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»

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

UNITED STATES OF AMERICA EMBASSY

REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

ECSI
European Cyber Security Initiative

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 енергокомппаній 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.

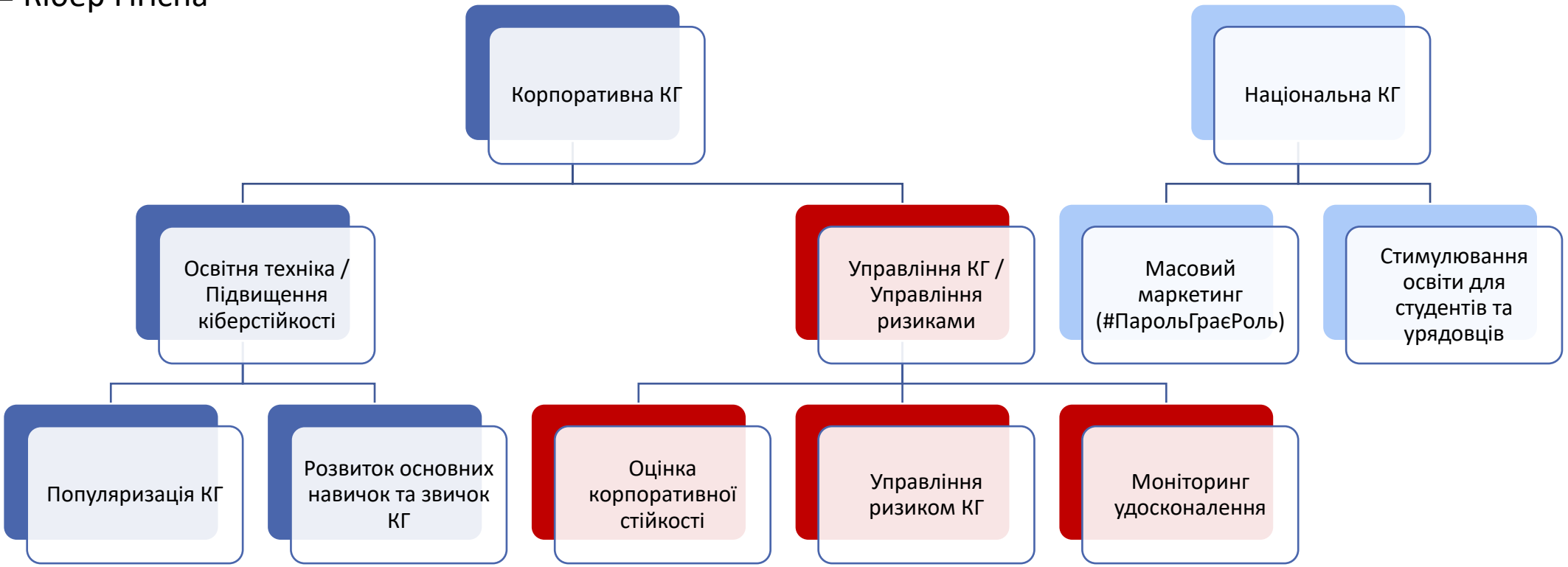
Ризики КГ незмірні

IT -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

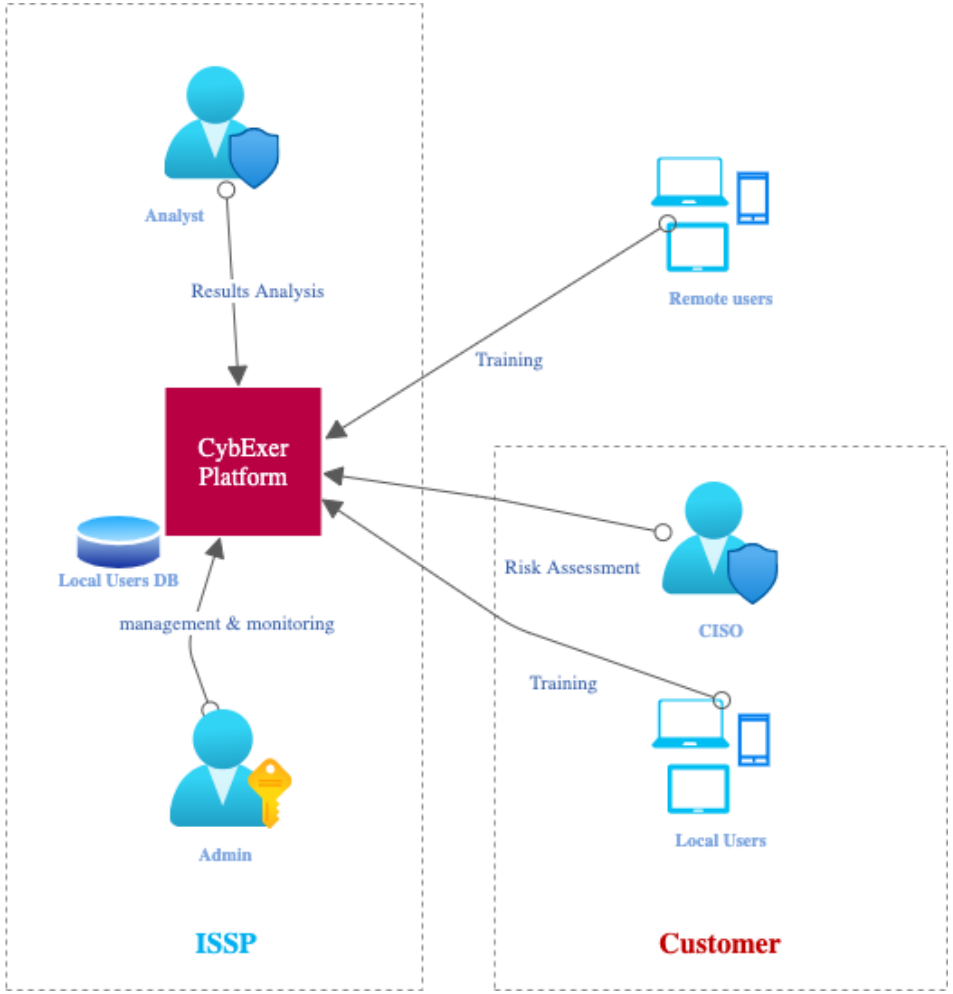


В Україні є платформи і проекти з КГ. Більшість з них відмінно викладають, але майже усі з них не дають зворотнього зв’язку про те, наскільки безпечнішою стала організація . Розуміння ризику КГ, що залишається на співробітнику і на організації є життєво важливою для вимірювання ефективності програми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

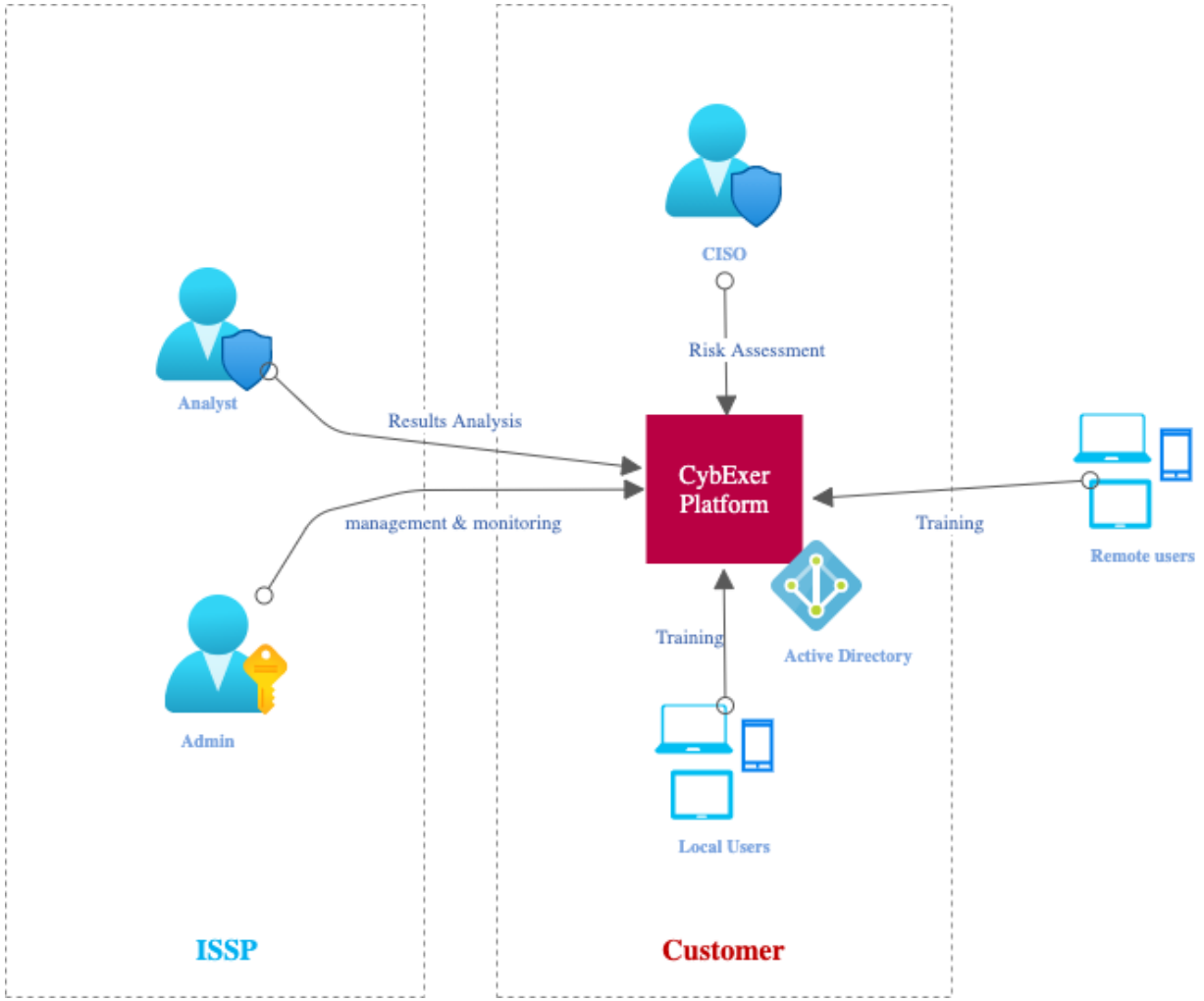
Концепція платформи Cybexer

- 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 навчаьний матеріал відповідно до специфічних потреб і політики організації.
- Спільнота: постійні зусилля для поліпшеня навчальної платформи

Варіанти архітектури рішення

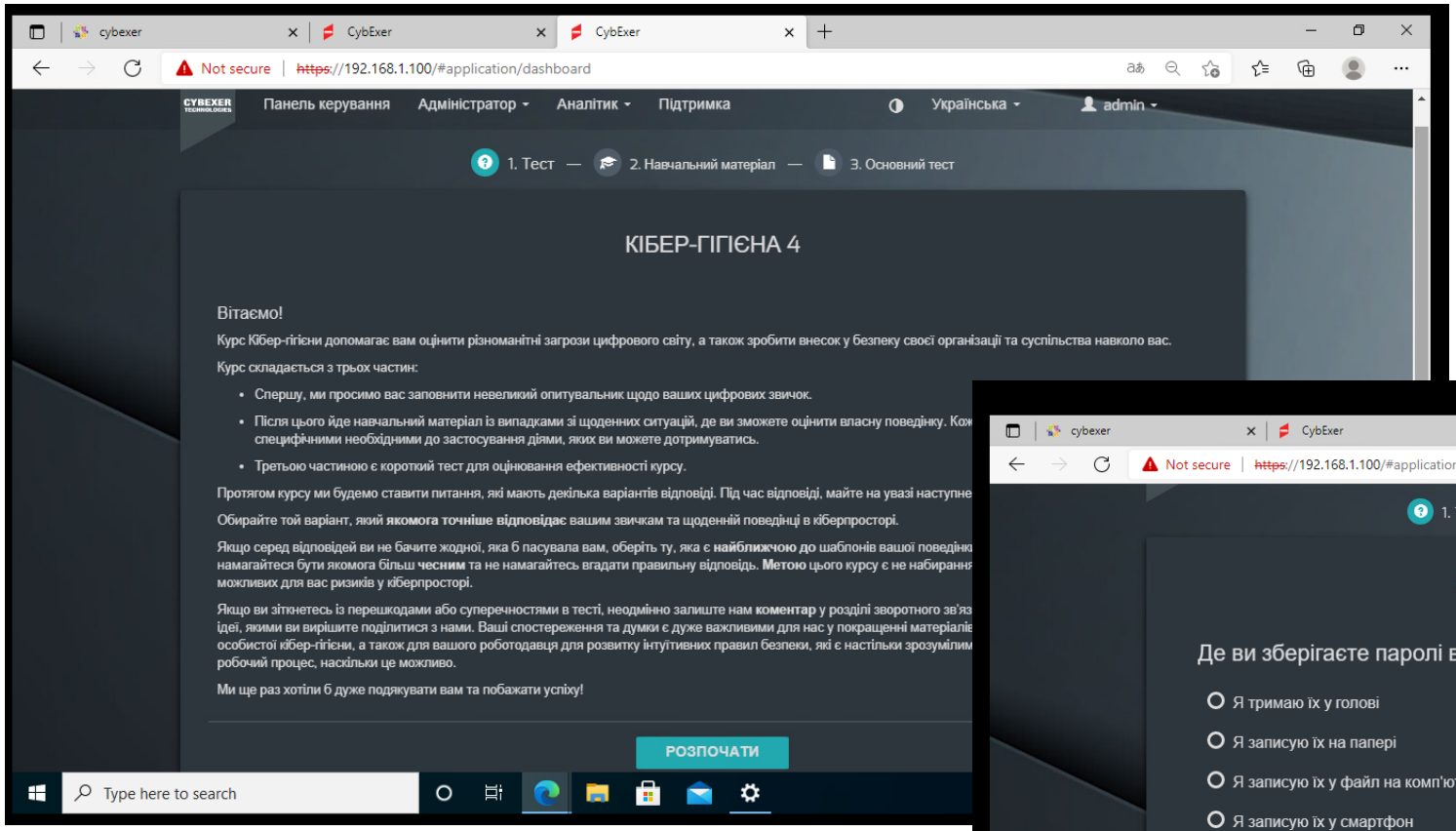


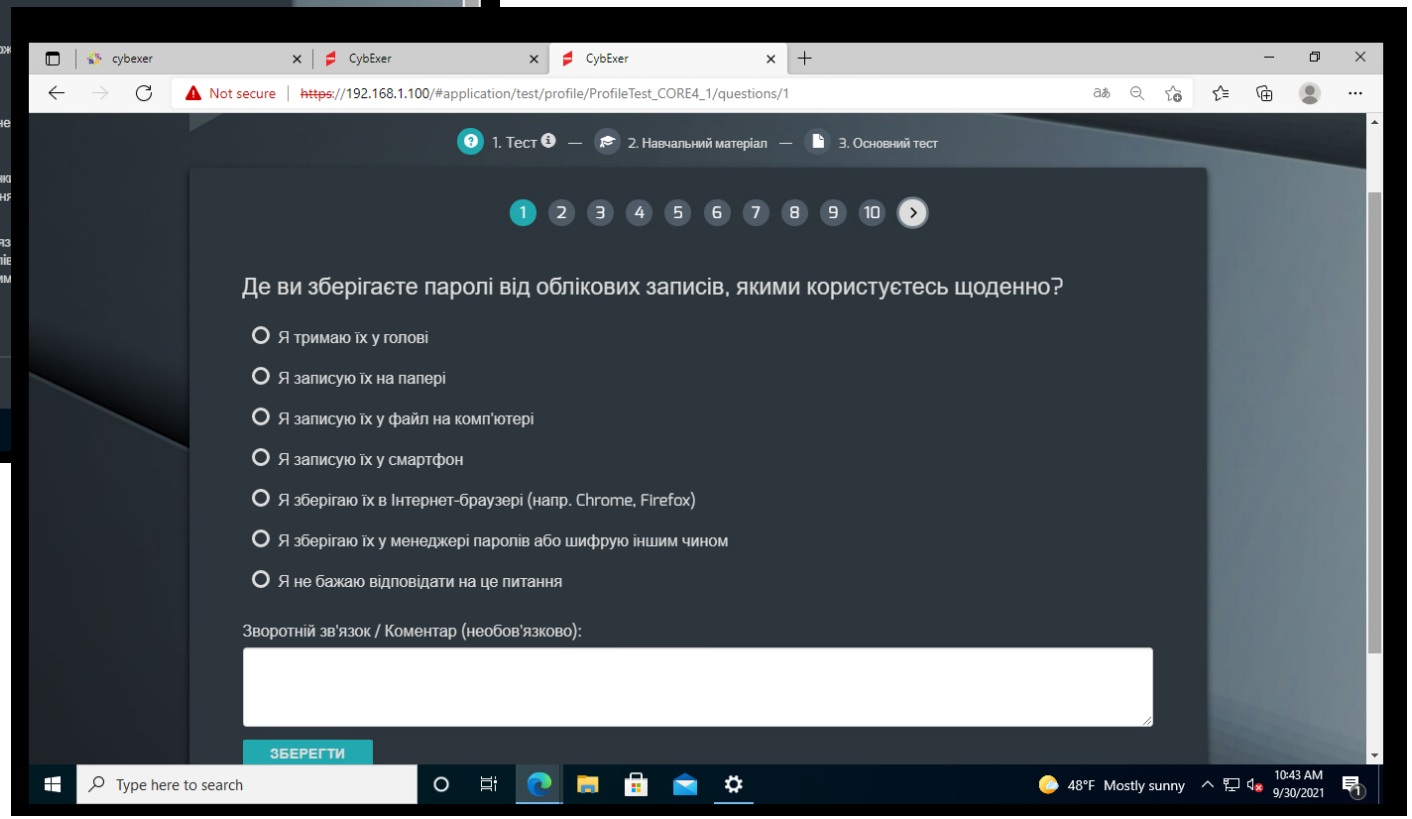
or



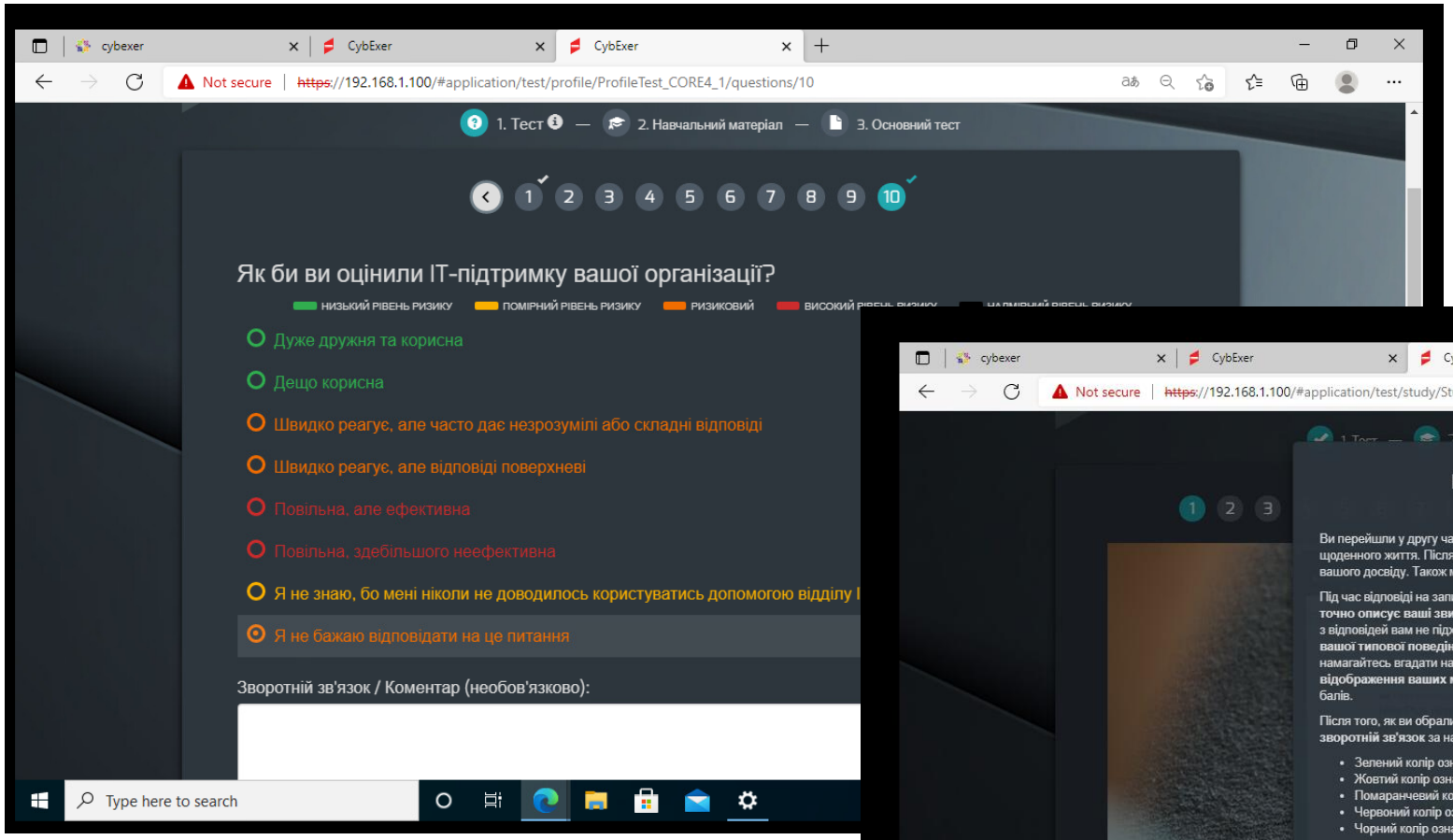
План проекту

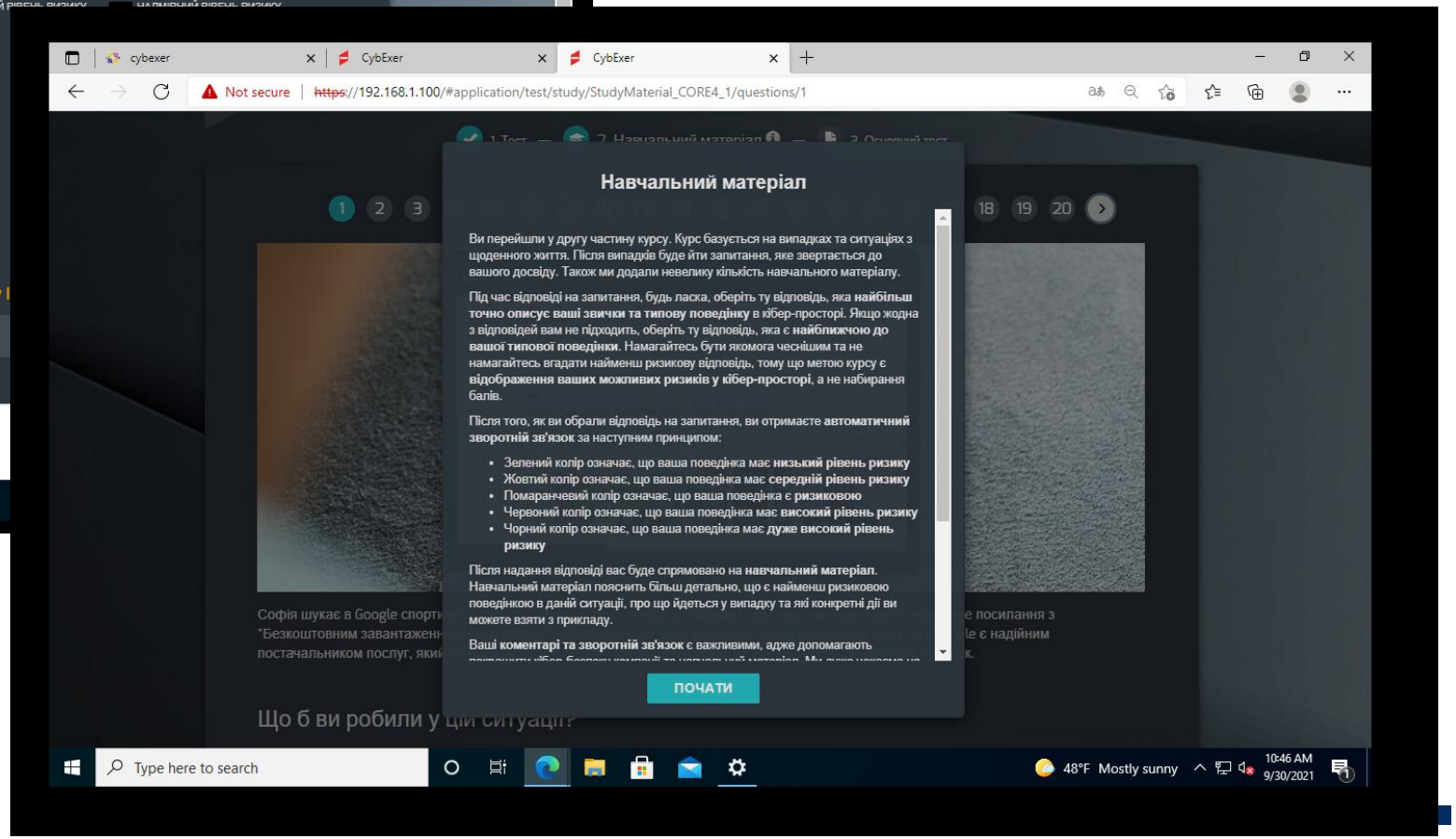
Скріншоти з курсу



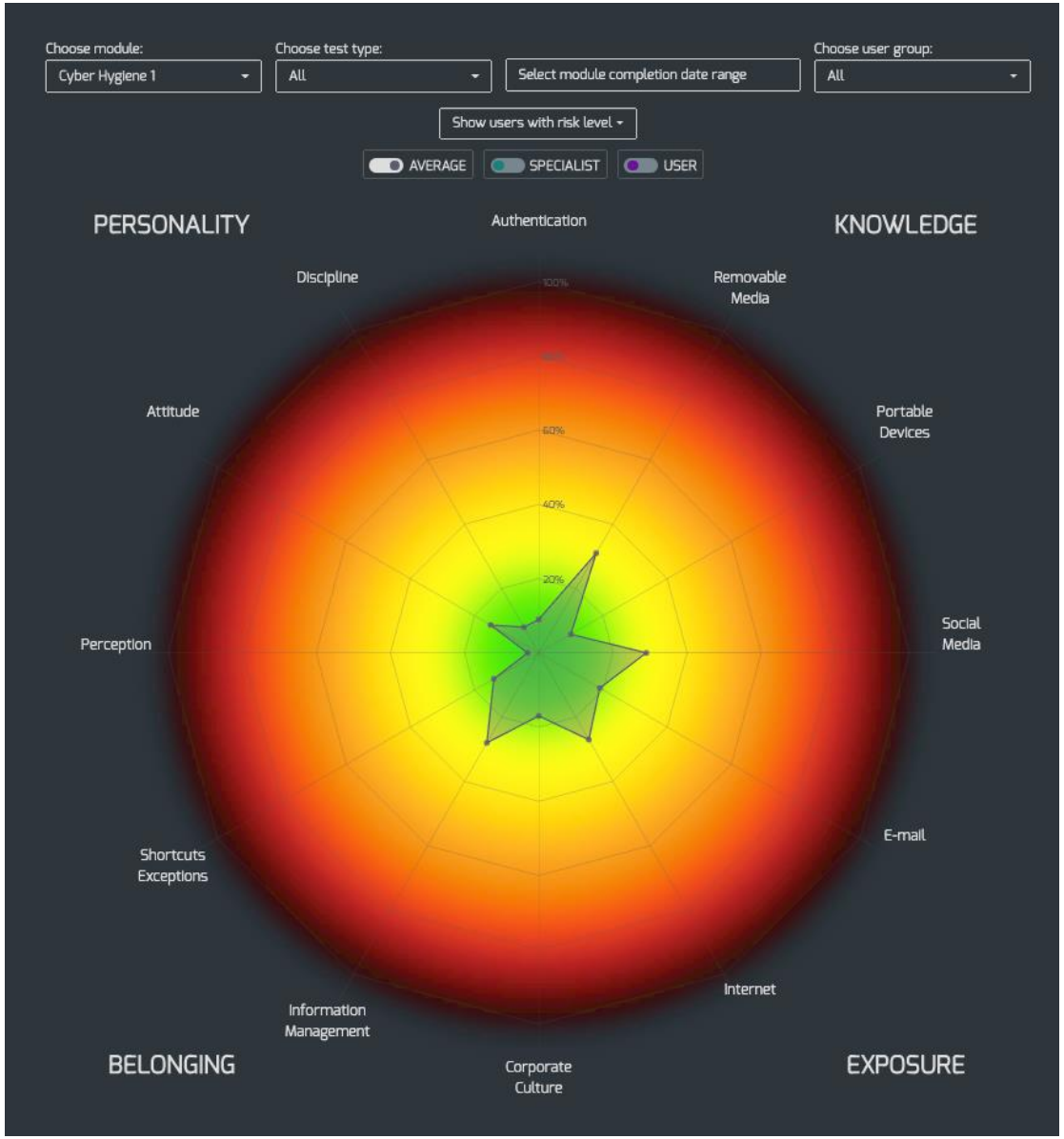


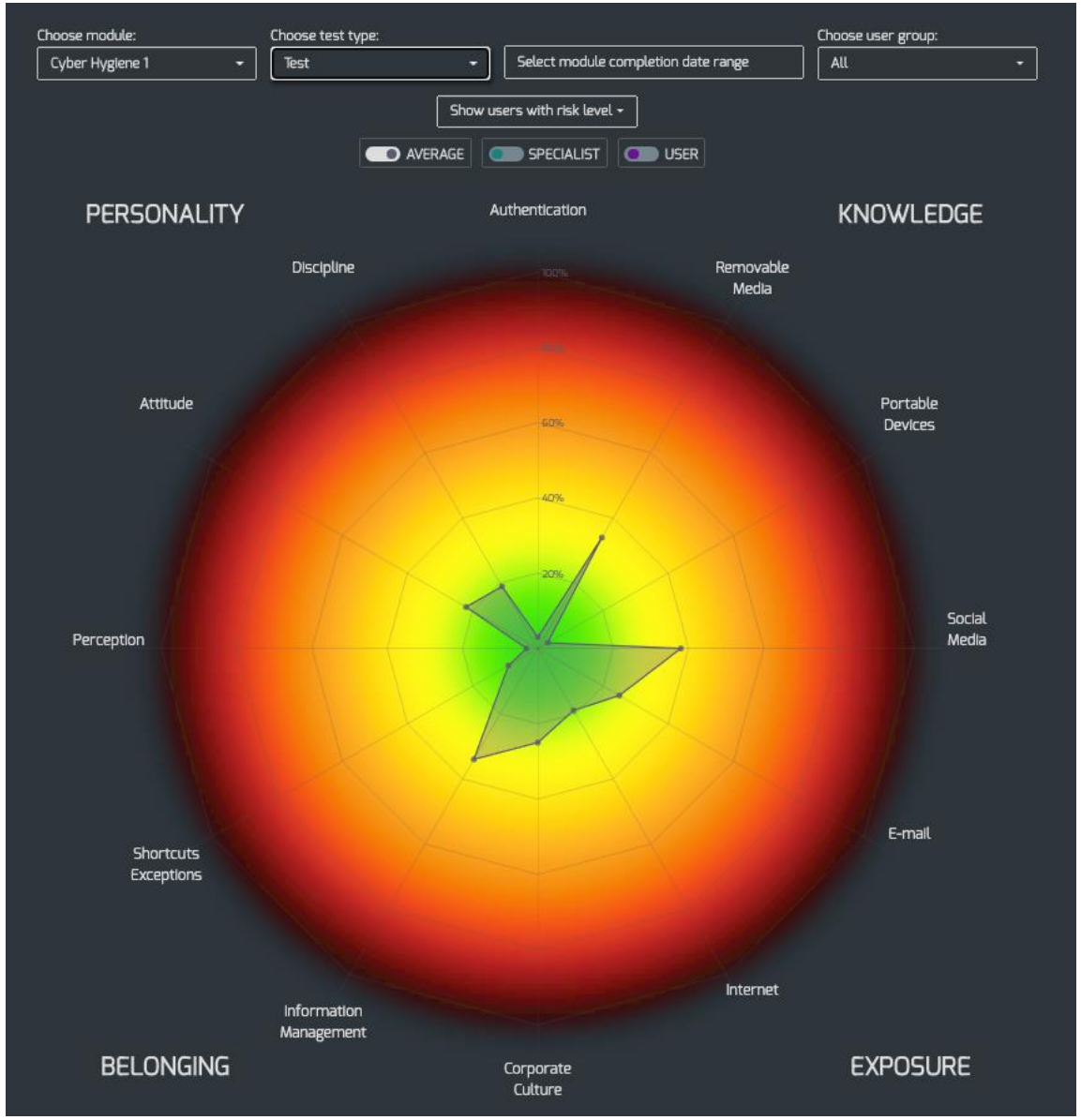
Скріншоти з курсу





ISSP


Choose module:
Cyber Hygiene 1
Choose test type:
All
Select module completion date range
Choose user group:
All
Show users with risk level
AVERAGE
SPECIALIST
USER
PERSONALITY
KNOWLEDGE
BELONGING
EXPOSURE
Authentication
Removable Media
Portable Devices
Social Media
E-mail
Internet
Corporate Culture
Information Management
Shortcuts Exceptions
Perception
Attitude
Discipline
100%
80%
60%
40%
20%


Choose module:
Cyber Hygiene 1
Choose test type:
Test
Select module completion date range
Choose user group:
All
Show users with risk level
AVERAGE
SPECIALIST
USER
PERSONALITY
KNOWLEDGE
BELONGING
EXPOSURE
Authentication
Removable Media
Portable Devices
Social Media
E-mail
Internet
Corporate Culture
Information Management
Shortcuts Exceptions
Perception
Attitude
Discipline
100%
80%
60%
40%
20%

ПРИКЛАДИ АНАЛІТИЧНИХ ЗВІТІВ

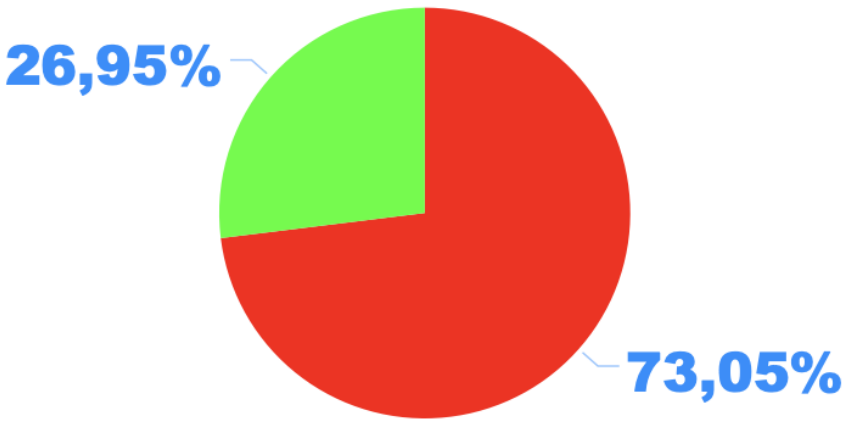
M-1

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



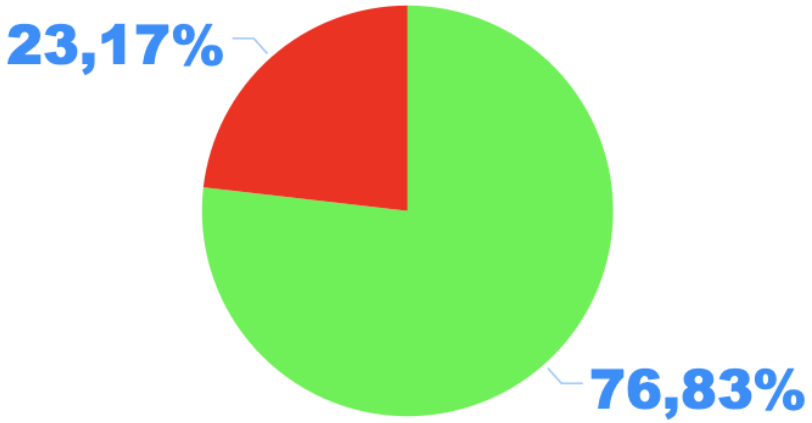
M-2

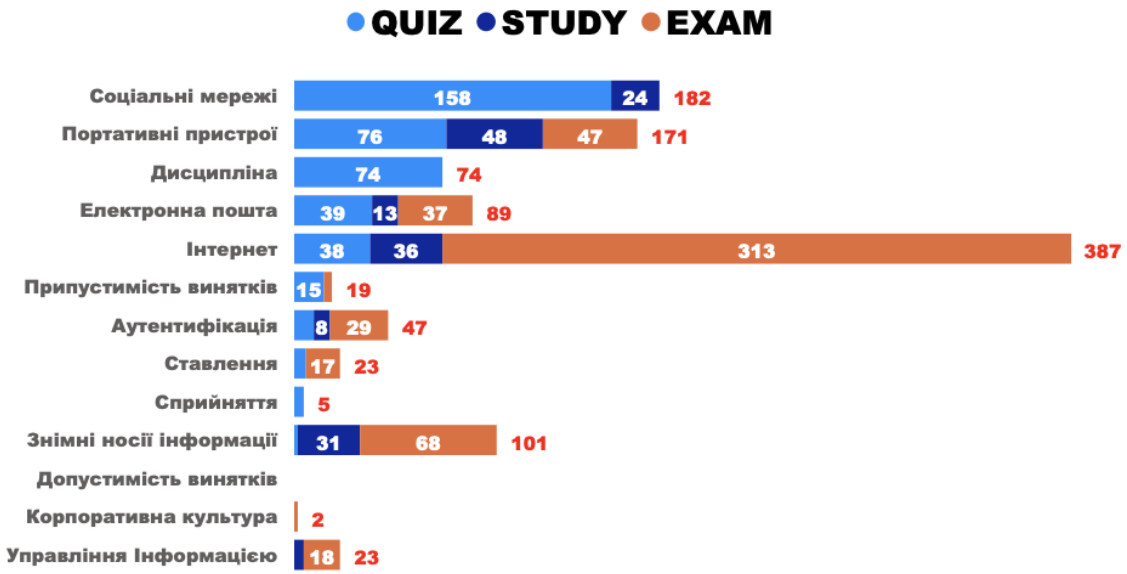
505

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



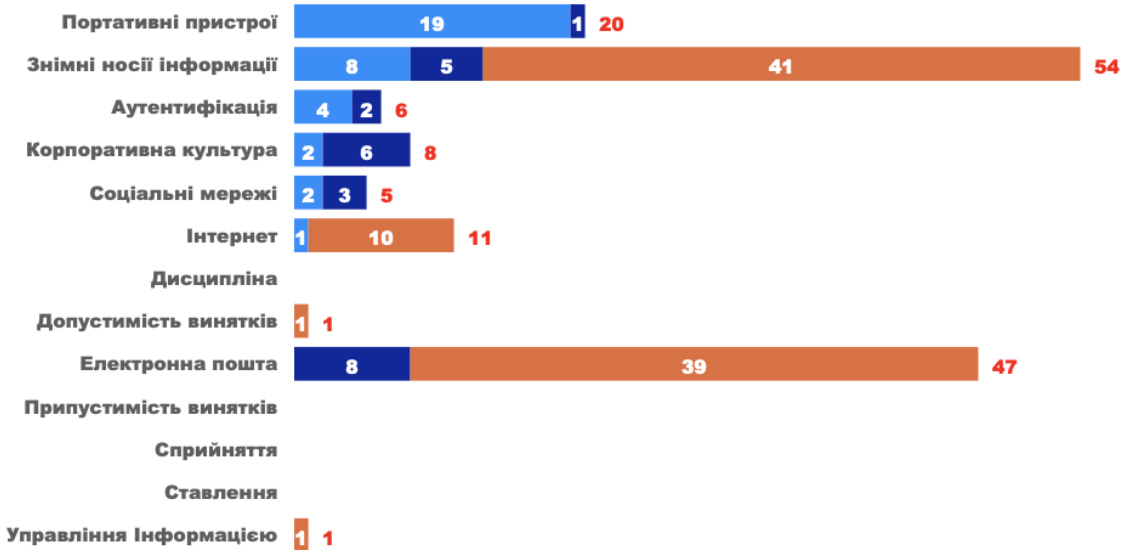


M-1

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**



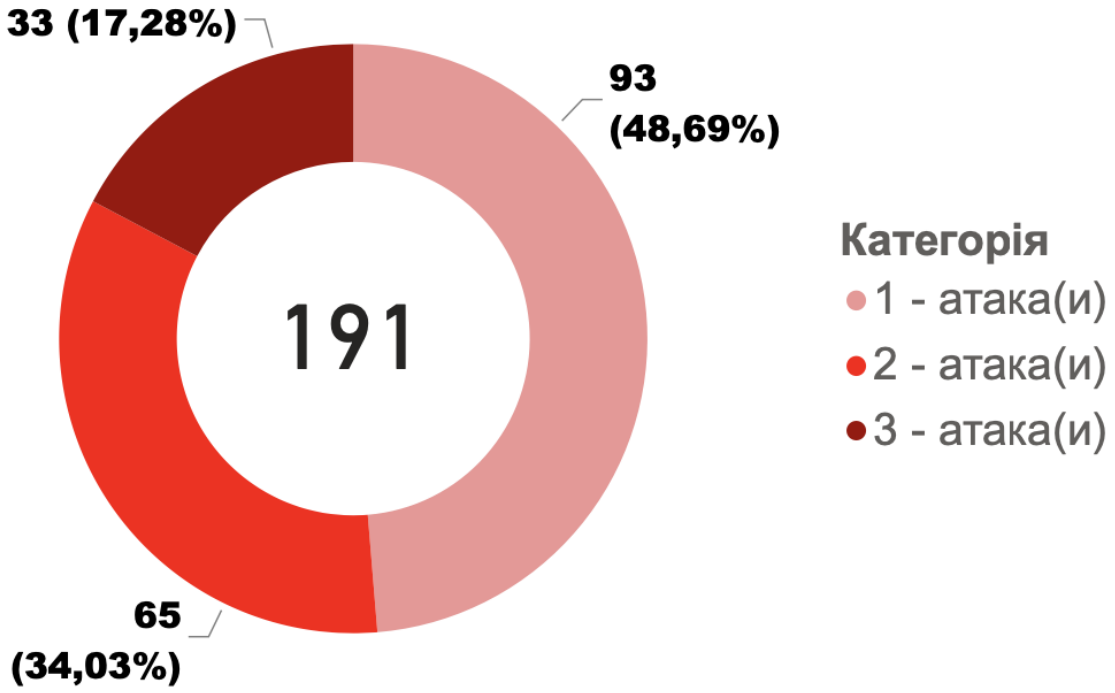
M-2

505

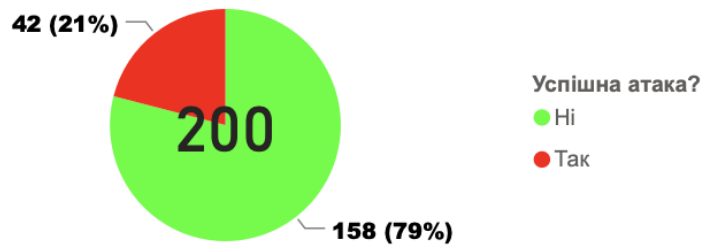
К-ть учасників

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**

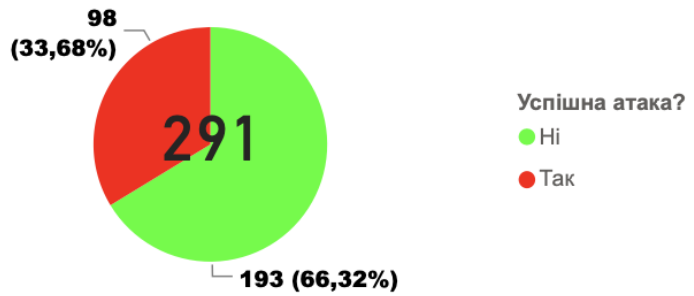
Кількість осіб щодо яких успішно проведено фішингову атаку



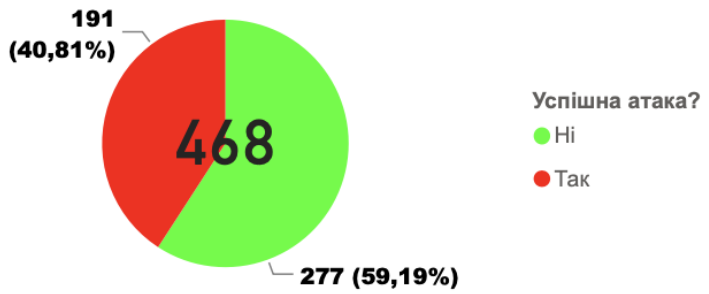
Атака № 1



Атака № 2



Атака № 3



! 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