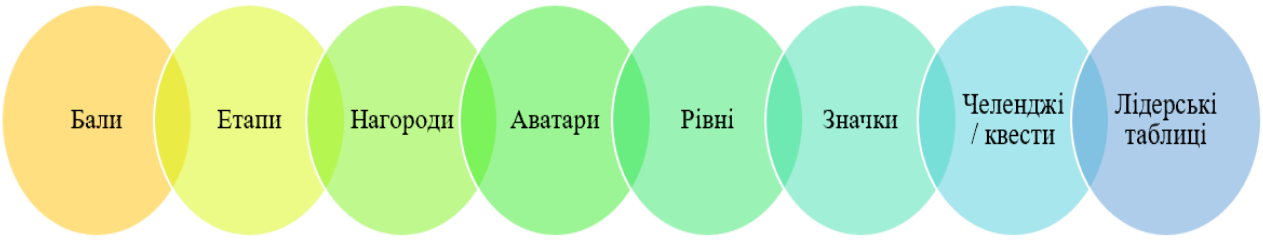


Рис. 3.3. Ігрові механіки [36]

Розглянемо кожну з механік детальніше.

Аватари – це цифрові репрезентації гравців в ігровому середовищі, що втілюють їхню особистість або персонаж. Вони дозволяють взаємодіяти з

ігровим світом та іншими гравцями, виконуючи роль довіреної особи гравця. Аватари варіюються від простих двовимірних іконок до складних тривимірних конструкцій, що відображають суть гри. Для багатьох аватарки стають відображенням самих себе, символізуючи їхній статус і досягнення.

В освіті аватари дозволяють учням виражати індивідуальність і творчість за допомогою налаштовуваних характеристик, таких як зовнішній вигляд і одяг. Така персоналізація посилює залученість, сприяючи емоційній прив'язаності та відчуттю контролю. Крім того, аватари забезпечують безпечний простір для відпрацювання соціальних і комунікативних навичок, дозволяючи учням досліджувати різні ролі та сценарії.

Бали – це фундаментальний ігровий механізм, який використовується в більшості ігор для забезпечення чіткої метрики для оцінки досягнень і відстеження прогресу. Гравці заробляють бали, виконуючи завдання, досягаючи проміжних етапів або здійснюючи визначні подвиги в грі. Ці бали кількісно вимірюють прогрес і підтримують залученість гравців, пропонуючи відчутний зворотній зв'язок у відповідь на їхні ігрові дії. Бали можуть слугувати зовнішніми стимулами, мотивуючи гравців продовжувати взаємодіяти з ігровим інтерфейсом. Системи балів варіюються залежно від характеру гри і можуть бути пристосовані до бажаних результатів навчання. Таким чином, бали - це не просто числові значення, вони відображають прогрес, просування в навчанні та досягнення, тим самим посилюючи внутрішню мотивацію гравців до виконання завдань.

У покрокових іграх проходження поділяється на окремі фази, відомі як "ходи". Ці ігри дозволяють гравцям ставити ігровий світ на паузу перед тим, як виконати якусь дію. Однак не всі ходи однакові: в деяких іграх гравцям дається період аналізу перед виконанням дії, тоді як в інших ходи можуть представляти довші періоди, такі як роки, місяці, тижні або дні. В освітньому контексті найпоширенішими підходами є хронометраж ходів і часовий ліміт, обидва з яких створюють певний часовий тиск, що спонукає гравців швидко думати і виконувати свої дії.

Рівні в грі – це сегментовані етапи, які гравці проходять, як правило, зі зростанням складності або ускладненням, щоб представити нові виклики. Проходження рівнів підтверджує майстерність гравців у певних ігрових техніках або освітніх цілях, забезпечуючи відчуття досягнення та прогресу. В освітньому контексті рівні можуть відповідати окремим навчальним сегментам або предметам. Перехід на вищий рівень означає завершення навчальної мети і готовність до вивчення більш складних тем. Ці градації забезпечують узгоджену структуру як для ігрової, так і для освітньої подорожі, гарантуючи структурованість і керованість досвіду, тим самим зменшуючи ризик того, що гравці або студенти відчують себе перевантаженими [37].

Значки візуально символізують досягнення гравців, які вони отримують після досягнення певних цілей або орієнтирів у грі. Ці значки не лише визнають і винагороджують гравців за їхню майстерність і відданість, але й підвищують їхню мотивацію та залученість. Окрім індивідуального визнання, бейджики мають ще й суспільний аспект, дозволяючи гравцям демонструвати свої успіхи одноліткам, тим самим розвиваючи почуття товариства і завершеності. В освіті бейджики відзначають досягнення певних освітніх цілей або заохочують активну участь і внесок у навчальний процес. Подібно до рівнів, бейджики відображають досягнення, надаючи учням уявлення про їхній прогрес і прояснюючи їхню позицію в освітньому процесі. Крім того, прагнення отримати значки може заохочувати критичне мислення та вирішення проблем, оскільки працівники з'ясовують, як їх заробити, збагачуючи таким чином навчальний досвід.

Квест – це конкретне завдання, яке виконує персонаж або група персонажів під управлінням гравця, щоб отримати винагороду. У квестових іграх гравці беруть участь у взаємопов'язаних діях, які зазвичай передбачають переміщення між різними точками дії. Успішне завершення квесту або набору квестів (квест-лінії) призводить до досягнення конкретної мети або винагороди. Як освітній підхід, квест-навчання структуроване як послідовність інструктажу, дій та підбиття підсумків. Отже, цей метод часто асоціюється з діяльністю, яка передбачає вирішення проблем, оскільки студенти-гравці повинні вирішувати

поставлені проблеми, щоб просуватися вперед і в кінцевому підсумку виконати поставлене завдання.

Системи винагород в іграх виконують подвійну роль: вони діють як стимули для гравців і допомагають пом'якшити потенційне розчарування. Ці механізми можна поділити на зовнішні винагороди, такі як значки, бали, фізичні або віртуальні товари, які привертають увагу користувачів, і внутрішні винагороди, такі як індикатори прогресу, сповіщення та статус у таблиці лідерів, які забезпечують довготривалу залученість у гру. Надання винагород може приймати різні форми, включаючи випадкові винагороди, фіксовані графіки винагород і винагороди, що залежать від часу. Найпоширенішими видами винагород є жетони, досягнення, повідомлення зворотного зв'язку, очки досвіду, надання предметів і розблокування контенту. Гравці можуть використовувати ці винагороди, щоб просуватися в грі або демонструвати свої знання інструкторам та одногрупникам.

Таблиці лідерів візуально ранжують гравців на основі їхніх досягнень і можуть бути розділені на два рівні: макрорівень, який відображає загальну ефективність, і мікрорівень, який фокусується на результатах виконання конкретних завдань. Незважаючи на відмінності в інформації, що надається на кожному рівні, ключові структурні елементи залишаються схожими. В освітньому контексті типова таблиця лідерів відображає інформацію, пов'язану з ідентифікацією слухачів, наприклад, імена або псевдоніми, а також їхній рейтинг, який визначається їхнім навчальним прогресом (наприклад, бали, виконані завдання) або успішністю (наприклад, оцінки, зароблені значки). Це дозволяє учням оцінити свою успішність порівняно з однолітками.

У геймдизайні естетика відноситься до досвіду гравця, охоплюючи початкову візуальну та емоційну залученість до занурення в динаміку та механіку гри. Дизайн персонажів і навколишнього середовища має на меті викликати певні емоційні реакції у гравців. Ігрові дизайнери класифікують основні естетичні принципи на основі емоцій, які вони викликають: відчуття (сенсорне задоволення), фантазія (уява), наратив (сюжет), виклик (смуга

перешкод), спілкування (соціальна взаємодія), відкриття (дослідження), самовираження (самопізнання) та підкорення (неквапливе проведення часу).

Залежно від теми навчальної гри, для покращення навчального процесу можна використовувати різні естетичні підходи. Ці елементи суттєво впливають на здатність гри залучати й мотивувати гравців, створюючи більш захоплююче та ефективне освітнє середовище. На рис. 3.4 зображено основні елементи ігрової естетики.

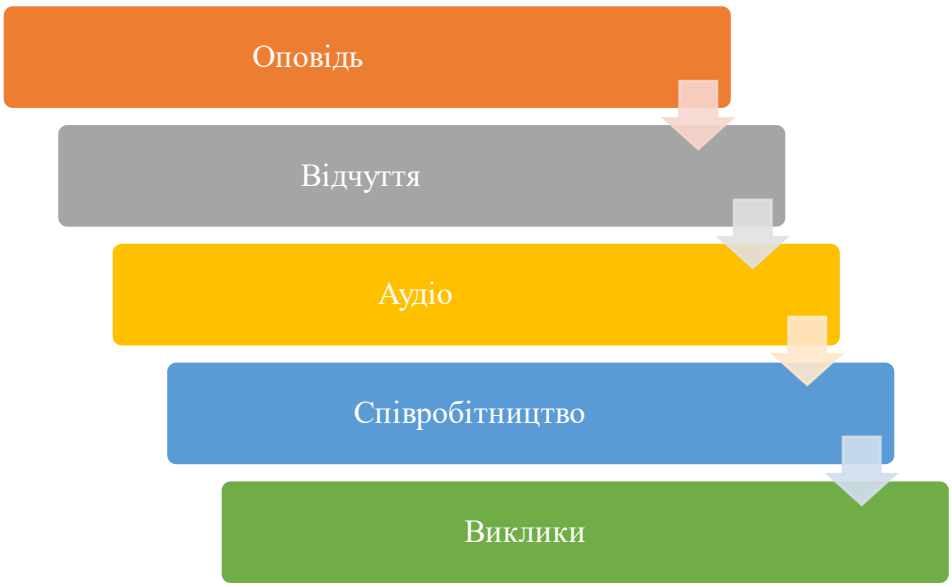


Рис. 3.4. Елементи ігрової естетики [38]

Естетика "відчуття" в іграх включає в себе відчутні стимули, такі як візуальна графіка, звукові елементи та тактильний зворотній зв'язок у реальному часі. Цей захоплюючий сенсорний макет миттєво захоплює гравців, сприяючи складним взаємодіям і відданості ігровому процесу та освітнім цілям. Це особливо важливо в освітніх іграх, які покладаються на практичний досвід і проактивні відкриття, наприклад, в науці та інженерії.

Естетика "фентезі" створює уявні світи та персонажів, які привертають увагу гравців, стимулюють складні когнітивні процеси і сприяють глибшому залученню та зануренню. Це сприяє вирішенню проблем, творчості та критичному мисленню. В освіті фентезі допомагає приземлити абстрактні ідеї, роблячи навчання більш цікавим.

Естетика "наративу" інтегрує основні елементи історії, такі як структура сюжету, розвиток персонажів і траєкторії, що розвиваються. Добре побудований наратив викликає емоційний резонанс і зацікавленість гравців, заохочуючи їх до подальшої взаємодії. В освіті наративи контекстуалізують інформацію, роблячи її кращою для запам'ятовування та сприяючи емпатії, пропонуючи розуміння різних точок зору.

Аудіоестетика включає в себе всі звукові елементи, такі як музика, звукові ефекти, навколишній шум і голос за кадром. Ці компоненти формують звуковий ландшафт гри, сприяючи зануренню, емоційному залученню та розумінню ігрової механіки. Звукові ефекти посилюють зворотний зв'язок, музика задає настрій і темп, а озвучення підсилює наративні аспекти, покращуючи загальний навчальний досвід.

Естетика "виклику" поєднує в собі завдання, головоломки та бар'єри, які гравці повинні долати, щоб просуватися в грі. Ці виклики відточують навички розв'язання проблем і надають учням практичний контекст для застосування їхніх знань. Протистояння цим викликам розвиває наполегливість і стратегічне мислення.

Естетика "товариства" підкреслює соціальну взаємодію, співпрацю та конкуренцію між гравцями. Вона включає в себе спільні місії, групові завдання та конкурентні рейтинги, що сприяють формуванню почуття спільноти. В освіті така соціальна взаємодія розвиває командну роботу, комунікацію, навички ведення переговорів та навчання за принципом "рівний-рівному", підвищуючи загальну залученість та відданість справі.

Ці елементи механізмів навчання, ігрові механіки та елементи ігрової естетики в сукупності сприяють створенню структурованого, цікавого і мотивуючого навчального середовища, покращуючи освітні результати і залучення студентів шляхом використання інтерактивних і динамічних ігрових стратегій.

3.2 Порівняльний аналіз програмних рішень для навчання персоналу у сфері інформаційної безпеки з елементами гейміфікації

На сучасному ринку представлені численні програми, що використовують гейміфікацію для ефективного навчання працівників, допомагаючи їм опановувати критичні навички з кібербезпеки у цікавій та інтерактивній формі.

Guardey – це рішення для підвищення обізнаності про безпеку, яке включає елементи гейміфікації, щоб підтримувати залученість користувачів під час навчання. Користувачі беруть участь у щотижневих мікро-випробуваннях тривалістю до 3 хвилин, які охоплюють такі теми, як фішинг, безпека пристроїв, шахрайство з боку керівників, глибокі підробки та безпека паролів. Успішне виконання цих завдань приносить бали для таблиць лідерів компанії або відділу, що сприяє дружній конкуренції та підвищенню рівня участі. Деякі організації ще більше заохочують учасників, пропонуючи призи щоквартальним переможцям.

Адміністратори можуть налаштовувати завдання Guardey відповідно до політики безпеки своєї організації та використовувати галузевий контент з бібліотеки Guardey. Розділ звітів дозволяє відстежувати прогрес у навчанні команди, відстежуючи такі показники, як рівень участі та бали для кожної команди і кожного учасника. Щотижневі звіти електронною поштою підтримують відповідність стандартам безпеки, таким як NIS2 та ISO 27001. Хоча Guardey не є безкоштовним, він доступний і пропонує 14-денну пробну версію [39].

Counterintelligence Trivia Twirl – це гра, в якій користувачі крутять колесо, щоб вибрати категорію і відповісти на запитання з декількома варіантами відповідей. Запитання якісні, але не охоплюють усіх сучасних кіберзагроз. Гру можна пройти за 20 хвилин, що робить її скоріше короткостроковим рішенням, ніж довгостроковим навчальним інструментом, придатним для щорічного оновлення знань. Хоча обертання колеса додає ностальгічного відтінку, грі бракує значних елементів гейміфікації для глибокого залучення користувачів. Ключовими перевагами гри є її безкоштовний доступ, цікава функція обертання

колеса та складні запитання. Однак до її недоліків можна віднести мінімальну гейміфікацію, обмежене охоплення кіберзагроз і непридатність для довготривалого використання [40].

The Weakest Link, створена компанією IS Decisions, - це гра, що містить складні запитання на актуальні теми. Вона розрахована на коротку тривалість, зазвичай менше години, що робить її придатною для щорічного оновлення знань, але не для сприяння довготривалим змінам у поведінці. Важливою особливістю гри є негайний детальний зворотній зв'язок після кожного питання, що дозволяє користувачам вчитися на своїх помилках або миттєво зрозуміти правильні відповіді. Хоча гра безкоштовна і пропонує складні запитання, вона має обмежені елементи гейміфікації і не призначена для довгострокового навчання.

Рис. 3.5. Інтерфейс The Weakest Link [41]

Football Fever – це гра з підвищення обізнаності про безпеку, розроблена відділом інформаційних технологій для студентів Техаського університету A&M, але вона доступна для всіх охочих. Гравці беруть участь як члени університетської команди з американського футболу, а спортивна тема інтегрована у всю гру. Хоча зв'язок між кібербезпекою і футболом незрозумілий, ця тема додає розважальної складової. Замість традиційної кнопки "Надіслати" гравці натискають кнопку "Подача", щоб відповісти на запитання, отримуючи миттєвий зворотній зв'язок за неправильні відповіді ("Перехоплення!"). Гра безкоштовна і забезпечує миттєвий зворотній зв'язок, але вона має обмежені елементи гейміфікації, футбольна тема

може не викликати належного резонансу, і вона не підходить як довгострокове рішення або для використання в організації [42].

Cyber Circus – це гра для підвищення обізнаності про безпеку, також створена Техаським університетом A&M, в першу чергу орієнтована на студентів університету, але доступна для всіх бажаючих. Гра має циркову тематику, що додає розважального характеру, хоча й не навчає користувачів реальним організаційним ризикам. Студенти, які грають у три з чотирьох ігор, отримують купон на їжу, що заохочує до участі, хоча цей стимул недоступний для звичайних користувачів або організацій. Однією з родзинок гри є гра "Кидок у кільце", де правильні відповіді дозволяють гравцям закинути баскетбольний м'яч, що додає веселого інтерактивного елементу. Хоча Cyber Circus є безкоштовною і забезпечує миттєвий зворотній зв'язок, вона має нереалістичний сюжет, обмежені елементи гейміфікації і не підходить як довгострокове рішення або для професійних організацій [43].

Deepspace Danger, створена компанією Infosec, – це гра для підвищення обізнаності з кібербезпеки, дія якої розгортається в космічному просторі і супроводжується вражаючими, але довгими анімаційними роликами. Сюжет гри передбачає управління комп'ютером, що містить персональні дані кожної істоти в Сонячній системі, поки ваш колега ремонтує пошкоджений космічний корабель. Після кожного відео-сегменту гравці відповідають на запитання з декількома варіантами відповідей, пропонуючи цікавий, але дещо пасивний досвід навчання. Творча космічна тема, хоча і є цікавою, не має прямого відношення до реального організаційного контексту, що потенційно обмежує її ефективність у створенні довготривалих змін у поведінці. Гра забезпечує прямий зворотній зв'язок у відеоформаті та може похвалитися високоякісною анімацією. Однак, нерелевантна історія та довгі відеоролики в поєднанні з незрозумілим ціноутворенням є помітними недоліками [44].

Targeted Attack, створена компанією Trend Micro, - це гра для підвищення обізнаності з кібербезпеки, що відрізняється високою виробничою вартістю, подібною до голлівудського фільму. У грі, яка зосереджена на бізнес-контексті,

використовується великий відеоматеріал з якісною акторською грою та захоплюючою фоновою музикою. Важливим елементом гейміфікації є бюджет на безпеку, представлений червоними позначками у верхньому лівому куті екрану.

Однак довгі відео можуть забирати багато часу і змушувати користувачів пропускати розділи, що може призвести до втрати важливого контексту. Гра призначена для фахівців з кібербезпеки, гравці беруть на себе роль CISO, що робить її менш придатною для всієї організації. У неї можна зіграти лише один раз, сценарії змінюються залежно від вибору гравця, але її корисність зменшується після досягнення щасливого кінця. Хоча гра є безкоштовною, забезпечує прямий зворотній зв'язок у відеоформаті та має актуальний для бізнесу сюжет, вона не є довгостроковим навчальним рішенням і в першу чергу призначена для фахівців з кібербезпеки[45].

Cybersecurity Escape Room, розроблена компанією Living Security, використовує популярну концепцію квест-кімнат для тренування обізнаності в галузі кібербезпеки. У цій цифровій грі гравці працюють у командах над розв'язанням кібер-головоломок, маючи на меті виконати завдання швидше, ніж команди-суперники, щоб виграти гру. Цей спільний підхід посилює взаємодію завдяки сильним змагальним елементам. Однак безкоштовної пробної версії немає, і для того, щоб зрозуміти, як працює гра, необхідно замовити демо-версію. Крім того, відсутня інформація про ціну. Хоча гра сприяє командній роботі та співпраці, вона вимагає значного планування і може зайняти багато часу [46].

Гра Cyber Awareness Challenge 2024, розроблена Міністерством оборони США, має ностальгічний дизайн у стилі Windows 98 (Рис. 3.6).

Гра, побудована на анімаційних відео, охоплює широке коло тем, таких як соціальна інженерія, шкідливий код і знімні носії, але в ній помітно бракує контенту про штучний інтелект. У грі може бути складно орієнтуватися, а довгі пояснювальні відео призводять до повільного і трудомісткого процесу навчання для працівників. Незважаючи на ці недоліки, гра є безкоштовною і пропонує широкий спектр тем із сюжетною лінією, заснованою на реальних бізнес-сценаріях. Однак застарілий дизайн та довгі відео є суттєвими мінусами.

Рис. 3.6. Інтерфейс Cyber Awareness Challenge 2024 [47]

Backdoors and Breaches – це аналогова карткова гра, розроблена для полегшення тренувань з реагування на інциденти. З 52 картками, вона пропонує загалом 3840 сценаріїв інцидентів, що дозволяє користувачам дізнатися про тактику кіберзлочинців та необхідні інструменти і методи для підтримки кібербезпеки. Призначена для команд кібербезпеки, вона допомагає підтримувати пильність учасників за допомогою спільної гри. Однак, через складність завдань, вона не підходить для тренінгу з підвищення рівня обізнаності з питань безпеки всієї організації. Гра недорога і пропонує широкий спектр сценаріїв інцидентів, що робить її цінною для експертів з кібербезпеки. Однак її висока складність і трудомісткість роблять її менш придатною для звичайних працівників [48].

Riskio – це настільна гра, розроблена для підвищення обізнаності з кібербезпеки для різноманітної аудиторії, починаючи від нетехнічних осіб і закінчуючи IT-експертами. У грі беруть участь від 3 до 5 гравців, один з яких має бути експертом з кібербезпеки, щоб керувати сесією. Вона слугує цінною вправою для командоутворення, одночасно покращуючи навички з кібербезпеки. Однак вона забирає багато часу і не підходить для регулярної гри в робочий час. Граючи в неї час від часу, наприклад, кожні шість місяців, можна ефективно освіжити знання з безпеки. Гра недорога, сприяє зміцненню командного духу і

розрахована на всі рівні навичок. Однак вона вимагає участі експерта з безпеки і не є довгостроковим рішенням для довготривалої зміни поведінки [49].

Security Awareness Escape Room від Deloitte – це квест-кімната, де учасники повинні розблокувати ноутбук, заражений програмою-вимагачем. Завдання охоплюють такі теми, як фішинг, соціальна інженерія, класифікація та обмін даними. Цей цікавий та ефективний метод навчання також сприяє зміцненню командного духу. Однак він відносно дорогий, коштує щонайменше $6000 за день, включно з налаштуванням, і не підходить для регулярних тренінгів. Хоча він охоплює широке коло тем і значно підвищує залученість і командний дух, його висока вартість і тривалість обмежують його практичність для частого використання [50].

ProProfs пропонує понад 40 тестів з кібербезпеки, створених різними користувачами, надаючи широкий вибір тестів на вибір. Хоча якість тестів варіюється в залежності від автора, відібрані тести, як правило, хороші. ProProfs - це платформа, яка дозволяє користувачам створювати вікторини, тобто контент може бути створений користувачами і з різних галузей. Це робить її корисним ресурсом для швидких, одноразових заходів, пропонуючи безкоштовний варіант серед доступних вікторин. Однак контроль якості контенту є незрозумілим, що робить його менш придатним для організаційного навчання. Крім того, платформі бракує функцій звітування [51].

Hacktale – це навчальна гра для підвищення обізнаності з питань безпеки, розроблена для молодих спеціалістів з кібербезпеки. Гра починається зі сценарію, в якому команда виявляє, що їхній веб-сайт було зламано, і генеральний директор вимагає негайного вирішення проблеми. Хоча гра безкоштовна, а її контент якісний, вона затягнута і має застарілу анімацію. Крім того, їй бракує інтерактивних завдань, які вимагають від гравців просто проходити історію, не беручи участі у вирішенні проблем і не відповідаючи на запитання. Незважаючи на інформативність, повільний темп гри та відсутність інтерактивності роблять її менш придатною для ефективного навчання [52].

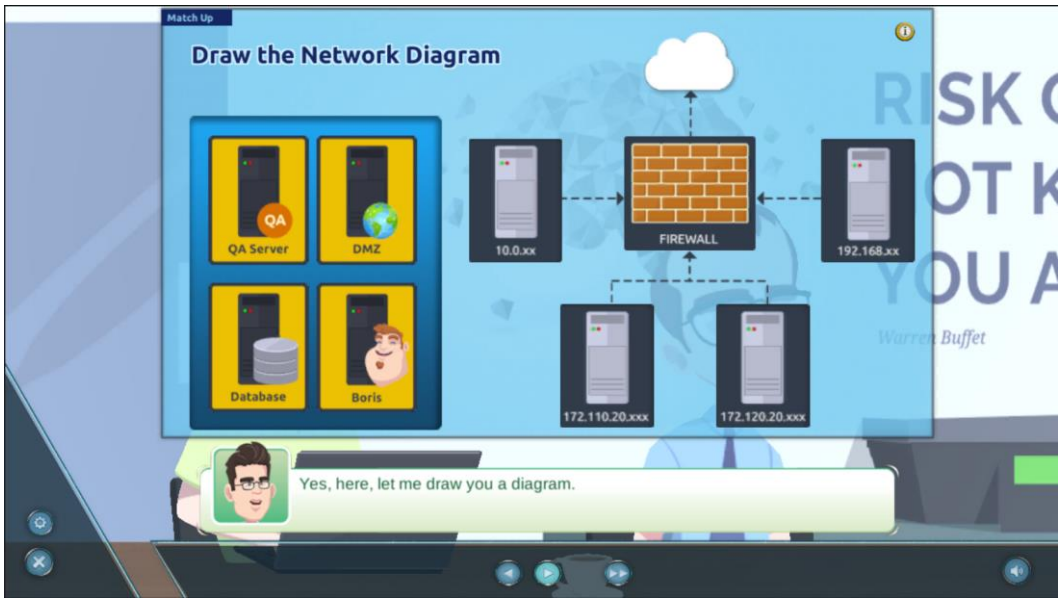


Рис. 3.7. Інтерфейс Hacktale

Cyberstart – це гра, спеціально розроблена для фахівців з кібербезпеки, що робить її менш привабливою для пересічних працівників. Однак вона є чудовою відправною точкою для новачків у сфері кібербезпеки, пропонуючи цікавий спосіб набуття початкового досвіду. Гра має приємний ігровий процес та інтерактивні запитання, а за відповіді на складні запитання можна отримати підказки, які коштують балів. Кожне завдання супроводжується пояснювальним відео, яке надає детальну довідкову інформацію. Хоча Cyberstart пропонує безкоштовну пробну версію та цікавий ігровий процес, вона не підходить для регулярного використання або загального навчання співробітників, а також не має можливостей для створення звітів [53].

Missing Link – це одноразова гра, призначена для навчання гравців розпізнаванню фішингових листів. Вона забезпечує цікавий навчальний процес, коли користувачі визначають ознаки фішингу, після чого на екрані з'являються чіткі пояснення. Хоча такий інтерактивний підхід є ефективним для підвищення обізнаності про фішинг, гра обмежується цією єдиною темою і не охоплює інші сфери кібербезпеки. Вона є безкоштовною і пропонує унікальний навчальний досвід, але не підходить для організаційного навчання через свою вузьку спрямованість і одноразовий характер [54].

Аналіз характеристик розглянутих ігор показано в таблицях 3.1 та 3.2.

Таблиця 3.1.

Порівняння розглянутих продуктів за загальними характеристиками

Характеристики	**Елементи гейміфікації**	**Налаштовуваний контент**	**Можливості звітування**	**Безкоштовна версія**
Guardey	Так	Так	Так	Ні
Counterintelligence Trivia Twirl	Так	Ні	Ні	Так
The Weakest Link	Так	Ні	Ні	Так
Football Fever	Так	Ні	Ні	Так
Cyber Circus	Так	Ні	Ні	Так
Deepspace Danger	Ні	Ні	Ні	Ні
Targeted Attack: The Game	Ні	Ні	Ні	Так
Cybersecurity Escape Room	Так	Так	Так	Ні
Cyber Awareness Challenge 2024	Ні	Ні	Ні	Так
Backdoors and Breaches	Так	Ні	Ні	Ні
Riskio	Так	Ні	Ні	Ні
Deloitte’s Security Awareness Escape Room	Так	Ні	Ні	Ні
40 short quizzes by Proprofs	Ні	Ні	Ні	Так
Hacktale	Ні	Ні	Ні	Так
Cyberstart	Так	Ні	Ні	Так
Missing Link	Так	Ні	Ні	Так

Таблиця 3.2.

Порівняння розглянутих продуктів за характеристиками інтерфейсу

Характеристики	**Підходить для організацій**	**Прямий зворотній зв'язок**	**Забирає багато часу**	**Реалістичний сюжет**
Guardey	Так	Так	Ні	Ні
Counterintelligence Trivia Twirl	Ні	Так	Ні	Ні
The Weakest Link	Ні	Так	Ні	Ні
Football Fever	Ні	Так	Ні	Ні
Cyber Circus	Ні	Так	Ні	Ні
Deepspace Danger	Ні	Так	Так	Ні
Targeted Attack: The Game	Так	Так	Так	Так
Cybersecurity Escape Room	Так	Так	Так	Так
Cyber Awareness Challenge 2024	Так	Так	Так	Так
Backdoors and Breaches	Так	Так	Так	Ні
Riskio	Так	Так	Так	Ні
Deloitte’s Security Awareness Escape Room	Так	Так	Так	Так
40 short quizzes by Proprofs	Ні	Ні	Ні	Ні
Hacktale	Ні	Так	Так	Так
Cyberstart	Так	Так	Ні	Ні
Missing Link	Ні	Так	Ні	Ні

Таким чином, такі ігри, як Guardey, Counterintelligence Trivia Twirl, The Weakest Link та Cyber Circus пропонують захоплююче навчання з безпеки завдяки гейміфікації, миттєвому зворотному зв'язку та інтерактивним сценаріям. Deepspace Danger і Targeted Attack використовують високоякісні відеоматеріали і реалістичні сюжетні лінії для покращення навчання фахівців з кібербезпеки. Аналогові ігри, зокрема Backdoors and Breaches та Riskio, сприяють розвитку командної роботи і практичних навичок. Тим часом Cyber Awareness Challenge 2024 та Hacktale надають всебічний контент, але страждають від застарілого дизайну. Нарешті, Cyberstart та Missing Link пропонують цілеспрямований, веселий досвід, хоча й обмежений за обсягом. Ці ігри в сукупності сприяють підвищенню зацікавленості, закріпленню знань і розвитку практичних навичок у навчанні з кібербезпеки.

3.3 Розроблення програми курсу підвищення обізнаності персоналу з питань інформаційної безпеки

Створення ефективної програми курсу підвищення обізнаності з питань інформаційної безпеки має важливе значення для організацій, щоб захиститися від зростаючих кіберзагроз. Програма починається з визначення унікального ландшафту організації та основних напрямів навчальних тем, таких як фішинг і шкідливе програмне забезпечення, на які припадає значна частка кібератак.

Для зміни поведінки та забезпечення розуміння персоналом своєї ролі в захисті організації вирішальне значення має індивідуальне навчання, яке залучає співробітників і спрямоване на вирішення їхніх повсякденних проблем. Використання різноманітних інструментів, зокрема цікавих відео, реалістичних сценаріїв, вікторин та симуляцій фішингових атак, підвищує ефективність навчання.

Безперервне і регулярне навчання протягом року необхідне для того, щоб іти в ногу з еволюцією загроз і підтримувати високий рівень обізнаності про безпеку серед співробітників. Ефективність навчання слід регулярно перевіряти

за допомогою симуляцій та оцінок, а також відстежувати показники, щоб виявити сфери, які потребують вдосконалення. Такий комплексний підхід забезпечує надійний захист від кіберзагроз і сприяє формуванню в організації культури, в якій безпека стоїть на першому місці.

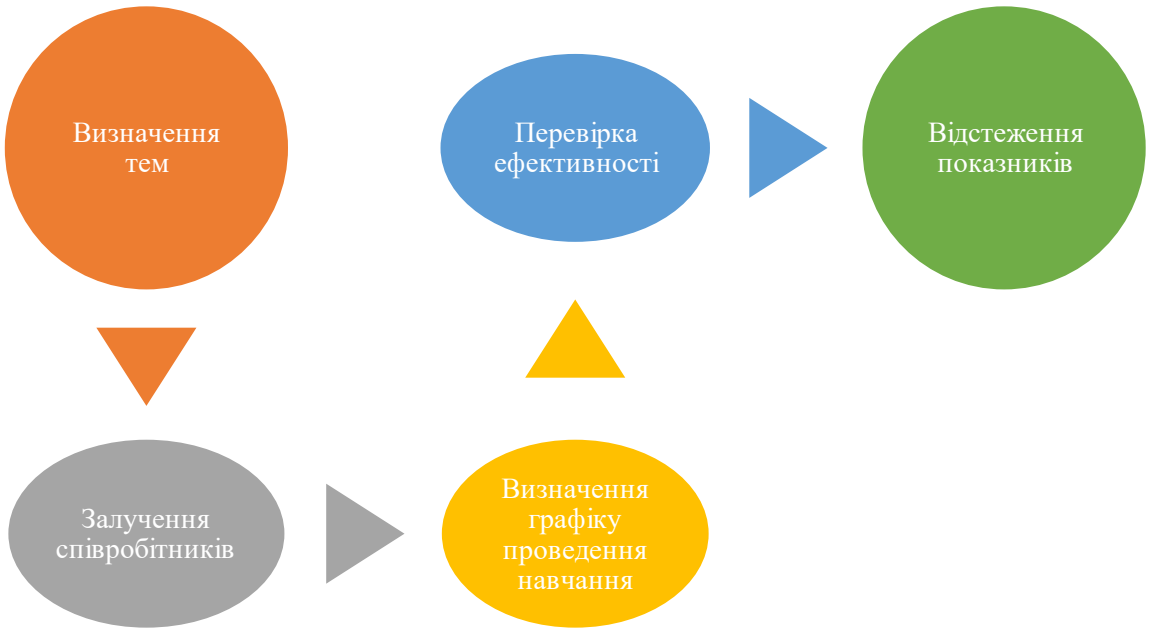


Рис. 3.8. Процес проведення навчання

Процес розробки програми курсу підвищення обізнаності персоналу з інформаційної безпеки починається з всебічного розуміння специфічного ландшафту загроз організації та визначення найбільш актуальних ризиків, таких як фішинг, шкідливе ПЗ й атаки соціальної інженерії.

Курс підвищення обізнаності персоналу з інформаційної безпеки має на меті сформувати уявлення про загрози інформаційній безпеці організації за допомогою серії інтерактивних модулів, які залучають персонал до практичних, реальних сценаріїв. Структура курсу представлена в Додатку А. Рисунок 3.9 показує основні блоки курсу. Додаток Б містить скріншоти з додаткових матеріалів курсу, які забезпечують візуалізацію основних його положень.

Програма підкреслює важливість індивідуального навчання, орієнтованого на конкретну посаду, щоб кожен співробітник розумів свою унікальну роль у захисті організації. Початковий модуль знайомить з основними поняттями кібербезпеки та інформаційної безпеки, використовуючи інтерактивні слайди,

щоб сприяти залученню та розумінню. Розглядаються такі теми, як конфіденційність, цілісність і доступність інформації, з прикладами і перевіркою знань для закріплення матеріалу.

Рис. 3.9. Структура курсу підвищення обізнаності з питань інформаційної безпеки

Наступні модулі заглиблюються в конкретні сфери, такі як фізична безпека, управління паролями та розпізнавання атак соціальної інженерії. Кожен модуль містить практичні поради та інтерактивні вправи, щоб зробити навчання інформативним та цікавим. Наприклад, у модулі з фізичної безпеки обговорюються найкращі практики захисту робочих станцій та поводження з портативними носіями інформації, а модуль з соціальної інженерії містить приклади з реального життя та вправи з моделювання фішингу.

Програма передбачає безперервне навчання шляхом регулярного оновлення та оцінювання. Такий підхід гарантує, що працівники залишаються пильними та обізнаними з найновішими загрозами та практиками безпеки. Включення елементів гейміфікації, таких як вікторини й таблиці лідерів, додатково мотивує персонал і робить процес навчання більш приємним.

Висновки до розділу 3

У процесі дослідження встановлено, що гейміфікація в освітньому процесі є ефективним інструментом для підвищення мотивації та залученості працівників, інтегруючи елементи ігрового дизайну в навчальне середовище. Це сприяє поліпшенню показників засвоєння матеріалу, мотивації та рівня участі

слухачів. Аналіз показав, що інтерактивні платформи та інструменти, такі як відео, анімації, та симуляції, надають учням можливість активно взаємодіяти з контентом, що покращує їх запам'ятовування та розуміння.

Дослідження також показало, що використання персоналізованих навчальних підходів, які враховують індивідуальні потреби та стилі навчання, значно підвищує ефективність навчання. Це підтверджується включенням елементів, таких як індивідуальні профілі, рівні та нагороди, які стимулюють працівників до досягнення нових цілей та покращення своїх результатів.

Порівняльний аналіз програм для навчання, проведений у дослідженні, показав, що на сучасному ринку існує широкий спектр інструментів з елементами гейміфікації, які можуть бути ефективно використані для навчання працівників з питань кібербезпеки. Програми, такі як Guardey, Cyber Circus, та Cyber Awareness Challenge 2024, пропонують інтерактивні та цікаві підходи до навчання, включаючи регулярні оцінки та звітність, що сприяє постійному підвищенню рівня обізнаності та компетентності працівників.

Гейміфікація може значно підвищити ефективність навчання та мотивацію слухачів. Однак її успішне впровадження залежить від ретельної розробки та узгодження з освітніми цілями, гарантуючи, що ігрові елементи підтримують навчальні цілі та не відволікають від них. Інтерактивність, персоналізація та регулярні оцінки є ключовими компонентами, які забезпечують успіх гейміфікації у навчальному процесі.

ВИСНОВКИ

Дослідження показало, що формування обізнаності й навчання персоналу з питань інформаційної безпеки є важливим елементом управління інформаційною безпекою організації, сприяє вихованню свідомого та відповідального ставлення до питань безпеки і, як результат, підвищенню загальної стійкості організації до кіберзагроз, зниженню ризику порушень безпеки та забезпеченню дотримання відповідних стандартів і норм. Використання кращих практик, представлених у публікаціях і стандартах провідних експертних організацій, таких як ISO, NIST та ENISA, забезпечує ефективність програм навчання та обізнаності.

Встановлено, що використання інноваційних технологій у процесі формування обізнаності й навчання персоналу з інформаційної безпеки сприяє підвищенню якості підготовки фахівців, забезпечуючи їх актуальними знаннями і практичними навичками. Це дозволяє організаціям ефективно протидіяти сучасним загрозам та забезпечувати захист інформаційних систем.

Традиційні методи навчання, хоча й забезпечують базову теоретичну підготовку, виявляються недостатніми для повноцінного розвитку практичних навичок та адаптації до нових викликів сучасного світу. Інноваційні технології, такі як електронне навчання, мікронавчання, гейміфікація, віртуальна та доповнена реальність, а також штучний інтелект і машинне навчання, пропонують більш гнучкий, інтерактивний і персоналізований підхід до освіти. Вони дозволяють організаціям надавати працівникам доступ до навчальних матеріалів будь-де і будь-коли, враховуючи їх індивідуальні потреби та стилі навчання.

У результаті дослідження з’ясовано, що електронне навчання, завдяки використанню онлайн-курсів і вебінарів, забезпечує значну гнучкість та знижує витрати на навчання, дозволяючи працівникам поєднувати навчання з іншими зобов'язаннями; інтерактивні платформи з мультимедійним контентом та інструментами для спільної роботи підвищують зацікавленість і ефективність навчального процесу; мікронавчання, яке передбачає надання коротких

цілеспрямованих модулів, дозволяє ефективніше засвоювати знання в умовах напруженого графіка; гейміфікація, інтегруючи ігрові елементи у навчальний процес, підвищує мотивацію та залученість учнів; технології віртуальної і доповненої реальності створюють реалістичні сценарії для практичного навчання, забезпечуючи безпечне середовище для відпрацювання навичок; штучний інтелект і машинне навчання надають персоналізовані рекомендації й адаптують навчальний процес до потреб кожного учня, що значно підвищує ефективність освіти.

Встановлено, що гейміфікація є ефективним інструментом для підвищення мотивації та залученості працівників, інтегруючи елементи ігрового дизайну в навчальне середовище. Це сприяє поліпшенню показників засвоєння матеріалу, мотивації та рівня участі слухачів. Інтерактивні платформи й інструменти відео, анімації та симуляції надають учням можливість активно взаємодіяти з контентом, що покращує їх запам'ятовування та розуміння. Використання персоналізованих навчальних підходів, які враховують індивідуальні потреби та стилі навчання, значно підвищує ефективність навчання. Це підтверджується включенням таких елементів як індивідуальні профілі, рівні й нагороди, які стимулюють працівників до досягнення нових цілей і покращення своїх результатів.

Порівняльний аналіз представлених на ринку програм для навчання з інформаційної безпеки з елементами гейміфікації показав, що такі інструменти можуть бути ефективно використані для навчання персоналу організацій. Так програми як Guardey, Cyber Circus, та Cyber Awareness Challenge 2024 пропонують цікаві інтерактивні підходи до навчання, зокрема регулярні оцінки та звітність, що сприяє постійному підвищенню рівня обізнаності та компетентності працівників.

За результатами дослідження розроблено програму курсу підвищення обізнаності з інформаційної безпеки, яка має на меті сформувати уявлення працівників про загрози інформаційній безпеці організації за допомогою серії інтерактивних модулів, які залучають персонал до практичних, реальних сценаріїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. SP 800-50. Nist. Effective from 2003-10-01. Official edition. Geithersburg : National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

2. Pradigdya C. A., Ginardi R. V. H. User Awareness Design for Electronic Money User Using Protection Motivation Theory and NIST 800-50 Framework. *IPTEK Journal of Proceedings Series*. 2019. No. 5. P. 416. DOI: https://doi.org/10.12962/j23546026.y2019i5.6380

3. Cybersecurity and Infrastructure Security Agency. Insider threat mitigation guide : defining, detecting, assesing, and managing insider threats: cybersecurity and infrastructure security agency. Independently Published, 2022

4. Liebman L. The definition of disability in social security and supplemental security income: drawing the bounds of social welfare estates. Harvard law review. 1976. Vol. 89, no. 5. P. 833. DOI: https://doi.org/10.2307/1340181

5. Krause M., Tipton H. Handbook of information security management. *Edpacs*. 1998. Vol. 26, no. 3. P. 15. DOI: https://doi.org/10.1201/1079/43275.26.3.19980901/31739.5

6. Giousmpasoglou C., Marinakou E. Culture and managers in a globalised world. *Handbook of research on human resources strategies for the new millennial workforce*. 2017. P. 1–27. DOI: https://doi.org/10.4018/978-1-5225-0948-6.ch001

7. Dessler G. Human resource management. Pearson Education, Limited, 2004. 752 p.

8. Lutz R. A. Leadership and management or leading and managing. IEEE engineering management review. 2017. Vol. 45, no. 3. P. 6–8. DOI: https://doi.org/10.1109/emr.2017.2739538

9. Raggad B. G. Information security management: concepts and practice. Boca Raton : Taylor & Francis, 2010.

10. Disterer G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*. 2013. Vol. 04, no. 02. P. 92–100. DOI: https://doi.org/10.4236/jis.2013.42011

11. Fauzi R. Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. *JTERA (Jurnal Teknologi Rekayasa)*. 2018. Vol. 3, no. 2. P. 145. DOI: https://doi.org/10.31544/jtera.v3.i2.2018.145-156

12. Buresh, Ph.D., J.D., LL.M. D. L. A Practical Evaluation of Remote Work Issues and the SolarWinds Breach Using the ISO/IEC 27001 Cybersecurity Framework and the ISO/IEC 27002 Guidelines. Studies in Social Science Research. 2022. Vol. 3, no. 2. P. p75. DOI: https://doi.org/10.22158/sssr.v3n2p75

13. Your guide to designing a cyber-awareness programme. *ENISA*. 2023. URL: https://op.europa.eu/en/publication-detail/-/publication/16917afa-efc2-11ed-a05c-01aa75ed71a1/language-en

14. Dunn Cavelty M., Smeets M. Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*. 2023. P. 1–23. DOI: https://doi.org/10.1080/13501763.2023.2173274

15. L. Oliveira et al., "Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 168-173, DOI: 10.1109/CSR57506.2023.10224910

16. Інноваційні технології навчання : навчальний посібник. Київ. 2017. URL: https://ukreligieznavstvo.wordpress.com/2019/01/18/itn/

17. Information and innovative technologies in the turbulence era. Publishing House of University of Technology, Katowice, 2022. URL: http://www.wydawnictwo.wst.pl/uploads/files/2912632ea83f285f98cb7b0c9bf6ab1b.pdf

18. Mentz, E. & Lubbe, A. (eds.), 2021, 'Learning through assessment: An approach towards Self-Directed Learning', in NWU Self-Directed Learning Series Volume 7. URL: https://www.researchgate.net/publication/356164719_Learning_through_assessment_An_approach_towards_Self-Directed_Learning

19. Nishat Zafar , Muhammad Hafeez S. A Critical Review on Discussion and Traditional Teaching Methods. *Psychology and Education Journal*. 2021. Vol. 58, no. 1. P. 1871–1886. DOI: https://doi.org/10.17762/pae.v58i1.1042

20. Pérez-Juárez M. Á., González-Ortega D., Aguiar-Pérez J. M. Digital Distractions from the Point of View of Higher Education Students. *Sustainability*. 2023. Vol. 15, no. 7. P. 6044. DOI: https://doi.org/10.3390/su15076044

21. Massive Open Online Courses (MOOCs) as Catalysts of Change in Education During Unprecedented Times: A Narrative Review / R. Rulinawaty et al. *Jurnal Penelitian Pendidikan IPA*. 2023. Vol. 9, SpecialIssue. P. 53–63. DOI: https://doi.org/10.29303/jppipa.v9ispecialissue.6697

22. S. Lee. Design of A Learner-Directed E-Learning Model. *University of Hertfordshire*. 2013. URL: https://www.researchgate.net/publication/266136183_Design_of_A_Learner-Directed_E-Learning_Model

23. EdTech Ukrainian Radar / Український радар EdTech. URL: https://www.facebook.com/edtech.ukraine/photos/a.108578624584550/1271933360564412/?type=3

24. Karagiorgas D. N., Niemann S. Gamification and Game-Based Learning. *Journal of Educational Technology Systems*. 2017. Vol. 45, no. 4. P. 499–519. DOI: https://doi.org/10.1177/0047239516665105

25. Гра як інструмент: що таке гейміфікація? *Mistosite*. URL: https://mistosite.org.ua/uk/articles/hra-iak-instrument-shcho-take-heimifikatsiia

26. Hartt M., Hosseini H., Mostafapour M. Game On: Exploring the Effectiveness of Game-based Learning. *Planning Practice & Research*. 2020. Vol. 35, no. 5. P. 589–604. DOI: https://doi.org/10.1080/02697459.2020.1778859

27. Kaledio P., Robert A., Frank L. The Impact of Artificial Intelligence on Students' Learning Experience. *SSRN Electronic Journal*. 2024. DOI: https://doi.org/10.2139/ssrn.4716747

28. Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review / I. Gligorea et al. 2023. Vol. 13, no. 12. P. 1216. DOI: https://doi.org/10.3390/educsci13121216

29. A.M.F. Pelser; V. Vaiman; S. Nagy. The improvement of Skills & Talents in the workplace. 2022. URL: https://www.researchgate.net/publication/369661218_The_improvement_of_Skills_Talents_in_the_workplace

30. SC Training (formerly EdApp). *Safetyculture*. URL: https://training.safetyculture.com

31. Whatfix Digital Adoption Platform. Whatfix. URL: https://whatfix.com

32. Panadero E., Lipnevich A. A. A review of feedback models and typologies: Towards an integrative model of feedback elements. *Educational Research Review*. 2022. Vol. 35. P. 100416. DOI: https://doi.org/10.1016/j.edurev.2021.100416

33. T. M. Nikolić, N. Perić, A. Bovan. The Role of Feedback as a Management Toolin Performance Management Program. *Quality - Access to Success*. Vol. 21, No. 177. URL: https://www.researchgate.net/publication/343152520_The_Role_of_Feedback_as_a_Management_Tool_in_Performance_Management_Program

34. Schechter C. Organizational Learning Mechanisms: The Meaning, Measure, and Implications for School Improvement. *Educational Administration Quarterly*. 2007. Vol. 44, no. 2. P. 155–186. DOI: https://doi.org/10.1177/0013161x07312189

35. Davis T. J., Merchant Z., Kwok O.-M. An Examination of Practice-Based Virtual Simulations and Pre-Service Mathematics Teaching Efficacy and Outcome Expectancy. *Education Sciences*. 2022. Vol. 12, no. 4. P. 262. DOI: https://doi.org/10.3390/educsci12040262

36. Howard C., Bevins K. Game mechanics and why they are employed: What we know about gamification so far. *Issues and Trends in Educational Technology*. 2018. Vol. 6, no. 1. DOI: https://doi.org/10.2458/azu_itet_v6i1_bevins

37. Christopoulos A., Mystakidis S. Gamification in Education. *Encyclopedia*. 2023. Vol. 3, no. 4. P. 1223–1243. DOI: https://doi.org/10.3390/encyclopedia3040089

38. Duarte L. C. S., Battaiola A. L. Distinctive features and game design. Entertainment Computing. 2017. Vol. 21. P. 83–93. DOI: https://doi.org/10.1016/j.entcom.2017.03.002

39. Drive behavior change with security awareness gaming. *Guardey*. URL: https://www.guardey.com

40. CDSE's Counterintelligence Trivia Twirl. *Usalearning*. URL: https://securityawareness.usalearning.gov/cdse/multimedia/games/citrivia/index.html

41. The weakest link. *Isdecisions*. URL: https://www.isdecisions.com/user-security-awareness-game/

42. Football Fever – Secure the Win. *Tamu*. URL: https://it.tamu.edu/footballfever/about/

43. The Aggie Cybersecurity Circus. *Tamu*. URL: https://it.tamu.edu/cybercircus/

44. Deepspace Danger. *Infosec*. URL: https://www.infosecinstitute.com/iq/content-library/deep-space-cybersecurity-game/

45. Targeted Attack. *The Fugle Company*. URL: https://targetedattacks.trendmicro.com

46. Cybersecurity Escape Room. *Livingsecurity*. URL: https://www.livingsecurity.com/products/cybersecurity-escape-games

47. Cyber Awareness Challenge 2024. *Dod Cyber Exchange Public*. URL: https://public.cyber.mil/training/cyber-awareness-challenge/

48. Backdoors and Breaches. *Blackhillsinfosec*. URL: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

49. Riskio. *Riskio*. URL: https://www.riskio.co.uk

50. Deloitte's Security Awareness Escape Room. *Deloitte*. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cyber-risk-the-security-awareness-escape-room.pdf

51. 40 short quizzes by Proprofs. *Proprofs*. URL: https://www.proprofs.com/quiz-school/topic/cyber-security

52. Hacktale. *Komodosec*. URL: https://www.komodosec.com/hacktale

53. Cyberstart. *Cyberstart*. URL: https://cyberstart.com

54. Missing Link. *Tamu*. URL: https://it.tamu.edu/missinglink/about/

Додаток А

ПРОГРАМА КУРСУ ТА ІНТЕРАКТИВНІ СЛАЙДИ

1 блок курсу

Вступ

Кібербезпека стала головним пріоритетом для всіх організацій. Доведено, що більшість витоків даних є прямим результатом помилок кінцевих користувачів. Незалежно від рівня навичок, всі ми вважаємося "кінцевими користувачами". Проходження цього ознайомчого курсу допоможе нам краще захистити довірену нам конфіденційні інформацію та дані, а також ознайомить з деякими типовими тактиками, які ми можемо використовувати для захисту нашої особистої інформації.

Теми курсу

Технології та загрози інформації, системам і мережам постійно розвиваються, проте існують деякі основні заходи, яких можна вжити, щоб краще захистити себе та свою організацію.

Що для вас означає інформаційна безпека?

//Слайд, де слухачі залучаються до обговорення: назвати ключові слова, що пов’язані з ІБ. за кожну відповідь +1 бал//

Національний інститут стандартів і технологій визначає інформаційну безпеку як "захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності". Забезпечення безпеки інформації - обов'язок кожного працівника.

Різні форми інформації

//інтерактивний слайд: вписати 3 види форми інформації. за кожну відповідь +1 бал//

У сучасному робочому середовищі багато інформаційних систем є електронними, але інформація (або дані) існує в різних форматах і повинна бути захищена. Нижче перераховані всі форми, в яких можуть поширюватися дані:

- Електронний
- Паперовий
- Усний

Кібербезпека

Національний інститут стандартів і технологій (NIST) дає таке визначення кібербезпеки: "Сукупність технологій, процесів і практик, призначених для захисту мереж, комп'ютерів, програм і даних від атак, пошкоджень або несанкціонованого доступу".

Інформаційна безпека проти кібербезпеки

Пам'ятайте, що інформаційна безпека стосується всієї інформації, незалежно від її формату, зберігання або способу передачі (електронного, паперового чи усного). Термін "кібербезпека" має цифровий або комп'ютерний підтекст. У цьому курсі основна увага приділяється спробам захистити інформацію, технології, які переносять інформацію, та інформаційні системи.

Мета інформаційної безпеки

//інтерактивний слайд: назвати 3 елементи мети ІБ. за кожну відповідь +1 бал//

Коли ми чуємо фразу "захист інформації", більшість з нас думає про збереження певної інформації та деталей у таємниці. Метою інформаційної безпеки є не створення та збереження секретів, а захист конфіденційності, цілісності та доступності інформації та інформаційних систем. Наступні 3 елементи включені в загальну мету інформаційної безпеки:

- Конфіденційність
- Цілісність
- Доступність

Приклад

Ваш банківський рахунок є гарним прикладом інформаційної системи, яка повинна бути конфіденційною, доступною та цілісною. Уявіть собі наступні сценарії:

- Ваш рахунок не був конфіденційним і хтось інший зміг отримати доступ до нього, підійшовши до банкомату. Яка сума збитків може бути завдана?

- Кожного разу, коли ви підходили до банкомату, баланс, який він показував, був неточним. Як погана достовірність інформації про ваш баланс може вплинути на ваше бюджетування та рішення про витрати?

- Банкомат вашого банку був недоступний, коли він вам був дуже необхідний. Чи продовжили б ви користуватися послугами цього банку?

Перевірка знань

//інтерактивний слайд: за правильну відповідь +5 балів//

Тепер, коли ви зрозуміли 3 ключові елементи інформаційної безпеки, ви готові дізнатися про загрози інформаційній безпеці та свою роль у захисті цієї інформації.

Яка мета інформаційної безпеки?

А - Впевненість, що працівники мають належну ідентифікацію

Б - Захист конфіденційності, цілісності та доступності інформації та інформаційних систем

В - Захист інформації паролями

Правильна відповідь: Б! Метою інформаційної безпеки є захист конфіденційності, цілісності та доступності інформації та інформаційних систем.

//інтерактивний слайд: підбиття підсумків, видача заохочувального бонусу; підсумкова таблиця + рамочки для 3-х лідерів по балам//

Робиться після кожного блоку

2 блок курсу

Фізична безпека

Фізична безпека є важливим елементом захисту інформаційних систем. Обмеження доступу уповноваженого персоналу до інформаційних систем та інфраструктури зменшує ймовірність викрадення або неправомірного використання інформації.

//інтерактивний слайд: назвати дії для забезпечення фізичної безпеки. за кожну відповідь +1 бал

Приклади відповідей: Уникайте переслідування - ніколи не дозволяйте нікому йти за вами в будівлю або на територію, що охороняється, без бейджа. Не бійтеся оскаржувати або повідомляти про тих, хто не показує бейдж відвідувача (пропуск). Не дозволяйте іншим використовувати вашу перепустку для доступу до будівлі або безпечної зони. Повідомляйте про будь-яку підозрілу активність співробітникам служби безпеки будівлі.//

Захистіть своє робоче місце //інтерактивний пост, за відповіді слухачів +1 бал//

Захист робочого місця є важливим компонентом фізичної безпеки, і часто не береться до уваги, оскільки ми відчуваємо себе комфортно або навіть самовдоволено на своєму робочому місці.

Нижче наведено лише кілька причин, чому варто заблокувати робоче місце:

- Правила щодо захисту конфіденційних даних, включаючи, але не обмежуючись ними: Інформація, що ідентифікує особу (PII), захищена інформація про здоров'я (PHI), федеральна податкова інформація (FTI), інформація про кримінальне минуле. Кожне з них має наслідки за недотримання належного протоколу обробки.

- Запобігання витоку конфіденційної інформації.

- Запобігання внутрішнім загрозам (зловмисним або випадковим)

Блокуйте робоче місце, коли залишаєте його, затиснувши CTRL/ALT/Delete - Блокування.

Інші поради щодо фізичної безпеки //інтерактивний пост, за відповіді слухачів +1 бал//

Зберігайте та транспортуйте знімні носії, такі як CD/DVD-диски, флеш-накопичувачі та зовнішні жорсткі диски, лише за наявності дозволу та у безпечний спосіб.

Підтримуйте "чистий стіл" і захищайте свій робочий простір, тобто замикайте всі конфіденційні файли та дискети.

Не залишайте документи без нагляду на принтері, копіювальному апараті або факсі.

Не викидайте конфіденційні документи у смітник. Замість цього утилізуйте інформацію належним чином за допомогою шредера.

Прибирайте папери та витирайте дошки після завершення використання конференц-залів.

Замикайте шафи, коли йдете.

Подрібнюйте або іншим чином знищуйте конфіденційні документи, коли викидаєте їх.

Портативні носії

Портативні носії - це пристрої, які зберігають інформацію, але фізично не є частиною комп'ютера. До них відносяться, зокрема, CD-ROM, DVD, флеш-накопичувачі USB.

Переконайтеся, що ви використовуєте тільки портативні носії відповідно до вашої політики.

Портативні носії - це чудовий винахід, який робить перенесення даних з одного комп'ютера на інший дуже зручним. Однак без захищеного мережевого з'єднання портативні носії можуть занести шкідливе програмне забезпечення на ваш комп'ютер та інформаційні системи. Портативні носії також піддаються підвищеному ризику втрати або крадіжки.

Поклади флешку: Ти не знаєш, де вона була!

Флешки та USB-накопичувачі становлять величезний ризик для організацій. Використання флеш-накопичувача або USB для перенесення файлів між особистими та державними пристроями може призвести до потрапляння вірусів або шкідливого програмного забезпечення на державні ресурси.

Не ризикуйте безпекою своїх приватних пристроїв та інформації. Доступ до інформації з чужого флеш-накопичувача може не лише зашкодити

технологіям та інформації вашої організації, але й завдати серйозної шкоди вашим власним ресурсам.

Якщо ви натрапите на флешку або USB-пристрій, що лежить поруч, не вставляйте його в будь-який пристрій.

Перевірка знань //за правильну відповідь слухачу +5 балів//

Аві потрібно залишити своє робоче місце, щоб поставити запитання колезі. Що вона повинна зробити перед тим, як покинути своє робоче місце?

А - Заблокуйте її робоче місце, натиснувши CTRL/ALT/Delete - Lock

Б - Вимкніть її монітори.

В - Вийдіть з її електронної пошти

Правильна відповідь - А.

Паролі

Паролі = Ціль

Паролі є часто атакованою вразливістю в будь-якій системі. Надійний пароль для вашого мережевого облікового запису та інших додатків є базовим механізмом захисту. Створити простий або загальний пароль легко, але небезпечно.

Системи та веб-сайти мають різні мінімальні стандарти для паролів. НЕ дотримуйтесь мінімальних стандартів!

Поради щодо створення кращих паролів //інтерактивний пост, за відповіді слухачів +1 бал//

- Не використовуйте знайомі імена.

- Уникайте використання загальних або легкодоступних фактів про себе (день народження, клички домашніх тварин тощо).

- Уникайте словникових слів. Чому? Тому що програми для "злому" можна легко придбати в Інтернеті. Просто замініть літери на спеціальні символи або цифри. Приклад: F00t6@11 замість "Football".

- Довжина та складність пароля значно ускладнюють завдання хакера.

Більше про довжину та складність пароля

Чи знали ви, що пароль з 8 символів можна зламати миттєво, якщо він містить лише цифри? На злам більш безпечного пароля, що містить цифри, великі та малі літери, а також спеціальні символи, такі як $ % & тощо, можуть піти тижні. Поєднання цифр, великих/малих літер і спеціальних символів робить пароль більш "складним".

Хоча нам важко запам'ятати кілька паролів, утримайтеся від використання одного і того ж пароля для більш ніж одного сайту. Використовуючи один і той самий пароль для кількох облікових записів, ви просто даєте ключ до всіх акаунтів.

Чи знали ви? Пароль, що містить 16 символів, включаючи цифри, великі та малі літери, а також спеціальні символи, можна зламати за 193 трильйони років?

Захист ваших паролів

Важливо не лише створювати надійні паролі, але й захищати їх. Нижче наведено лише кілька порад щодо захисту ваших паролів:

- Не діліться своїми паролями - службі підтримки не обов'язково знати ваш пароль, оскільки у них є доступ до інших засобів, які допоможуть вам відновити систему. Вважайте будь-який електронний лист або телефонний дзвінок з проханням повідомити ваш пароль шахрайством.

- Не записуйте свій пароль і не зберігайте його на робочому місці

- Паролі не повинні зберігатися в елекронному файлі.

- Не використовуйте один і той самий пароль у різних системах або на різних сайтах.

Пам'ятайте!

Пам'ятайте, що більшість систем вимагають від вас змінювати пароль через певні проміжки часу, і ви повинні робити те ж саме для своїх особистих облікових записів. Ваші гроші, особисті дані та інформація про кредитні картки є спокусливими цілями і постійно піддаються атакам. Пам'ятати про зміну паролів і мати унікальні паролі для всіх облікових записів - клопітка справа, але якщо ви коли-небудь ставали жертвою крадіжки особистих даних або у вас вкрали гроші, це варте зусиль. Встановіть собі календарне нагадування!

Перевірка знань //+5 балів за відповідь//

Який з наведених нижче паролів найбезпечніший?

А - Дженні!21

Б - B1@ckH@wksRule!!!

В - ChicagoBears2018

Г - 1234567891011123

Б - правильна відповідь, оскільки вона складається з 16 символів і є складною (цифри, великі та малі літери, спеціальні символи).

Варіант А має складність, але він складається лише з 8 символів.

Варіант В має гарну довжину, але не має складності. Використовує слова зі словника, так прості числа.

Варіант D має довжину, але складається лише з чисел. Його можна зламати за лічені секунди.

3 блок курсу

Соціальна інженерія

Що таке соціальна інженерія?

Простіше кажучи, соціальна інженерія - це спосіб обманом змусити людей розкрити особисту інформацію або інші конфіденційні дані. Це загальний термін, який включає в себе фішинг, фармінг, смішинг, вішинг та інші види маніпуляцій. Термін "соціальна інженерія" звучить досить невинно, але це зловмисна дія і тема, яку повинні розуміти всі користувачі Інтернету. Саме тут ВИ стаєте найслабшою ланкою в периметрі безпеки вашої організації. Ви стаєте мішенню вдома і на роботі.

Атаки соціальної інженерії є більш поширеними і більш успішними, ніж комп'ютерні хакерські атаки на мережу.

На відміну від хакерства, соціальна інженерія більше покладається на хитрість і психологічну маніпуляцію, ніж на технічні знання. Наприклад, зловмисник може надіслати вам "фішинговий" електронний лист, в якому йдеться про необхідність скинути ім'я користувача та пароль для певного веб-сайту. Лист може виглядати легітимним, але якщо ви натиснете на посилання в

повідомленні, то потрапите на фальшивий веб-сайт, який викраде вашу інформацію.

Хибні тривоги на веб-сайтах

Інший поширений тип соціальної інженерії використовує неправдиві повідомлення на веб-сайтах. Наприклад, коли ви відкриваєте веб-сторінку, ви можете отримати повідомлення про те, що на вашому комп'ютері вірус і вам потрібно завантажити певну програму або зателефонувати за номером телефону, щоб виправити це.

У більшості випадків ці сповіщення генеруються автоматично і є абсолютно неправдивими. Якщо ви будете дотримуватися інструкцій у попереджувальному повідомленні, ви можете завантажити шпигунське програмне забезпечення або розголосити особисту інформацію по телефону.

Доцільно скептично ставитися до будь-яких повідомлень, електронних листів або веб-сайтів, які просять вас поділитися особистими даними - особливо якщо запит надійшов з невідомого джерела.

Пояснення соціальної інженерії

Соціальним інженерам потрібна будь-яка інформація, яка дасть їм доступ до державних систем або об'єктів. Поширеними цілями є //інтерактивний пост, за відповіді слухачів +1 бал//:

- Паролі
- Бейджики безпеки (пропуски)
- Доступ до захищених зон будівлі
- Смартфони
- Гаманці
- Особиста інформація працівника або клієнта

4 блок курсу

Фішинг

Фішери розсилають електронні листи, які виглядають як такі, що надходять від легітимних веб-сайтів або банківських установ.

В електронному листі зазначено, що вашу інформацію необхідно оновити або підтвердити. Після цього вам буде запропоновано ввести ім'я користувача та пароль після переходу за посиланням, що міститься в електронному листі. У деяких листах вас попросять ввести ще більше інформації, наприклад ваше повне ім'я, адресу, номер телефону, номер соціального страхування та номер кредитної картки.

Розголошення вашого імені користувача та пароля може дати "фішеру" доступ до інших облікових записів, якщо ви повторно використовуєте паролі.

Поради щодо фішингу

Фішингові електронні листи часто виглядають напрочуд легітимно і навіть веб-сторінки, на яких вас просять ввести свої дані, можуть бути справжніми. Однак URL-адреса в адресному полі може дати вам деякі підказки про те, чи це шахрайство, чи ні.

//приклад – інтерактивний, за правильні відповіді +1 бал//

Уявімо, що ім'я популярного ритейлера, з яким ви часто працюєте, - "Discount.com".

- "http://www.discount.com" та "http://cgi3.discount.com" є дійсними веб-адресами

- А от "http://www.discount.validate-info.com" та "http://discount.login123.com" - це фальшиві адреси, які можуть бути використані фішерами.

Якщо ви отримали електронного листа з проханням оновити вашу інформацію і ви вважаєте, що вона може бути дійсною, перейдіть на веб-сайт, набравши URL-адресу в адресному полі вашого браузера, а не переходячи за посиланням в електронному листі.

Якщо ви підозрюєте, що лист недійсний//інтерактив//:

- НЕ переходьте за посиланнями, наданими в електронному листі

- НЕ відкривайте жодних вкладень в електронному листі

- НЕ надавайте особисту інформацію та фінансові дані

Ставтеся з підозрою до будь-якого електронного листа, який: //інтерактив//

- Запитує особисту інформацію
- Містить орфографічні та граматичні помилки
- Просить перейти за посиланням
- є неочікуваним або від організації, з якою ви не маєте нічого спільного

Повідомленя про фішинг

Знайдіть інструмент для звітування про фішинг, який використовується провайдером послуг електронної пошти вашої організації. Якщо у вас немає такої можливості, повідомте про повідомлення вашій команді IT-безпеки, а потім видаліть його!

Ніколи не повідомляйте свій пароль НІКОМУ в електронному листі або по телефону!

Приклад фішингу №1

Від: XXXXX.XXXXX

Відправлено: Вівторок, 24 березня 2024 8:30 AM

Тема: Важливе повідомлення

Важливе повідомлення від служби підтримки. Ваша поштова скринька досягла максимального ліміту в 20 ГБ і ваш обліковий запис буде вимкнено, якщо ви не оновите його зараз.

Для вашого ж блага ви повинні надати правильну інформацію, щоб ми могли оновити ваш обліковий запис електронної пошти і пам'ятайте, що без правильної інформації ваш обліковий запис електронної пошти буде закрито.

Оновити свій обліковий запис електронної пошти вже сьогодні

НАТИСНІТЬ ТУТ.

Ваш обліковий запис залишиться активним після того, як ми успішно підтвердимо вашу електронну пошту.

Приклад фішингу №2

Від: XXXXXXXX@gov.bm

Відправлено: Четвер, 10 грудня 2023 6:00 AM

Тема: Призупинений акаунт (Служба підтримки)

Увага!

Термін дії вашого пароля закінчується через 2 години. Ви можете змінити свій пароль нижче на СТОРІНЦІ УПРАВЛІННЯ АККАУНТОМ.

Натисніть на ЗМІНИТИ ПАРОЛЬ

Якщо пароль не буде змінено протягом наступних 2 годин, у наступному вході буде відмовлено. Якщо у вас виникли труднощі зі зміною пароля, оновленням облікового запису електронної пошти, квотами доступу до файлів або відсутніми файлами, будь ласка, зв'яжіться зі службою підтримки ITC (itshelpdesk@webmail.org/XXXXX).

З повагою, IT Services

Пояснення фішингу зі списом

Списовий фішинг - це спроба маніпулювати особою, яка володіє інформацією, до якої хакер хоче отримати доступ. Зловмисник може володіти однією або кількома частинами внутрішньої інформації, яку він, як правило, використовує як важіль впливу, намагаючись отримати інформацію від особи.

Завжди перевіряйте запити, перш ніж надсилати будь-яку конфіденційну або чутливу інформацію

Списовий фішинг в дії: //розставити слухачами//

Крок 1 - Зловмисник отримує ім'я людини з відділу кадрів.

Крок 2 - Озброївшись вищевказаною інформацією та ім'ям керівника компанії, зловмисник надсилає електронного листа (підробленого так, щоб виглядало ніби він надійшов від самого керівника компанії) безпосередньо людині у відділі кадрів.

Крок 3 - У фальшивому електронному листі керівник просить надати всю інформацію про заробітну плату всіх, хто працював у компанії за попередній рік.

Крок 4 - Працівник відділу кадрів виконує запит

Крок 5 - Після того, як інформація була відправлена, працівник відділу кадрів може навіть не здогадатися, що вона потрапила на неправильну електронну адресу. Вся інформація просто потрапила до зловмисника.

Інші фішингові терміни

"Смішинг" - фішингове шахрайство, що здійснюється за допомогою текстових повідомлень (СМС)

"Вішинг" - фішингове шахрайство, що здійснюється за допомогою телефонного дзвінка

Кіберзлочини не обмежуються лише комп'ютерами. Як робочі, так і приватні телефонні лінії можуть стати об'єктом "смішингу" та "вішингу".

Приклад смішингу та вішингу

- Злочинці налаштовують автоматизовану систему набору, щоб надсилати повідомлення або телефонувати людям у певному регіоні або за певним телефонним кодом. Жертви отримують повідомлення на кшталт: "З вашим рахунком виникли проблеми" або "Вашу банківську картку заблоковано", а потім перенаправляють на телефонний номер або веб-сайт з проханням надати особисту інформацію. Озброївшись цією інформацією, злочинці можуть красти з банківських рахунків жертв, оплачувати покупки з їхніх платіжних карток, створювати фальшиві банкомати тощо.

- Смішинг за допомогою текстових повідомлень з використанням проблемного сценарію: "Кредитна спілка. Будь ласка, зателефонуйте за номером 1-800-555-1212 з приводу транзакції по вашій кредитній картці".

- Смішинг з текстовим повідомленням за сценарієм сповіщення: "Банк. Баланс вашого рахунку перевищує $5000. Будь ласка, зателефонуйте за номером 1-800-555-1212".

- Вішинг за допомогою телефону, використовуючи самозванство: "Привіт, Джиме, це Майк з відділу доставки. Я забув номер рахунку для купівлі матеріалів. Можеш мені допомогти?"

- Вішинг по телефону з використанням співчуття: "Мені потрібно, щоб ця заява була подана до 17:00, інакше мене оштрафують на 100 доларів. Я не знаю номер свого рахунку, але він не змінився з минулого року. Чи можете ви сказати мені номер мого рахунку з минулорічної заяви?"

Перевірка знань //5 балів//

Фішинговий лист...

А - Є різновидом соціальної інженерної атаки

Б - Може бути від організації, яку ви знаєте, наприклад, від професійної асоціації

В - Містить посилання на веб-сайт, який просить вас надати особисту інформацію

Г - Все вищезгадане

З усіх перерахованих вище варіантів найкращою відповіддю є варіант Г.

5-ий блок курсу

Конфіденційність

Конфіденційність - це сукупність інформаційних практик, які гарантують, що особиста інформація є точною, релевантною та актуальною; всі способи збору, використання та розкриття особистої інформації є відомими та належними; особиста інформація є захищеною.

Що таке конфіденційні дані?

Дані слід класифікувати як Конфіденційні, якщо несанкціоноване розкриття, зміна або знищення цих даних може спричинити значний рівень ризику для громадян, клієнтів і вашої організації, наших постачальників і партнерів. Приклади конфіденційних даних включають: дані, захищені державними або федеральними нормами про конфіденційність, дані, захищені угодами про конфіденційність.

Конфіденційні дані включають, але не обмежуються ними: //інтерактив//

Інформація про судимість

Інформація, що дозволяє ідентифікувати особу

Персональна інформація про здоров'я

Індивідуальна ідентифікаційна медична інформація

Федеральна податкова інформація

Управління соціального забезпечення

Управління з примусового стягнення аліментів

Національний довідник даних про нових працівників

Інформація про освіту

Загрози

Категорії загроз

Коли ви думаєте про загрози для інформаційних систем і даних, ви можете розбити їх на 4 загальні категорії:

- Стихійні лиха, такі як торнадо, урагани, повені та грозові розряди, можуть завдати шкоди IT-системам

- Зловмисні аутсайдери - іноземні держави, злочинні угруповання, хакери, спамери, промислові шпигуни тощо.

- Зловмисны інсайдери - незадоволені співробітники або постачальники, шпигуни, активісти, незадоволені клієнти

- Випадкові інсайдери - будь-який співробітник!

Що ви можете зробити?

Очевидно, що ви не можете контролювати стихійні лиха та загрози, але як працівник або приватна особа ви можете забезпечити резервне копіювання та захист важливої інформації та систем на випадок катастрофи. Захист від зловмисників починається з того, щоб не піддаватися на фішингові афери, використовувати надійні паролі та розумно користуватися інтернетом.

Внутрішня загроза

Зловмисний інсайдер приймає свідоме рішення навмисно завдати шкоди організації; він повністю усвідомлює свої дії і розуміє, яку шкоду або вплив вони можуть мати на організацію. Деякі з них є технічно підкованими користувачами, які реагують на виклики. Вони використовують свої знання про слабкі місця та вразливості, щоб обійти систему допуску та отримати доступ до конфіденційної інформації.

Випадковим інсайдером може стати будь-хто. Кожен з нас може стати випадковим інсайдером. Випадкові інсайдери часто метафорично "відкривають двері" зловмисникам, залишаючи конфіденційні дані та паролі поблизу або залишаючи своє робоче місце незамкненим.

Випадкові інсайдери - це те, як зловмисники отримують доступ до наших інформаційних систем або даних. Випадкові інсайдери переходять за посиланнями в електронних листах або розголошують ідентифікатори користувачів і паролі під час фішингових атак.

Випадковим інсайдером може бути той, хто випадково розкриває дані - наприклад, працівник, який отримує доступ до даних компанії через громадський Wi-Fi, не знаючи, що він не захищений.

Інформаційна безпека - це відповідальність КОЖНОГО

У разі втрати, крадіжки або неправомірного використання даних важливо реагувати належним чином. Поширені інциденти та питання, пов'язані з безпекою, включають, але не обмежуються ними: //інтерактив//

- Підозра на вірус
- Відсутній файл
- Пошкоджені дані
- Неможливість підключитися до сервера або робочої станції
- Загублений або вкрадений ноутбук
- Загублений мобільний телефон
- Конфіденційна інформація, випадково надіслана несанкціонованому одержувачу
- Конфіденційна інформація, надіслана незахищеним способом

Ваш обов'язок як співробітника //інтерактив//

Як співробітник або підрядник, ви несете відповідальність за захист інформаційних і технологічних ресурсів нашої організації.

ВИ є передньою лінією захисту і найпростішим способом для кіберзлочинців отримати доступ до інформації.

Це може призвести до інцидентів, пов'язаних з конфіденційністю та даними:

Неспроможність нашої організації виконувати свою місію

Порушення повсякденної діяльності

Нанесення шкоди репутації нашої організації

Заподіяння шкоди здоров'ю або фінансовому стану особи

Служба підтримки/Сервісна служба

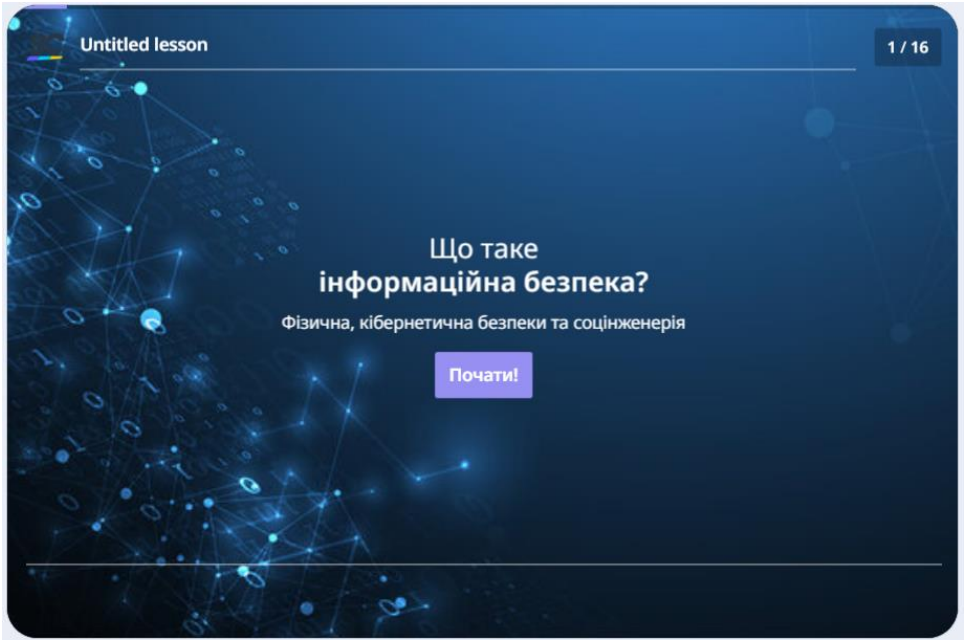
Служба підтримки НІКОЛИ не надсилатиме електронних листів з вимогою надіслати особисту інформацію через електронну пошту, зовнішні веб-сайти, посилання або спливаючі вікна. Будь-який небажаний запит інформації про обліковий запис, який ви отримуєте через електронну пошту, веб-сайти, посилання або спливаючі вікна, слід вважати шахрайством.

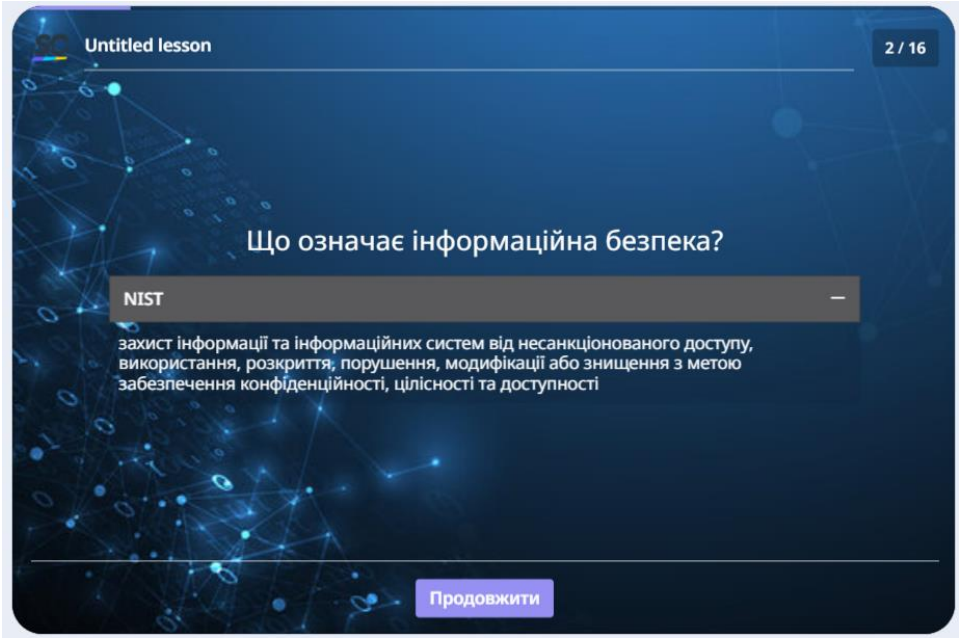
Кінець!

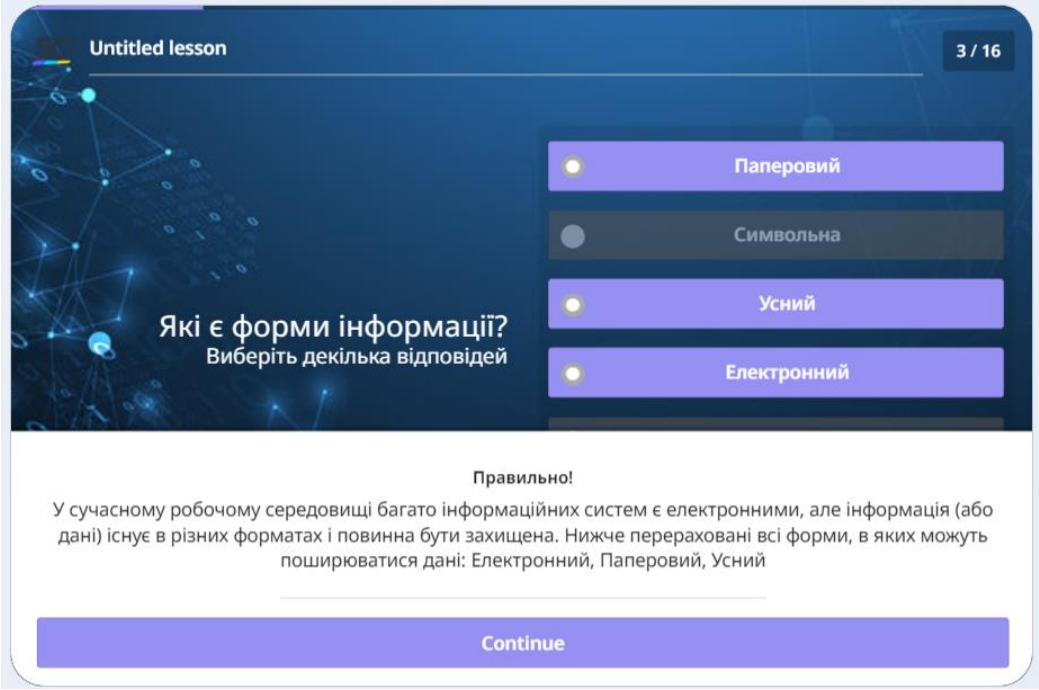
Додаток Б

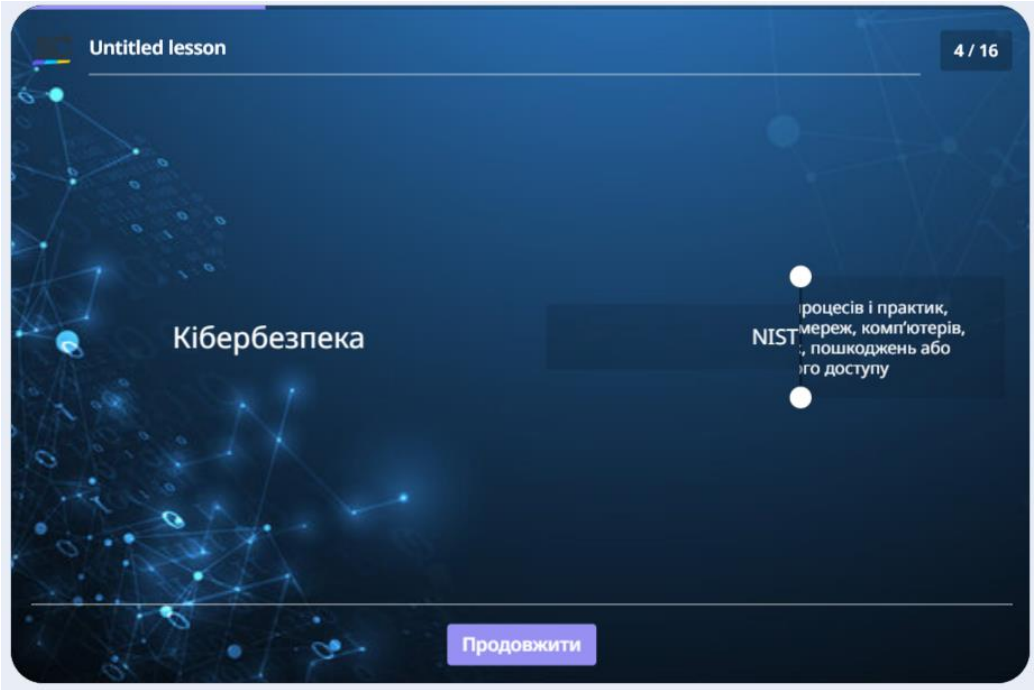
Візуалізація програми курсу навчання персоналу з ІБ

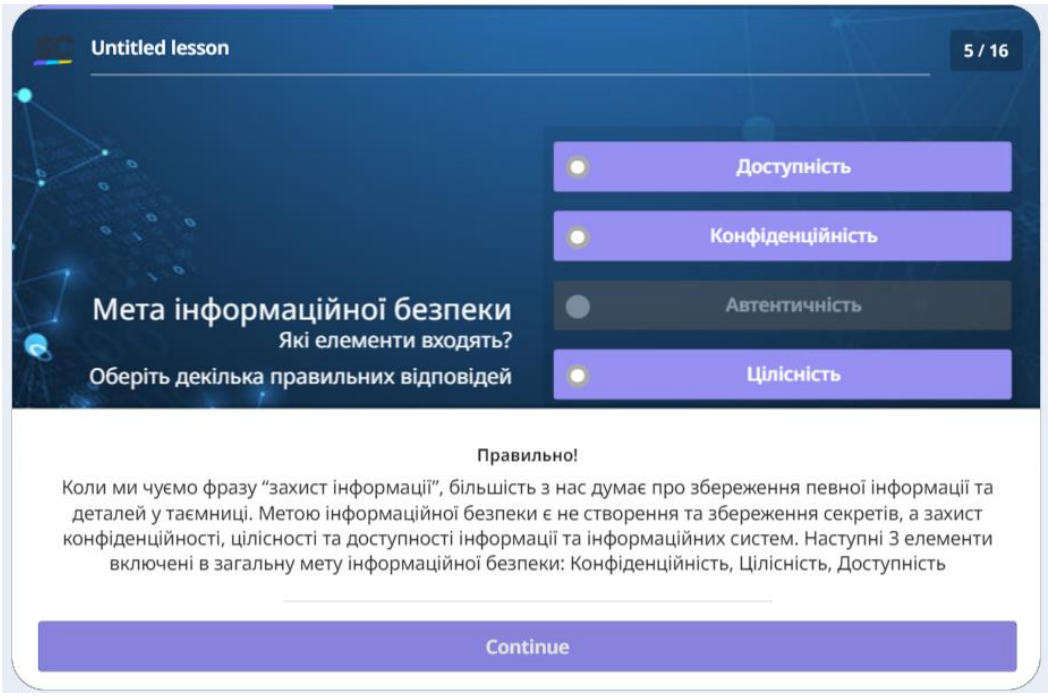
Нижче наведені скріншоти з додаткових матеріалів курсу підвищення обізнаності персоналу з інформаційної безпеки. Цей інтерактивний продукт містить як короткі тези, що підсумовують основну доповідь спікера курсу, так і тести, де слухачі можуть отримати додаткові бали за правильні відповіді, а по успішному завершенню навчальної програми, отримати визначені організаторами курсу бонуси.

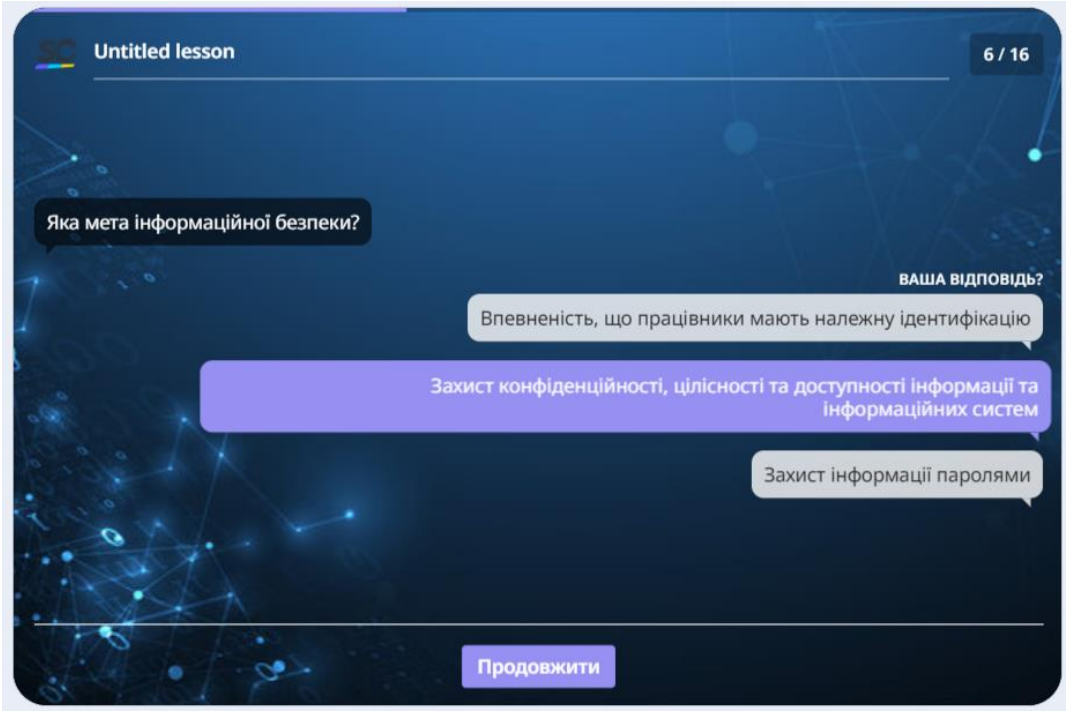


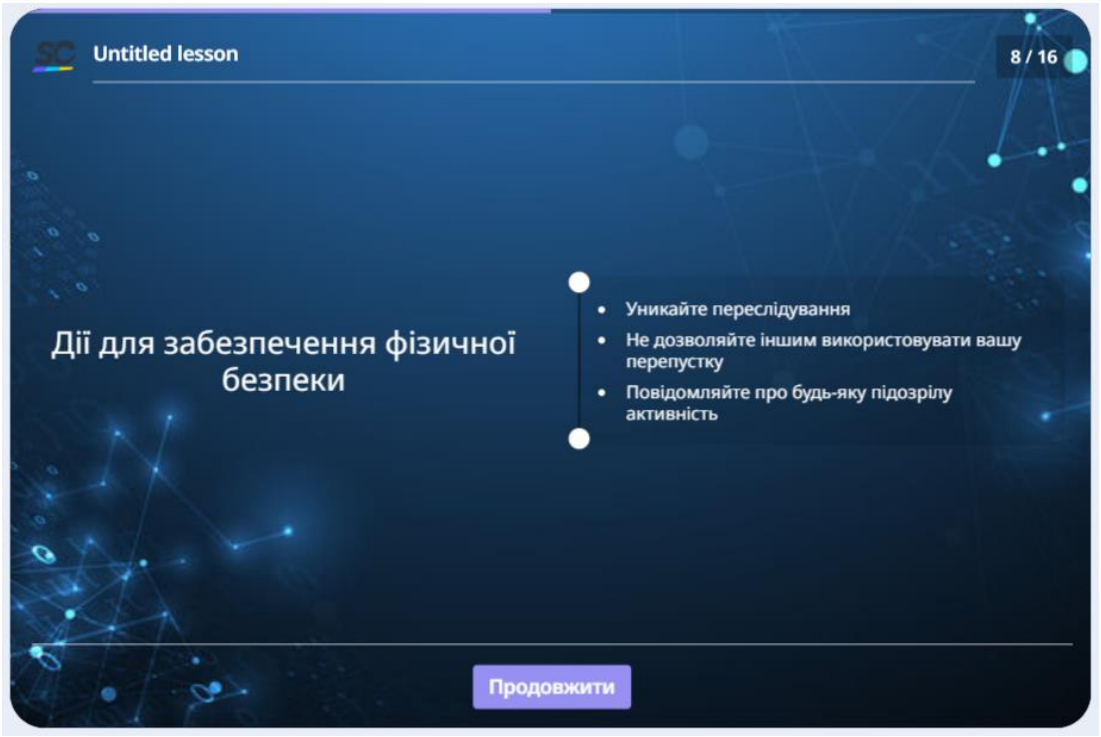


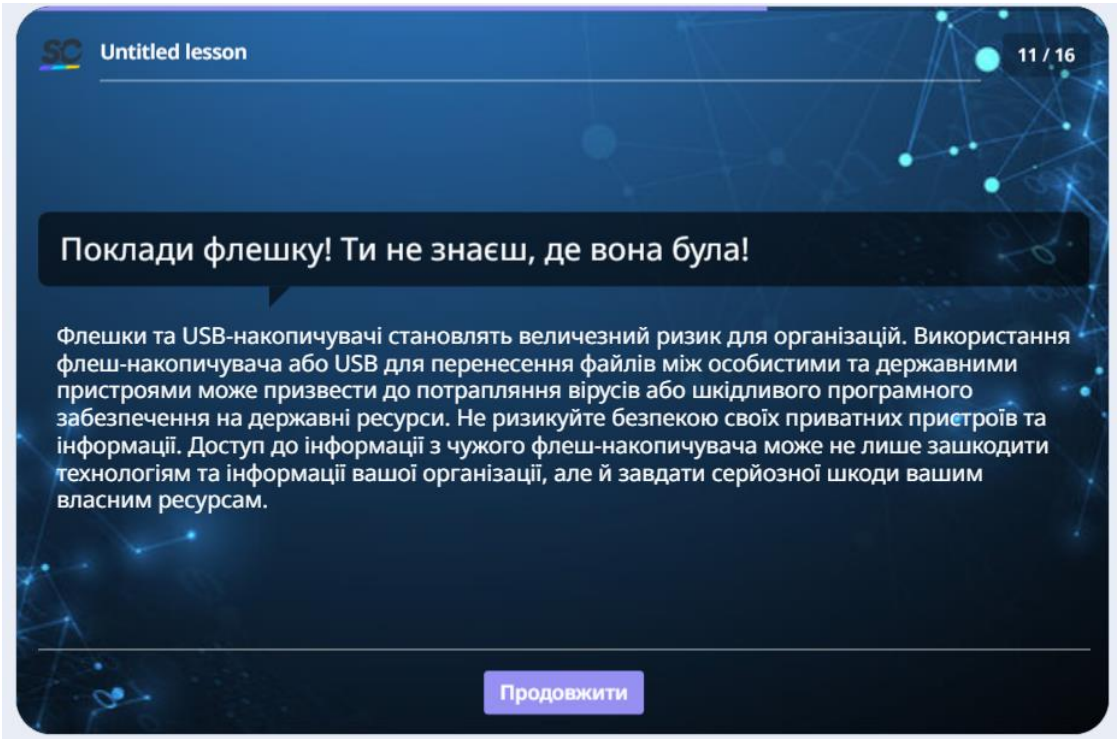

Untitled lesson
3 / 16
Які є форми інформації?
Виберіть декілька відповідей
Паперовий
Символьна
Усний
Електронний
Правильно!
У сучасному робочому середовищі багато інформаційних систем є електронними, але інформація (або дані) існує в різних форматах і повинна бути захищена. Нижче перераховані всі форми, в яких можуть поширюватися дані: Електронний, Паперовий, Усний
Continue

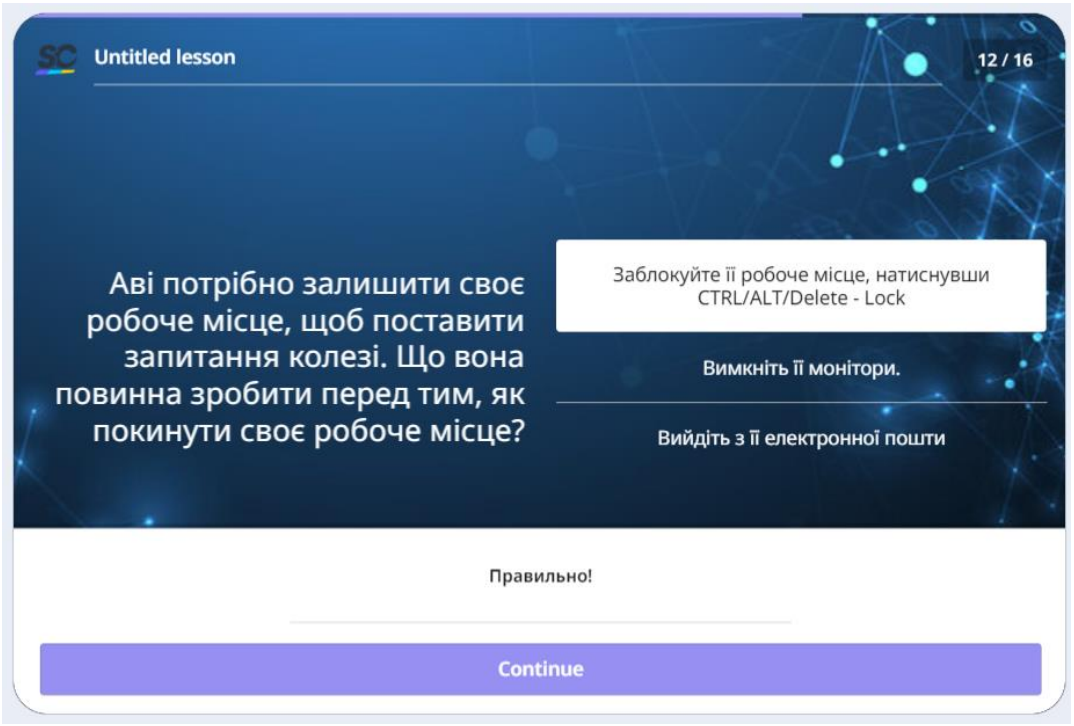

Untitled lesson
4 / 16
Кібербезпека
Продовжити

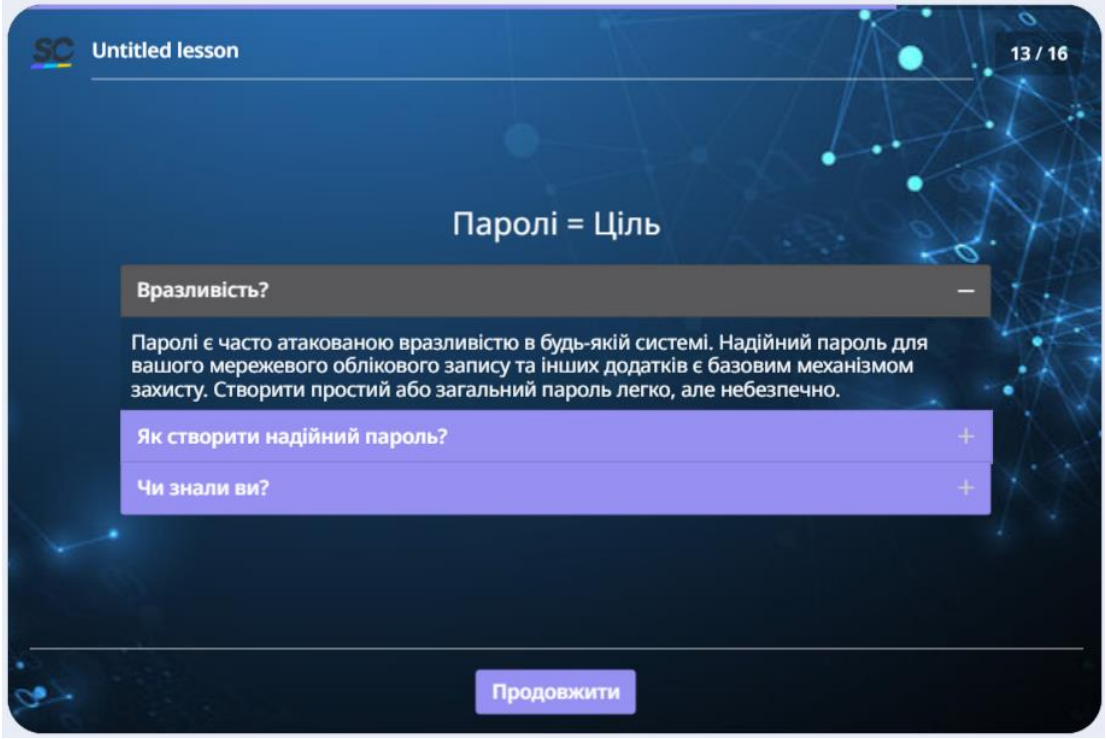

Untitled lesson
5 / 16
Доступність
Конфіденційність
Автентичність
Цілісність
Мета інформаційної безпеки
Які елементи входять?
Оберіть декілька правильних відповідей
Правильно!
Коли ми чуємо фразу "захист інформації", більшість з нас думає про збереження певної інформації та деталей у таємниці. Метою інформаційної безпеки є не створення та збереження секретів, а захист конфіденційності, цілісності та доступності інформації та інформаційних систем. Наступні 3 елементи включені в загальну мету інформаційної безпеки: Конфіденційність, Цілісність, Доступність
Continue

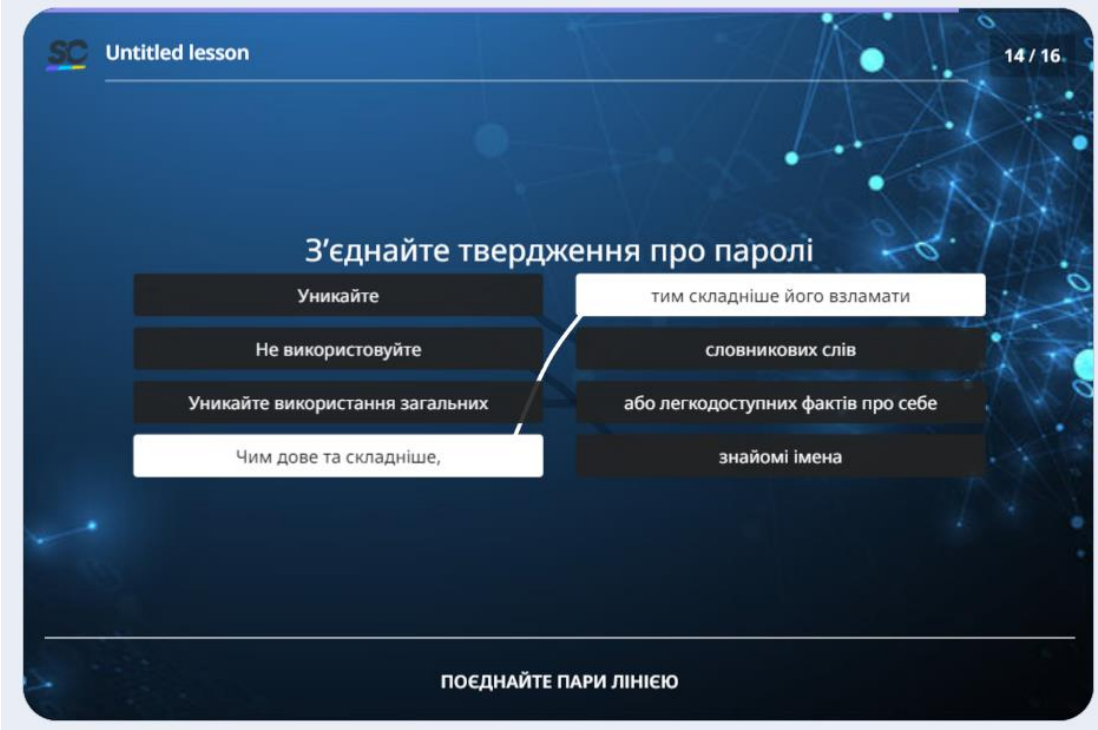

Untitled lesson
6 / 16
Яка мета інформаційної безпеки?
ВАША ВІДПОВІДЬ?
Впевненість, що працівники мають належну ідентифікацію
Захист конфіденційності, цілісності та доступності інформації та інформаційних систем
Захист інформації паролями
Продовжити

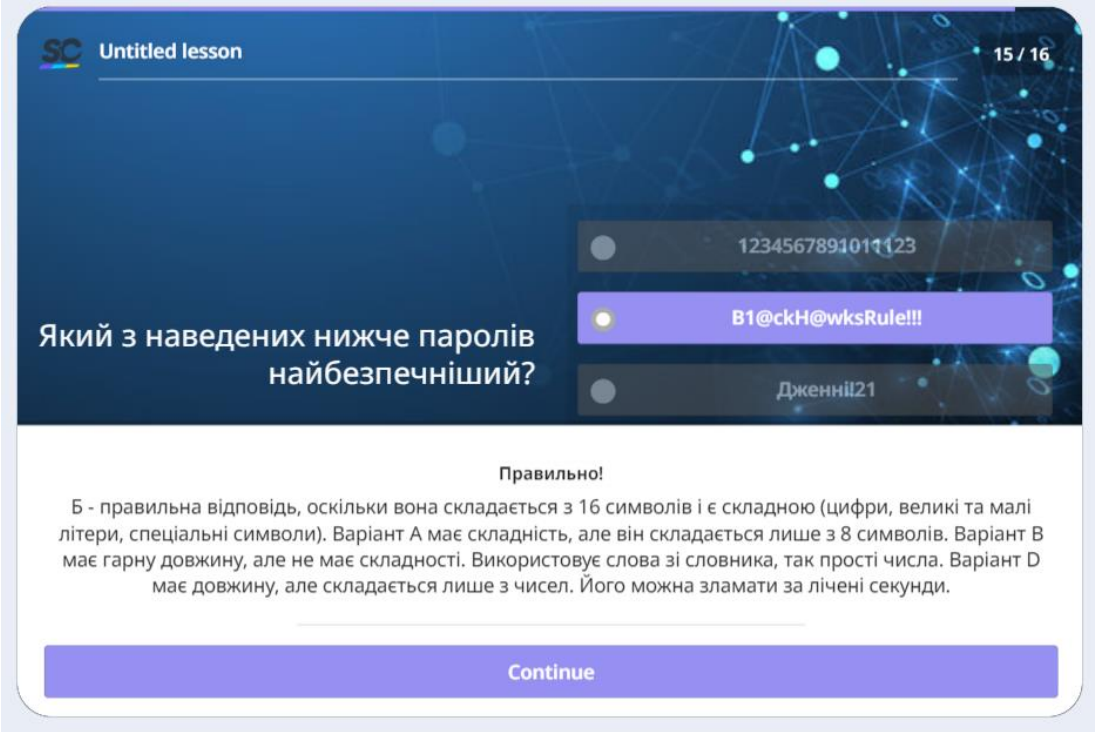

Untitled lesson
8 / 16
Дії для забезпечення фізичної безпеки
Уникайте переслідування
Не дозволяйте іншим використовувати вашу перепустку
Повідомляйте про будь-яку підозрілу активність
Продовжити


Untitled lesson
11 / 16
Поклади флешку! Ти не знаєш, де вона була!
Флешки та USB-накопичувачі становлять величезний ризик для організацій. Використання флеш-накопичувача або USB для перенесення файлів між особистими та державними пристроями може призвести до потрапляння вірусів або шкідливого програмного забезпечення на державні ресурси. Не ризикуйте безпекою своїх приватних пристроїв та інформації. Доступ до інформації з чужого флеш-накопичувача може не лише зашкодити технологіям та інформації вашої організації, але й завдати серйозної шкоди вашим власним ресурсам.
Продовжити


Untitled lesson
12 / 16
Аві потрібно залишити своє робоче місце, щоб поставити запитання колезі. Що вона повинна зробити перед тим, як покинути своє робоче місце?
Заблокуйте її робоче місце, натиснувши CTRL/ALT/Delete - Lock
Вимкніть її монітори.
Вийдіть з її електронної пошти
Правильно!
Continue


Untitled lesson
13 / 16
Паролі = Ціль
Вразливість?
Паролі є часто атакованою вразливістю в будь-якій системі. Надійний пароль для вашого мережевого облікового запису та інших додатків є базовим механізмом захисту. Створити простий або загальний пароль легко, але небезпечно.
Як створити надійний пароль?
Чи знали ви?
Продовжити


Untitled lesson
14 / 16
З'єднайте твердження про паролі
Уникайте
Не використовуйте
Уникайте використання загальних
Чим дове та складніше,
тим складніше його взламати
словникових слів
або легкодоступних фактів про себе
знайомі імена
ПОЄДНАЙТЕ ПАРИ ЛІНІЄЮ


Untitled lesson
15 / 16
Який з наведених нижче паролів найбезпечніший?
1234567891011123
B1@ckH@wksRule!!!
Дженні21
Правильно!
Б - правильна відповідь, оскільки вона складається з 16 символів і є складною (цифри, великі та малі літери, спеціальні символи). Варіант А має складність, але він складається лише з 8 символів. Варіант В має гарну довжину, але не має складності. Використовує слова зі словника, так прості числа. Варіант D має довжину, але складається лише з чисел. Його можна зламати за лічені секунди.
Continue