

ПРОЄКТ

"Проведення спеціалізованого тренінго-навчального курсу "Основи Кібергігієни" для 20 000 працівників енергетичної галузі України, як частини критичної інфраструктури»

В рамках підтримки Плану заходів з реалізації «Концепції кібербезпеки
енергетичної галузі України»

(Проект реалізується за підтримки Посольства США в Україні та Міністерства
Закордонних справ Естонії)



REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

ECSI
European Cyber Security Initiative

a.
cyber.academy

ISSP

CYBEXER TECHNOLOGIES

Проект реалізується в рамках прогарми «Development Cooperation Partnership (DCP), Round 8» в рамках якого є можливість підвищити рівень базових навичок та знань з кібербезпеки для 20.000 співробітників з 15 обраних компаній з українського енергетичного сектору шляхом проведення спеціалізованого онлайн курсу **навчання з використанням інтерактивної платформи кібергігієни.**

Реалізація проекту: **жовтень 2021 року - грудень 2022 року**, з залученням провідних експертів, та використанням естонської навчальної платформи з кібергігієни “CybExer”.

Проект буде проводитись онлайн без відриву персоналу енергокомпаній від основної роботи, **безкоштовно для зареєстрованих учасників.**

Проект включено до Плану Заходів галузезої Концепції з кібербезпеки енергетичної галузі 2021-2024.

Виклики КГ

Мотивація

КГ подібна до основ безпеки життєдіяльності, ніхто не має мотивації вивчати КГ: вона не приносить доданої вартості на ринкову вартість навичок працівників. Необов'язкове навчання ніколи не матиме успіху.

Важливість

Відсутність досвіду в галузі кібербезпеки для нетехнічних працівників заважає зрозуміти, до яких обставин може призвести неправильна поведінка в кіберзахисті.

Співробітник

CISO/CIO

У CISO немає дієвих інструментів для оцінки готовності працівників до визначення та пом'якшення фактичного рівня ризику. Навіть якщо працівник вивчає основи КГ, немає інструменту, щоб зрозуміти його ефективність.

Ризики КГ незмірні

ІТ-відділ не має технічного рішення для ризикованої поведінки співробітників. Звичайний брандмауер та IPS не врятують від усіх випадкових натискань та фішингових кампаній.

Жоден інструмент не може замінити "людський брандмауер"

Постановка проблеми

КГ = Кібер Гігієна

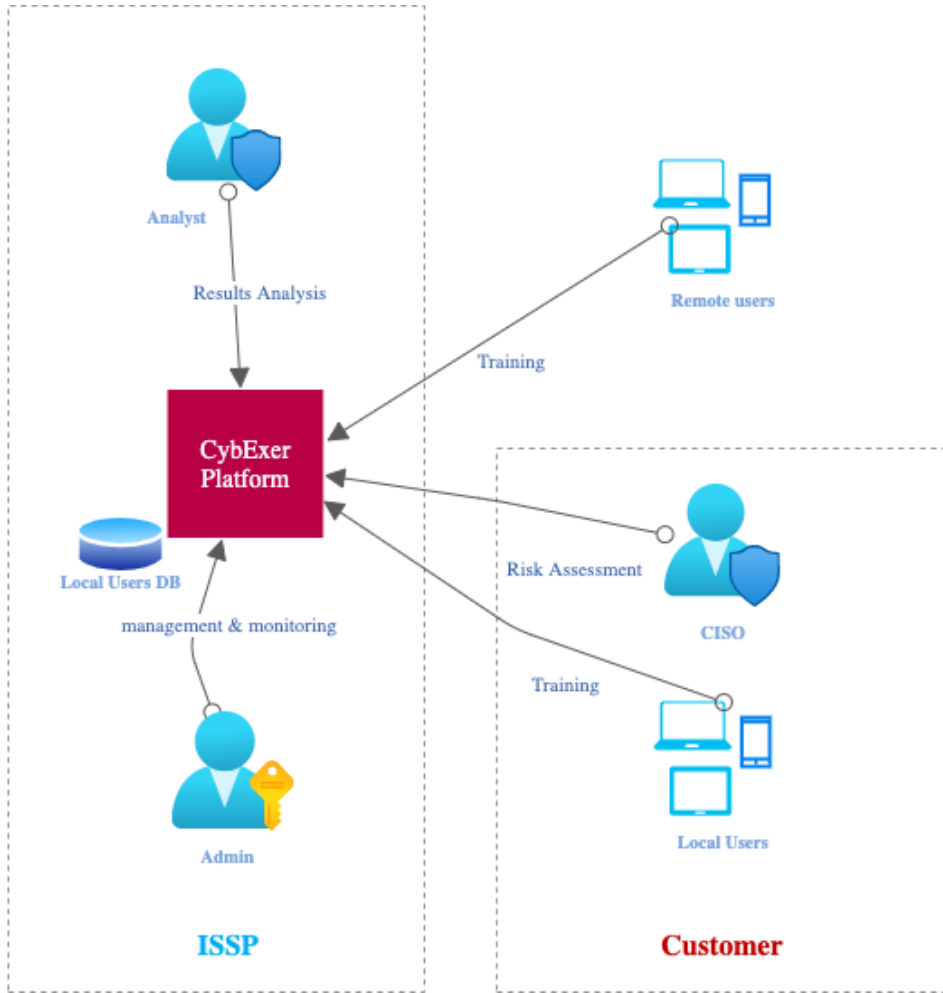


В Україні є платформи і проекти з КГ. Більшість з них відмінно викладають, але майже усі з них не дають зворотнього зв'язку про те, наскільки безпечнішою стала організація. Розуміння ризику КГ, що залишається на співробітнику і на організації є життєво важливою для вимірювання ефективності програми КГ в цілому і перетворення результатів програми в дієвий інструмент для ІТ і відділів щодо управління ризиками.

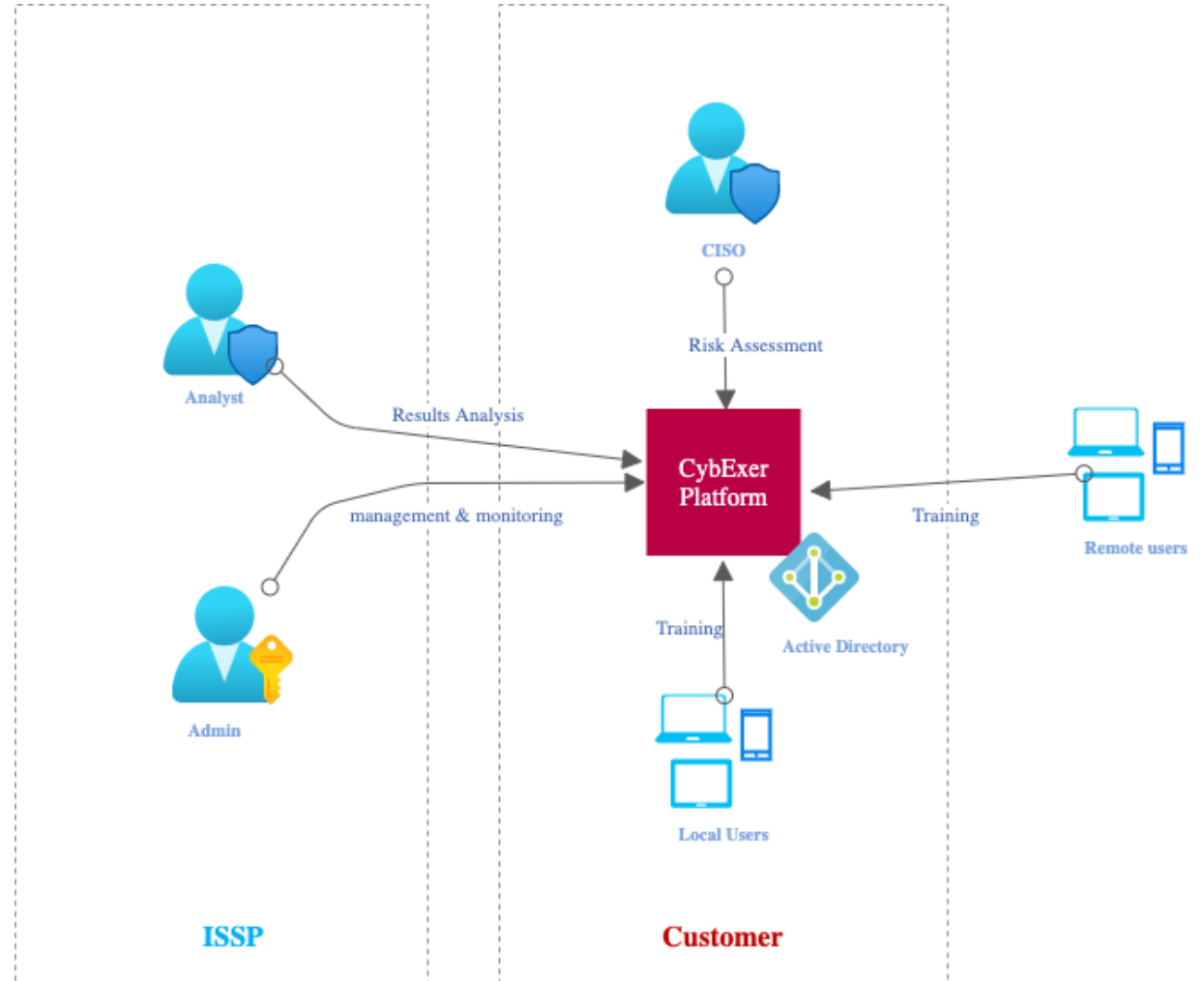
Концепція платформи Cybexer

- Не використовується підхід «пройшов або не пройшов тест»: навіть 90% отриманих балів можуть означати потенційний ризик.
- Ефективність використання часу: дозволяє учням швидко та у зручний час отримувати знання
- Зворотній зв'язок: необхідно навчати викладачів, часто ігнорується аспект тренінгів з підвищення обізнаності викладачів
- «Підхід брандмауера»: визнання впливу проблеми на поведінку людини
- Створення «матриці ризиків»: міцна концептуальна основа у співпраці з академічною спільнотою
- Персональний підхід: готовність коригувати навчальний матеріал відповідно до специфічних потреб і політики організації.
- Спільнота: постійні зусилля для поліпшення навчальної платформи

Варіанти архітектури рішення



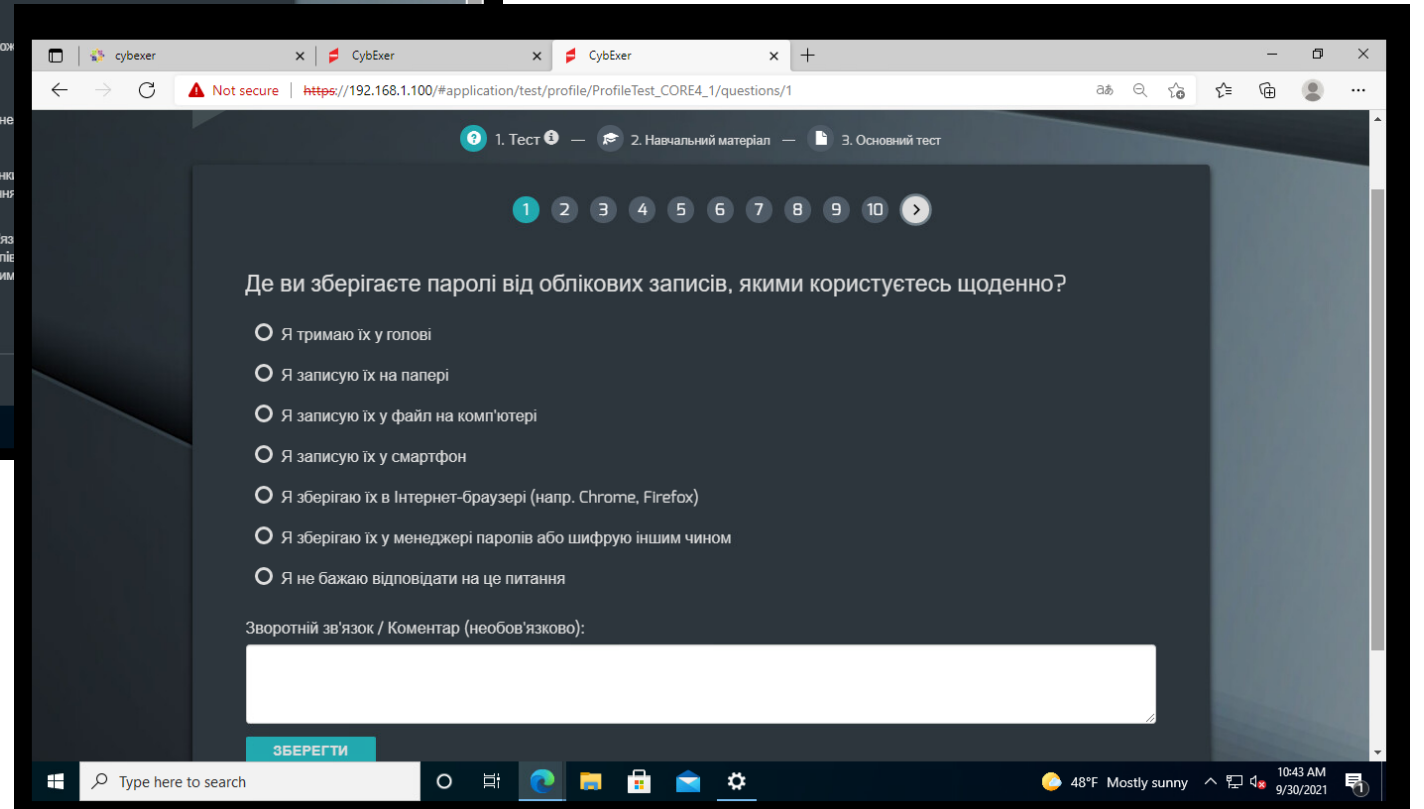
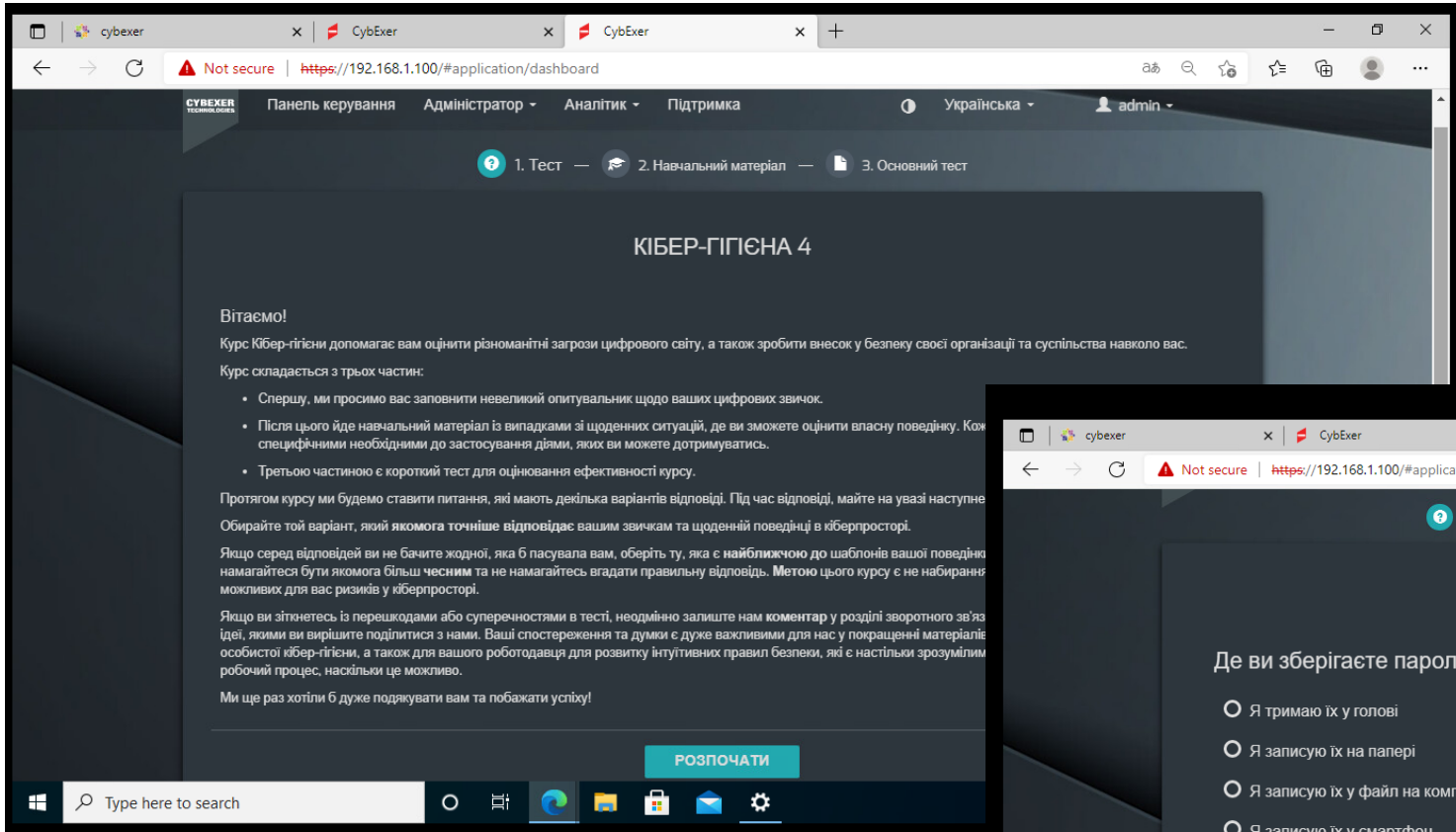
or



План проекту



Скріншоти з курсу



Скріншоти з курсу

The screenshot shows a web browser window with the URL https://192.168.1.100/#application/test/profile/ProfileTest_CORE4_1/questions/10. The page displays a quiz question: "Як би ви оцінили IT-підтримку вашої організації?". Below the question are five radio button options, each associated with a risk level: "Дуже дружня та корисна" (Low risk), "Дещо корисна" (Low-Medium risk), "Швидко реагує, але часто дає незрозумілі або складні відповіді" (Medium risk), "Швидко реагує, але відповіді поверхневі" (High risk), and "Повільна, але ефективна" (Very High risk). The first option is selected. A progress bar at the top shows 10 questions, with the 10th question being the current one.

1. Тест — 2. Навчальний матеріал — 3. Основний тест

1 2 3 4 5 6 7 8 9 10

Як би ви оцінили IT-підтримку вашої організації?

НИЗЬКИЙ РІВЕНЬ РИЗИКУ ПОМІРНИЙ РІВЕНЬ РИЗИКУ РИЗИКОВИЙ ВИСОКИЙ РІВЕНЬ РИЗИКУ

- Дуже дружня та корисна
- Дещо корисна
- Швидко реагує, але часто дає незрозумілі або складні відповіді
- Швидко реагує, але відповіді поверхневі
- Повільна, але ефективна
- Повільна, здебільшого неефективна
- Я не знаю, бо мені ніколи не доводилось користуватись допомогою відділу IT
- Я не бажаю відповідати на це питання

Зворотній зв'язок / Коментар (необов'язково):

The screenshot shows a web browser window with the URL https://192.168.1.100/#application/test/study/StudyMaterial_CORE4_1/questions/1. A modal window titled "Навчальний матеріал" is open, displaying text about the course and a legend for risk levels. The text explains that the course is based on real-life scenarios and aims to help users understand their own risk levels in a cyber environment. It lists five risk levels with corresponding colors: Green (Low), Yellow (Low-Medium), Orange (Medium), Red (High), and Black (Very High). A "ПОЧАТИ" button is visible at the bottom of the modal.

Навчальний матеріал

Ви перейшли у другу частину курсу. Курс базується на випадках та ситуаціях з щоденного життя. Після випадків буде йти запитання, яке звертається до вашого досвіду. Також ми додали невелику кількість навчального матеріалу.

Під час відповіді на запитання, будь ласка, оберіть ту відповідь, яка найбільш точно описує ваші звички та типову поведінку в кібер-просторі. Якщо жодна з відповідей вам не підходить, оберіть ту відповідь, яка є найближчою до вашої типової поведінки. Намагайтесь бути якомога чеснішим та не намагайтесь вгадати найменш ризикову відповідь, тому що метою курсу є відображення ваших можливих ризиків у кібер-просторі, а не набирання балів.

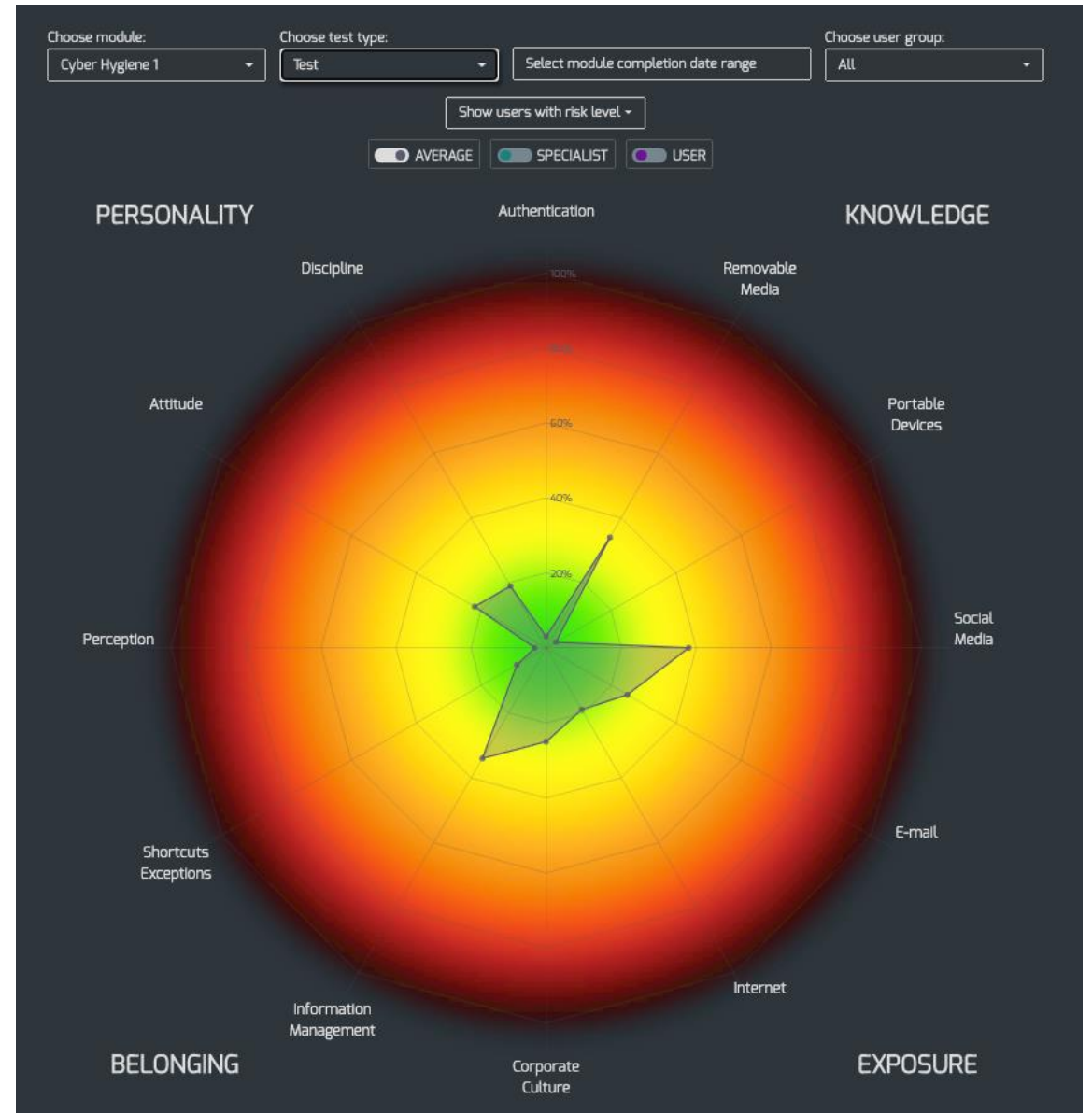
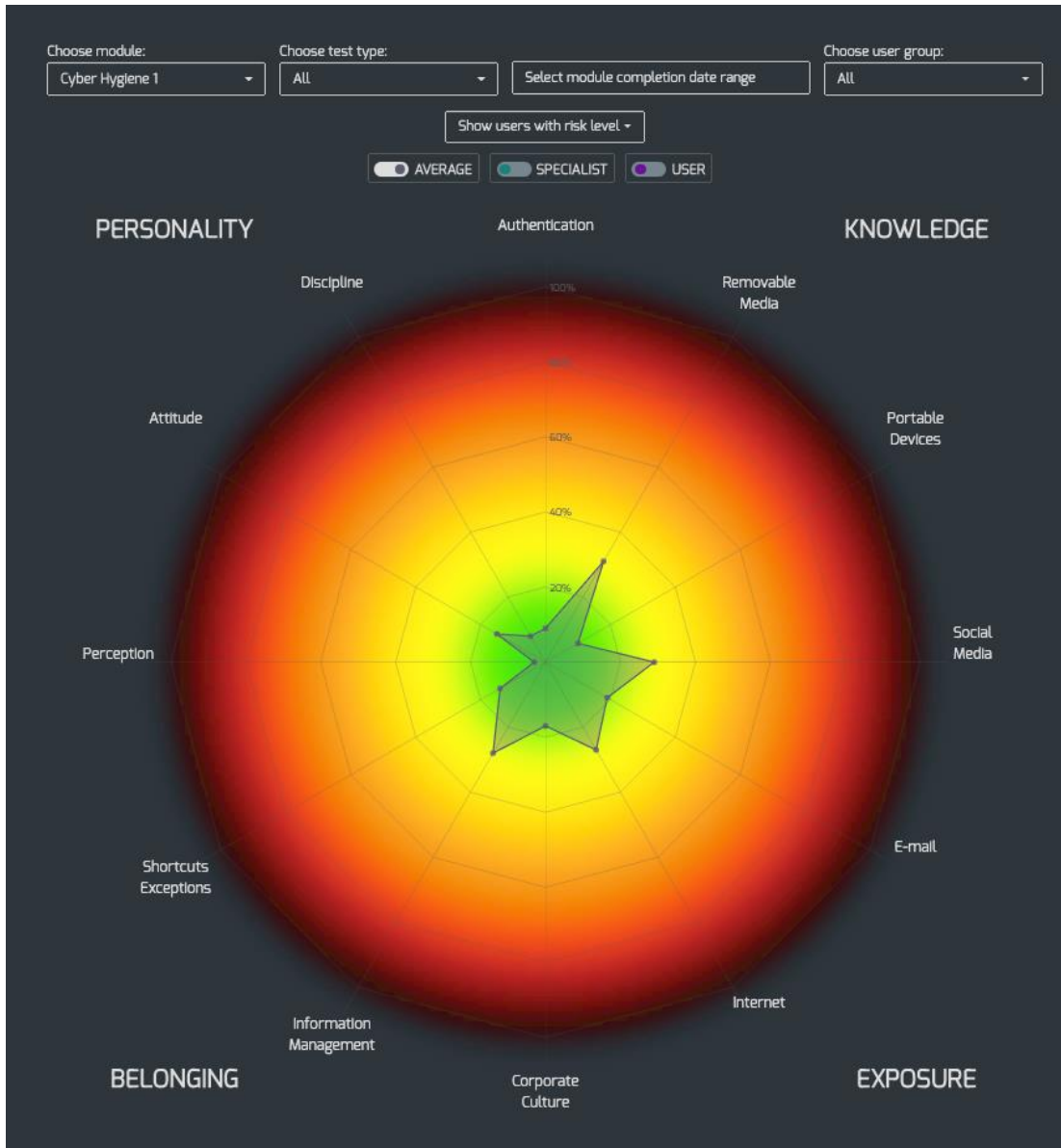
Після того, як ви обрали відповідь на запитання, ви отримаєте автоматичний зворотній зв'язок за наступним принципом:

- Зелений колір означає, що ваша поведінка має низький рівень ризику
- Жовтий колір означає, що ваша поведінка має середній рівень ризику
- Помаранчевий колір означає, що ваша поведінка є ризиковою
- Червоний колір означає, що ваша поведінка має високий рівень ризику
- Чорний колір означає, що ваша поведінка має дуже високий рівень ризику

Після надання відповіді вас буде спрямовано на навчальний матеріал. Навчальний матеріал пояснить більш детально, що є найменш ризиковою поведінкою в даній ситуації, про що йдеться у випадку та які конкретні дії ви можете взяти з прикладу.

Ваші коментарі та зворотній зв'язок є важливими, адже допомагають покращити курс. Будь ласка, використовуйте цей матеріал. Ми завжди вдячні за ваші коментарі та зворотній зв'язок.

ПОЧАТИ



ПРИКЛАДИ АНАЛІТИЧНИХ ЗВІТІВ

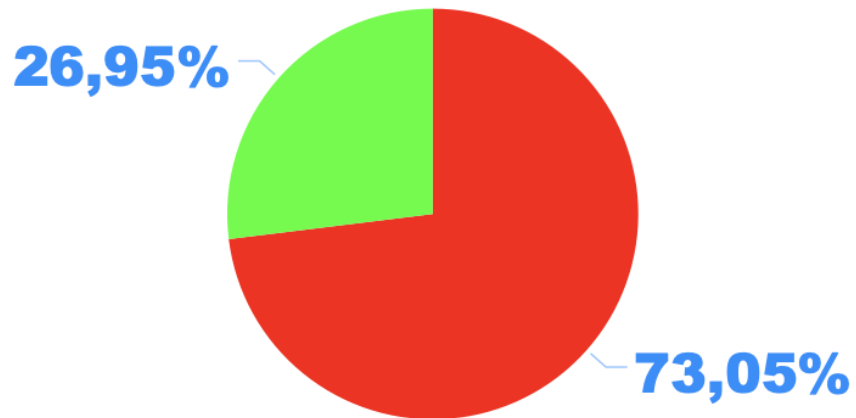
M-1

679

К-ть учасників

	К-ть проблемних питань на ОДНУ особу	К-ть осіб	%
Від 18 до 27		20	2,95%
Від 9 до 17		231	34,02%
До 9		245	36,08%
Немає проблем		183	26,95%
Усього		679	100,00%

Наявність проблематичного питання



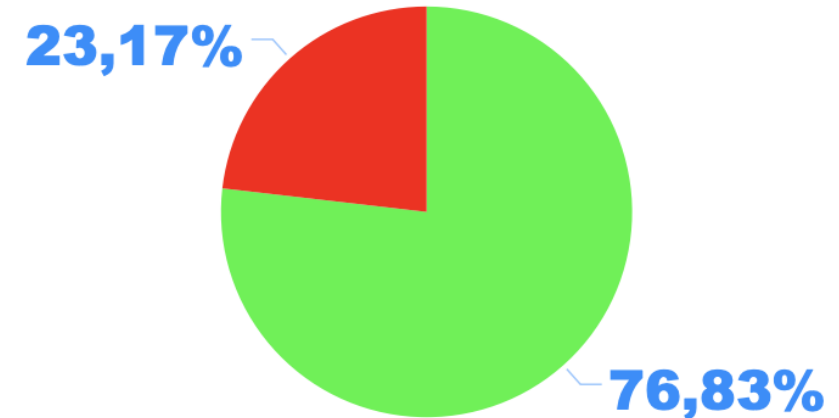
M-2

505

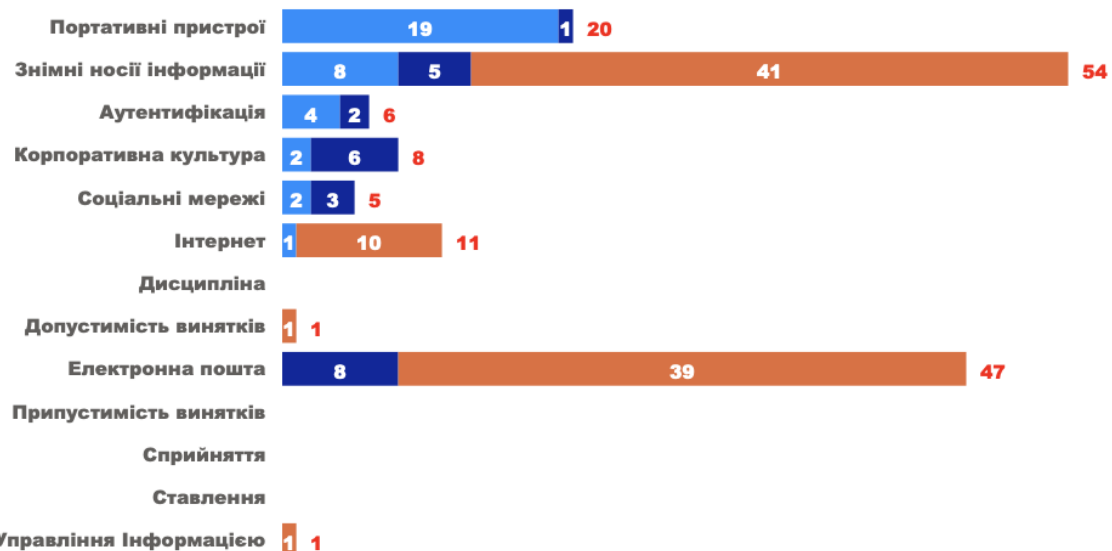
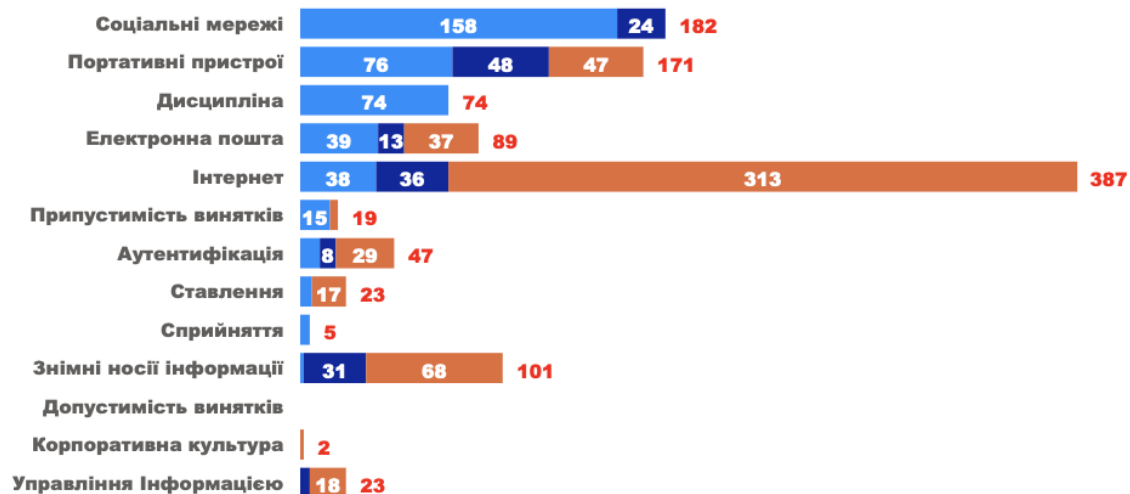
К-ть учасників

	К-ть проблемних питань на ОДНУ особу	К-ть осіб	%
Від 9 до 17		28	0,49%
До 9		89	4,97%
Немає проблем		388	94,53%
Усього		505	100,00%

Наявність проблематичного питання



● QUIZ ● STUDY ● EXAM



M-1

679

К-ть учасників

К-ть ризиків на ОДНУ особу	%	К-ть
Від 1 до 3	61,71%	419
Від 4 до 7	9,43%	64
Від 8 і більше	1,91%	13
Немає	26,95%	183
Усього	100,00%	679

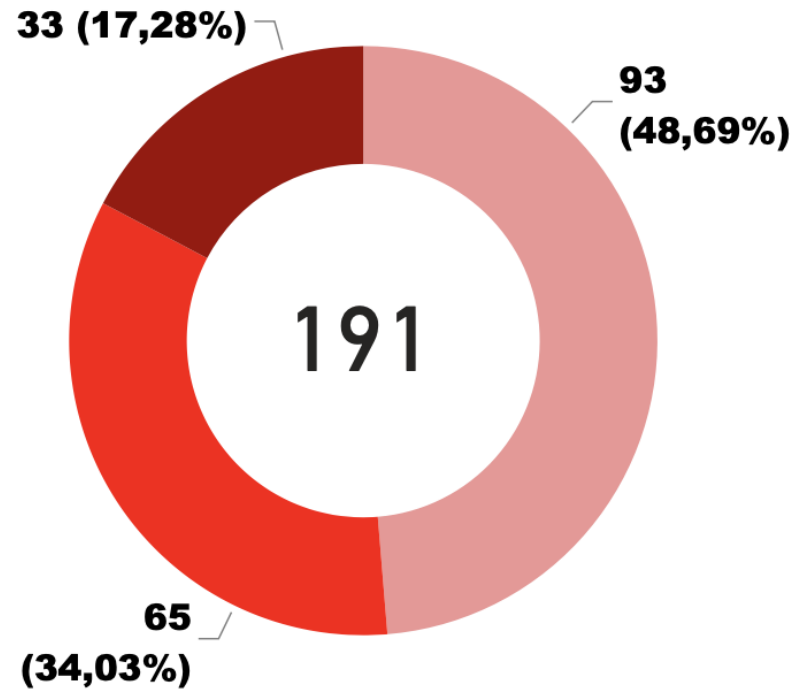
M-2

505

К-ть учасників

К-ть ризиків на ОДНУ особу	%	К-ть
Від 1 до 3	22,38%	113
Від 4 до 7	0,79%	4
Немає	76,83%	388
Усього	100,00%	505

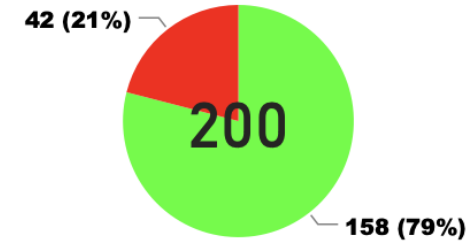
Кількість осіб щодо яких успішно проведено фішингову атаку



Категорія

- 1 - атака(и)
- 2 - атака(и)
- 3 - атака(и)

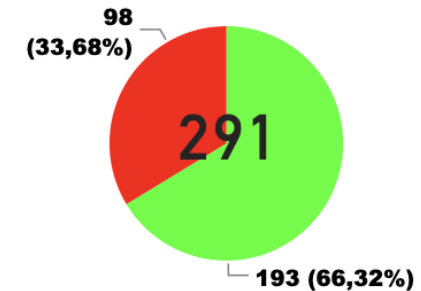
Атака № 1



Успішна атака?

- Ні
- Так

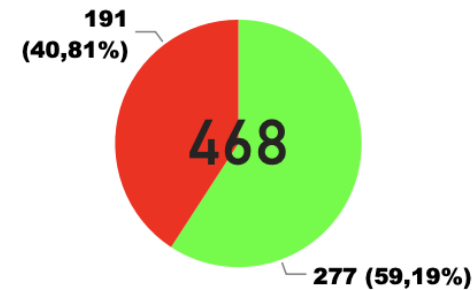
Атака № 2



Успішна атака?

- Ні
- Так

Атака № 3



Успішна атака?

- Ні
- Так

! Для реєстрації у Проєкті (отримання безкоштовних ліцензій для проведення навчання та тестування персоналу) необхідно подати дані про компанію-учасника, контактну особу відповідальну за комунікацію щодо проєкту, та вказати орієнтовну кількість необхідних ліцензій для доступу персоналу до навчальної Платформи (1 ліцензія на 1 співробітника)

КОНТАКТ ДЛЯ ПОДАННЯ ІНФОМАЦІЇ ДЛЯ РЕЄСТРАЦІЇ У ПРОЄКТІ :
cyberhygiene_energo@cyber.academy



REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

ECSI
European Cyber Security Initiative

a.
cyber.academy

ISSP

