

НАВЧАЛЬНО-НАУКОВА ЛАБОРАТОРІЯ КІБЕРБЕЗПЕКИ

при кафедрі кібербезпеки та математичного моделювання



Кафедра кібербезпеки та математичного моделювання

У складі кафедри кібербезпеки та математичного моделювання функціонує навчально-наукова лабораторія кібербезпеки (ННЛКБ)





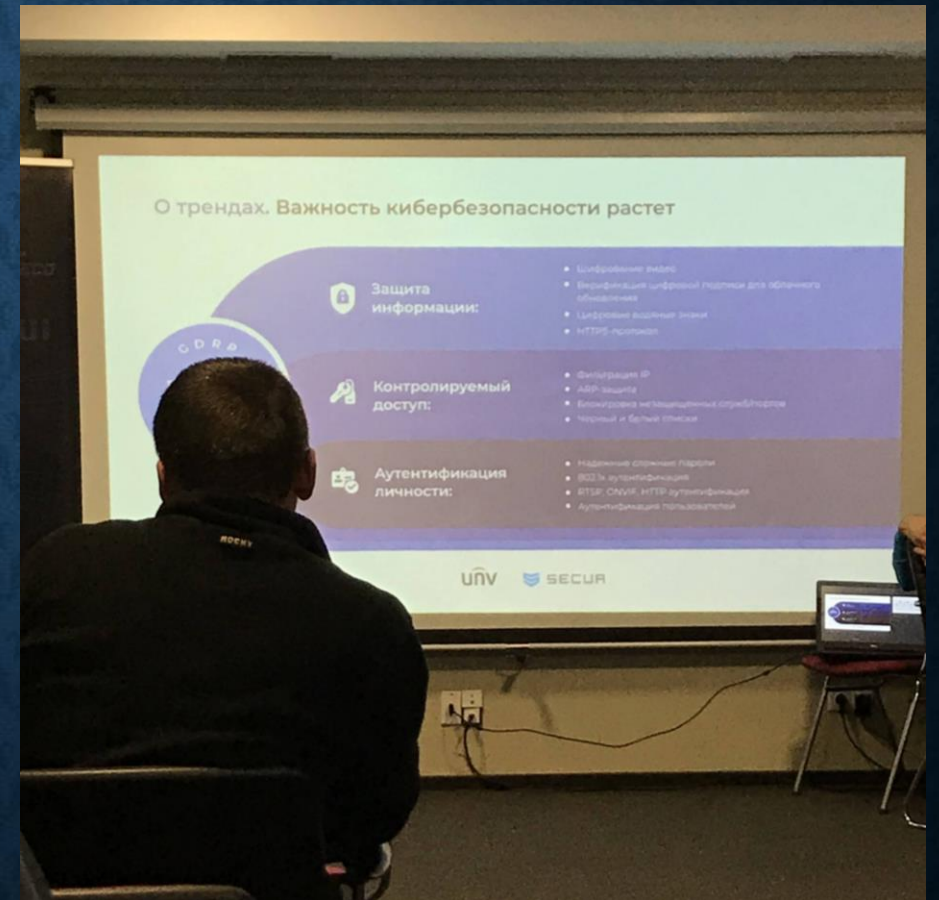
Кафедра кібербезпеки та математичного моделювання

Лабораторія забезпечує науково-методичну діяльність кафедри відповідно до освітньо-професійних програм підготовки фахівців спеціальності 125 «Кібербезпека», проведення наукових досліджень у межах затверджених наукових напрямів кафедри та впровадження результатів досліджень у практичну діяльність, роботу творчих колективів здобувачів вищої освіти, створених для вирішення конкретної наукової проблеми, наукових товариств та гуртків.



Основні завдання ННЛКБ:

- забезпечення умов для проведення тематичних лекцій, лабораторних, практичних та семінарських занять, навчальних практик, виконання курсових та кваліфікаційних проектів (робіт) студентами та дисертаційних робіт аспірантами і здобувачами;



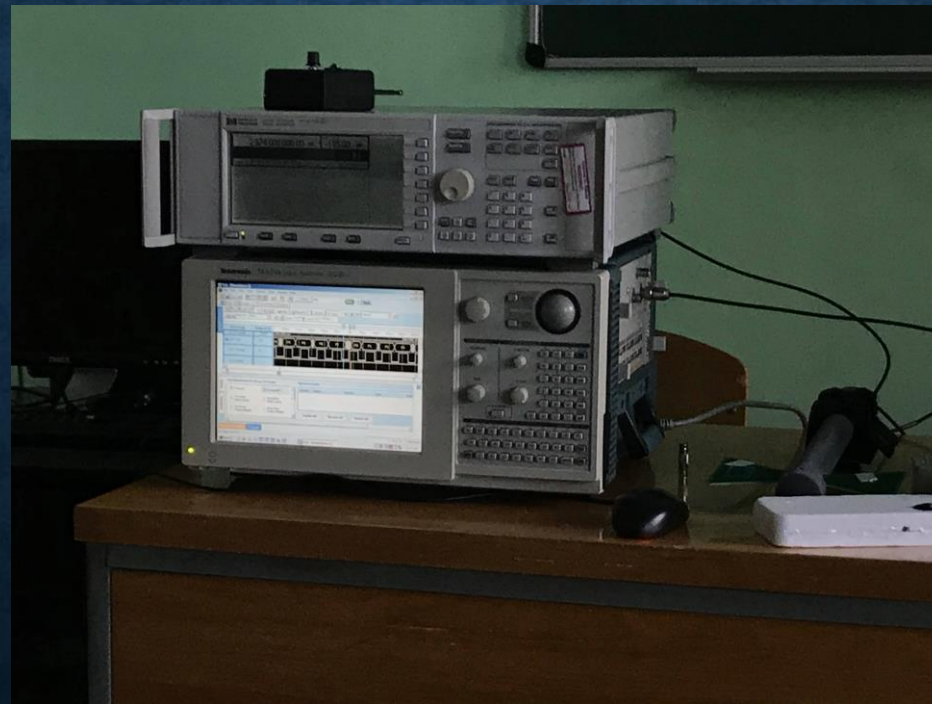
Основні завдання ННЛКБ:

- організація науково-дослідної роботи здобувачів вищої освіти, впровадження наукових досліджень в освітній процес;
- забезпечення умов для набуття здобувачів вищої освіти умінь та навичок в науково-дослідницькій роботі та застосування отриманих знань на практиці;



Основні завдання ННЛКБ:

- систематичне оновлення та удосконалення навчально-лабораторної бази, технічних засобів навчання, комп'ютеризації та інформатизації навчального процесу;



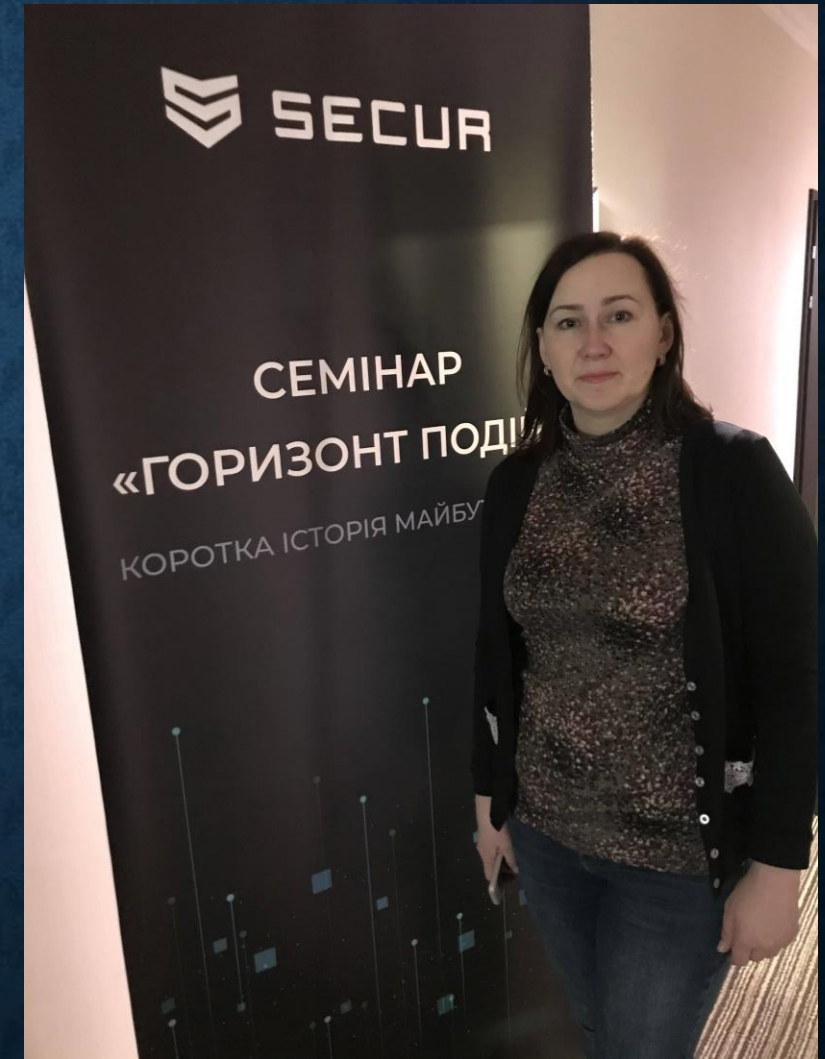
Основні завдання ННЛКБ:



- забезпечення умов для проведення теоретичних і експериментальних досліджень, науково-дослідних робіт за науковими напрямками кафедри кібербезпеки та математичного моделювання;

Основні завдання ННЛКБ:

- співпраця з представниками державних, приватних і громадських органів та організацій у сфері кібербезпеки;
- проведення науково-практичних конференцій, семінарів, тренінгів та інших заходів з питань кібербезпеки;



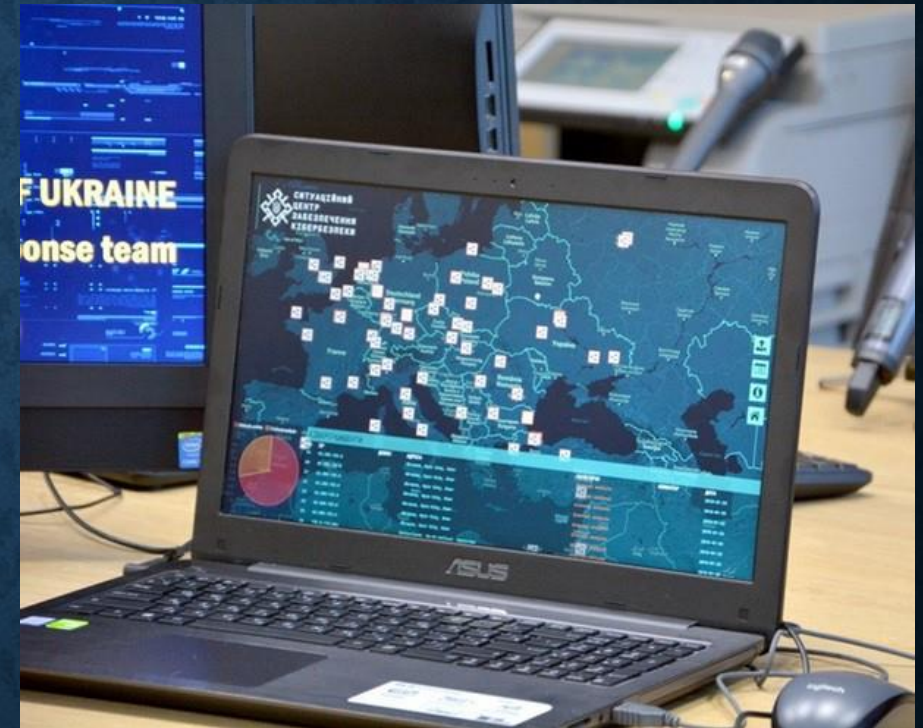
Основні завдання ННЛКБ:

- консультування з питань кібербезпеки;
- проведення підготовки та підвищення кваліфікації кадрів в сфері кібербезпеки;
- розробка та реалізація проектів в сфері кібербезпеки.



КІБЕРНЕТИЧНИЙ ПОЛІГОН

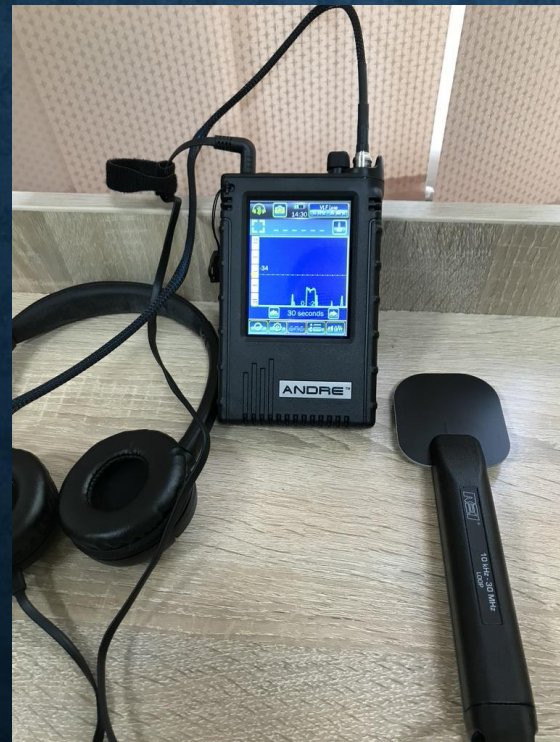
На базі лабораторії створений програмно-апаратний комплекс «Кібернетичний полігон», мета якого — відпрацювання технологій виявлення кібератак та протидії ним, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж.



**Cyber
Polygon**

КІБЕРНЕТИЧНИЙ ПОЛІГОН

Кіберполігон - високопродуктивна лабораторія для дослідження програмних продуктів і устаткування.



КІБЕРНЕТИЧНИЙ ПОЛІГОН

Будь-який продукт може бути проаналізований на предмет вразливостей і незадекларованих можливостей з використанням найсучасніших технологій і рішень. Тестування продукту включає в себе:

- аналіз коду програмних продуктів, в тому числі з використанням методів зворотної інженерії;

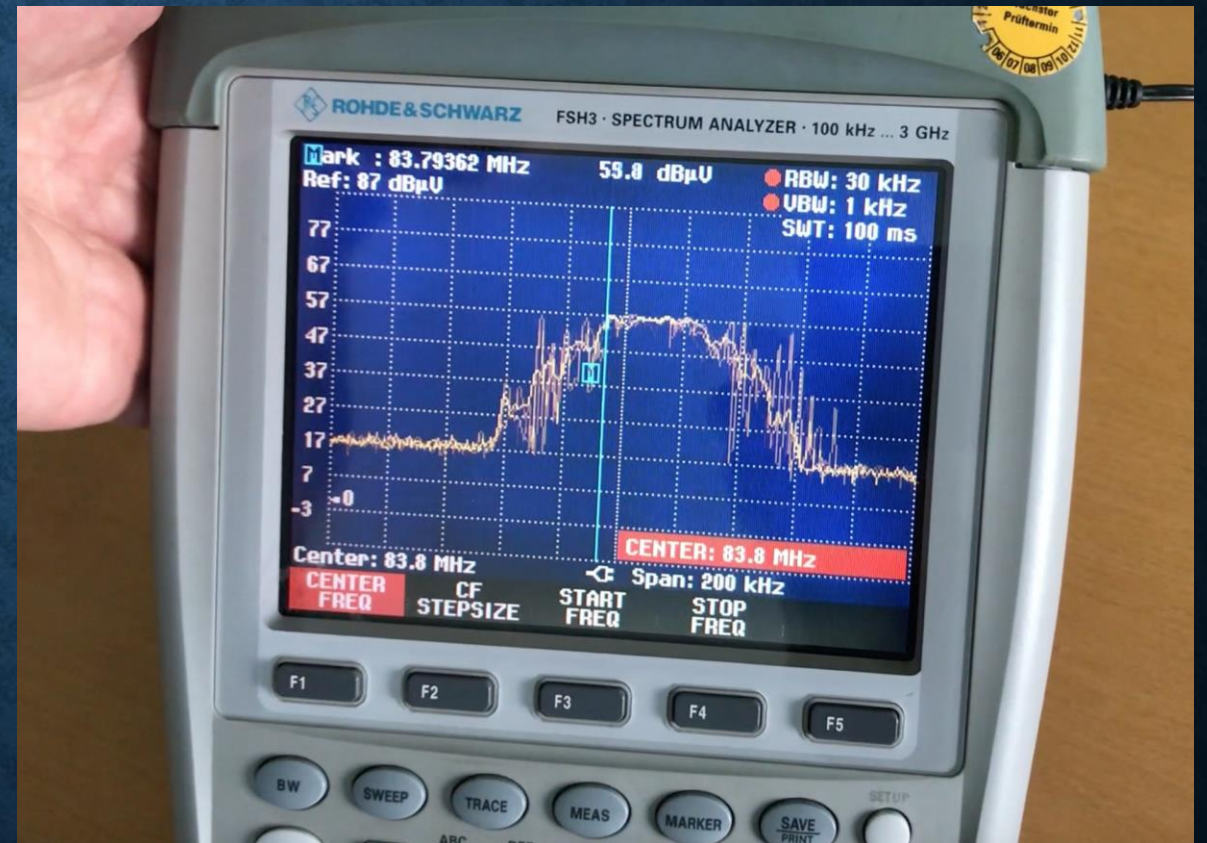
- аналіз функціональності програмно-апаратних комплексів;

- виявлення вразливостей в автоматизованих системах управління;

- тестування навантаження систем управління і систем захисту інформації;

- перевірка оновлень ПО перед застосуванням;

- перевірка захищеності мереж зв'язку.



КІБЕРНЕТИЧНИЙ ПОЛІГОН



Проводиться практична підготовки фахівців в області інформаційної та кібернетичної безпеки. Відпрацьовуються сценарії виникнення і розвитку кібернетичних загроз, вивчаються механізми їх нейтралізації та активної протидії, методи виявлення вразливих місць систем захисту локальних мереж.

КІБЕРНЕТИЧНИЙ ПОЛІГОН

Проводяться наукові дослідження програмно-апаратних засобів кібернетичної розвідки, захисту і впливу (активної протидії) на навчальні об'єкти з критичної інфраструктурою.

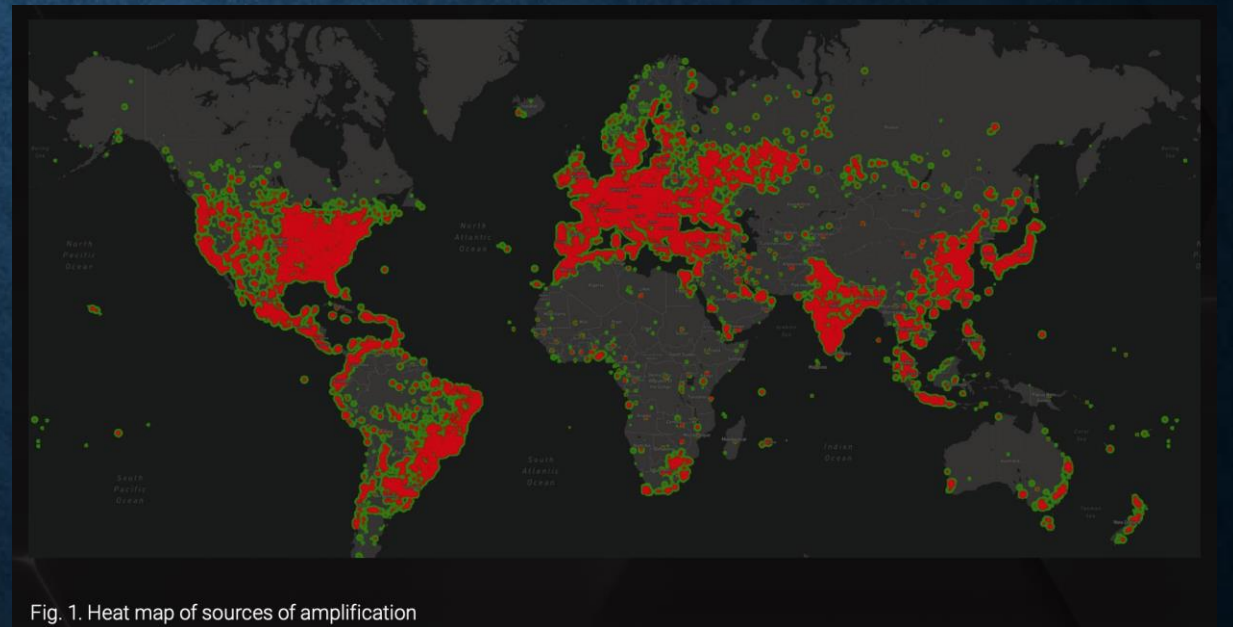
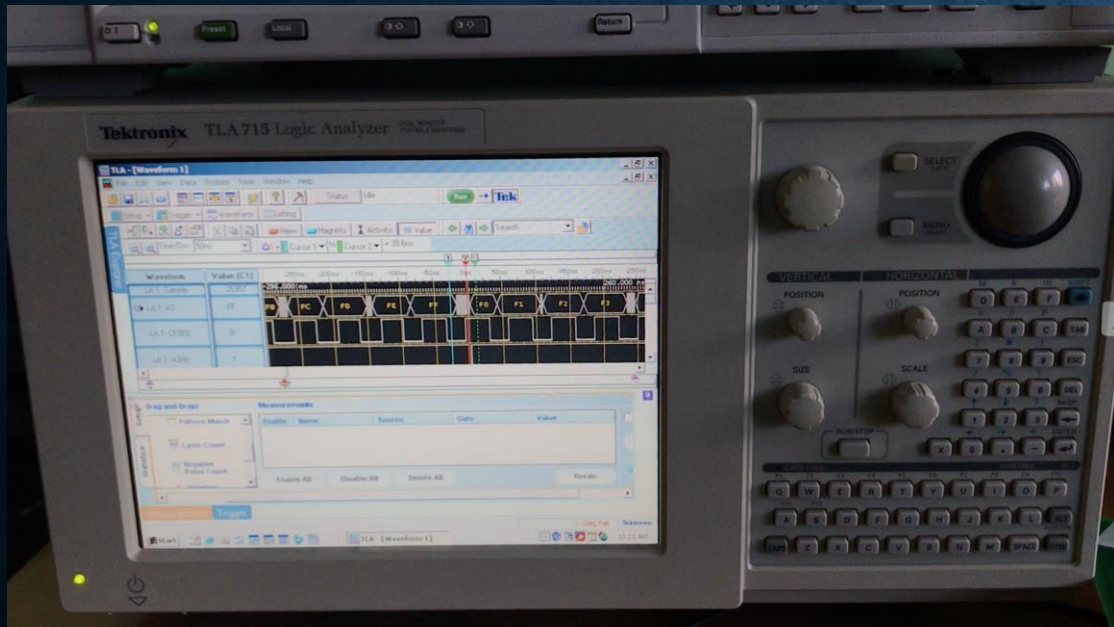


Fig. 1. Heat map of sources of amplification

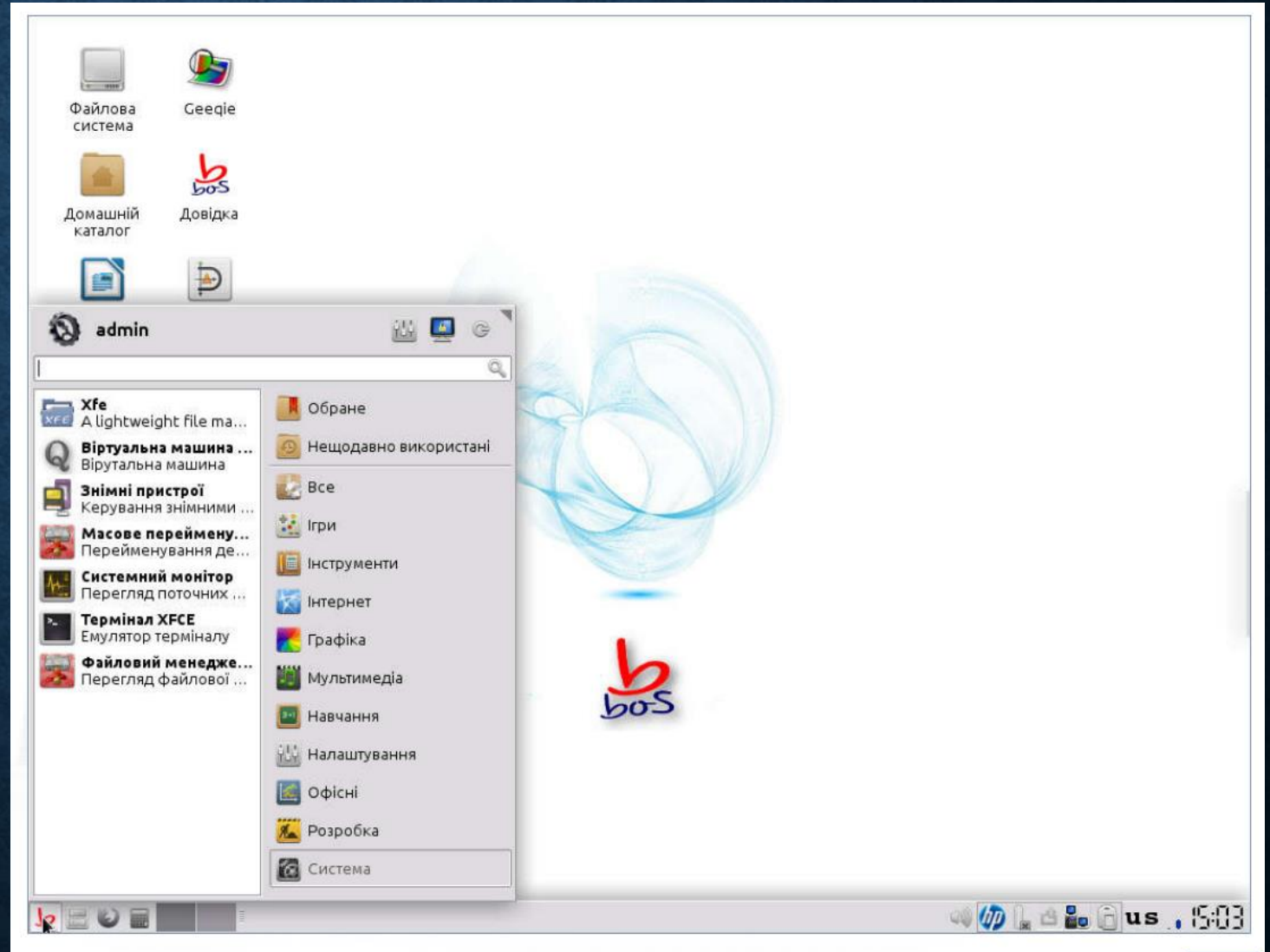
ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

проводити за допомогою сучасного радіоелектронного обладнання моніторинг інформаційного простору з метою виявлення внутрішніх і зовнішніх загроз і оцінювати їх рівень за певними критеріями



ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

розробляти перспективне спеціалізоване програмне забезпечення для захисту від несанкціонованого доступу до інформаційних систем;



ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

проводити спецдослідження в галузі технічних та програмних засобів кіберзахисту та відповідних методик захисту об'єктів критичної інфраструктури;



ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

визначати оптимальні способи
нейтралізації загроз в кіберпросторі з
урахуванням наявних апаратно-
програмних засобів технічного
захисту інформації;

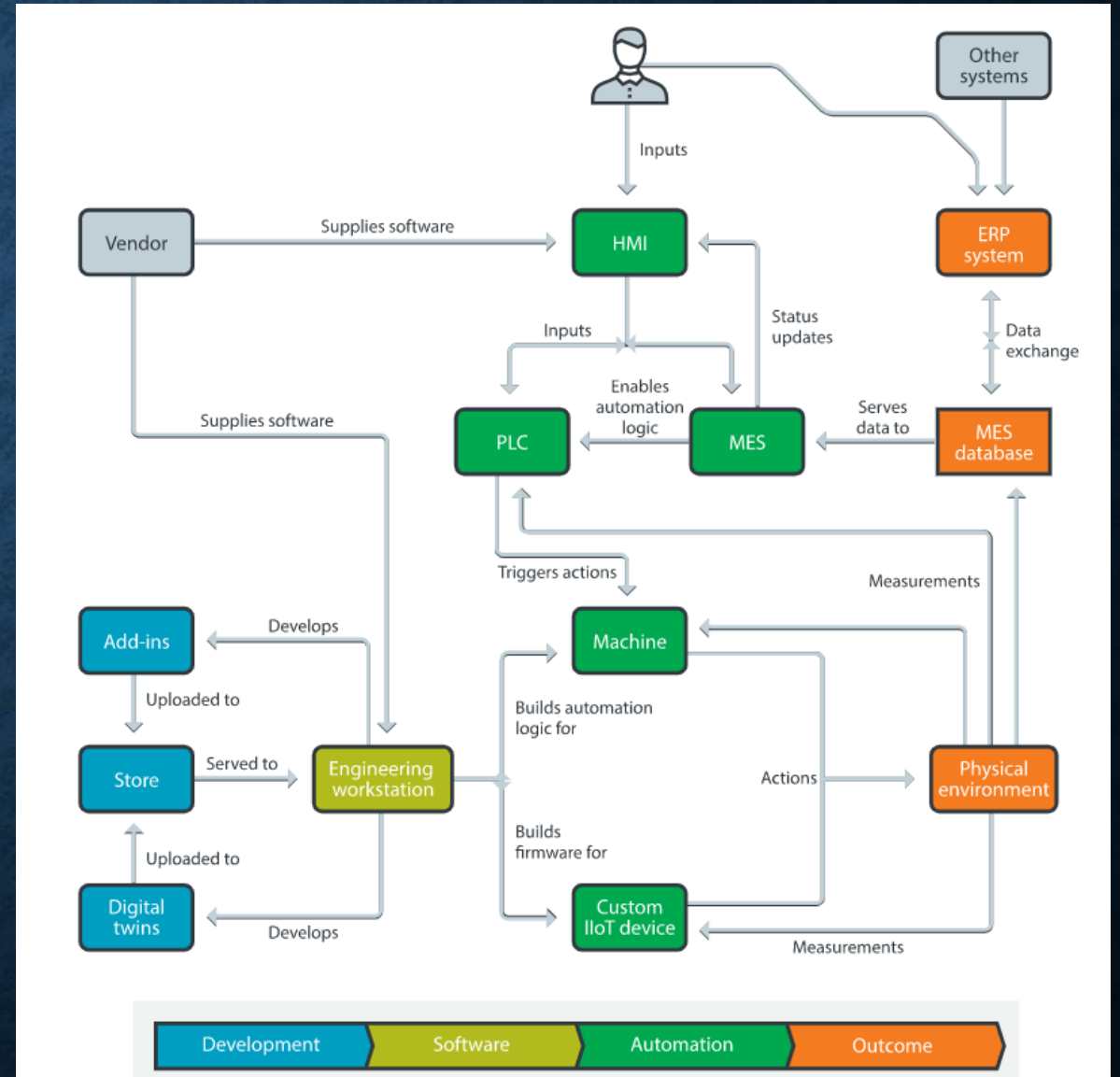
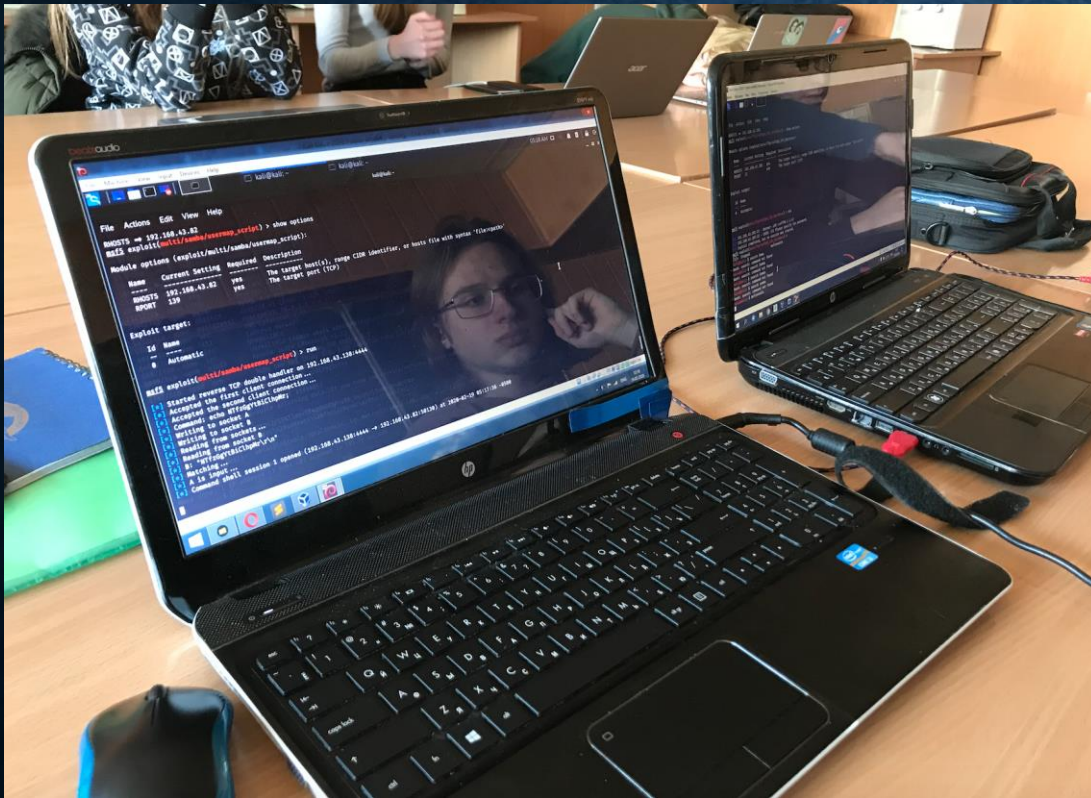


Encryption Speed: 100 Mb/s
1/10/100 Gb/s

The complex block contains three images of IN-CYBER encryption hardware. At the top, there are two USB sticks and one small black device. Below them, the text 'Encryption Speed: 100 Mb/s' and '1/10/100 Gb/s' is displayed. At the bottom, there is a rack-mounted device labeled 'IN-CYBER NEO-900'. In the bottom left corner, there is a logo for 'SANS Sarawak Encryption Standard'.

ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

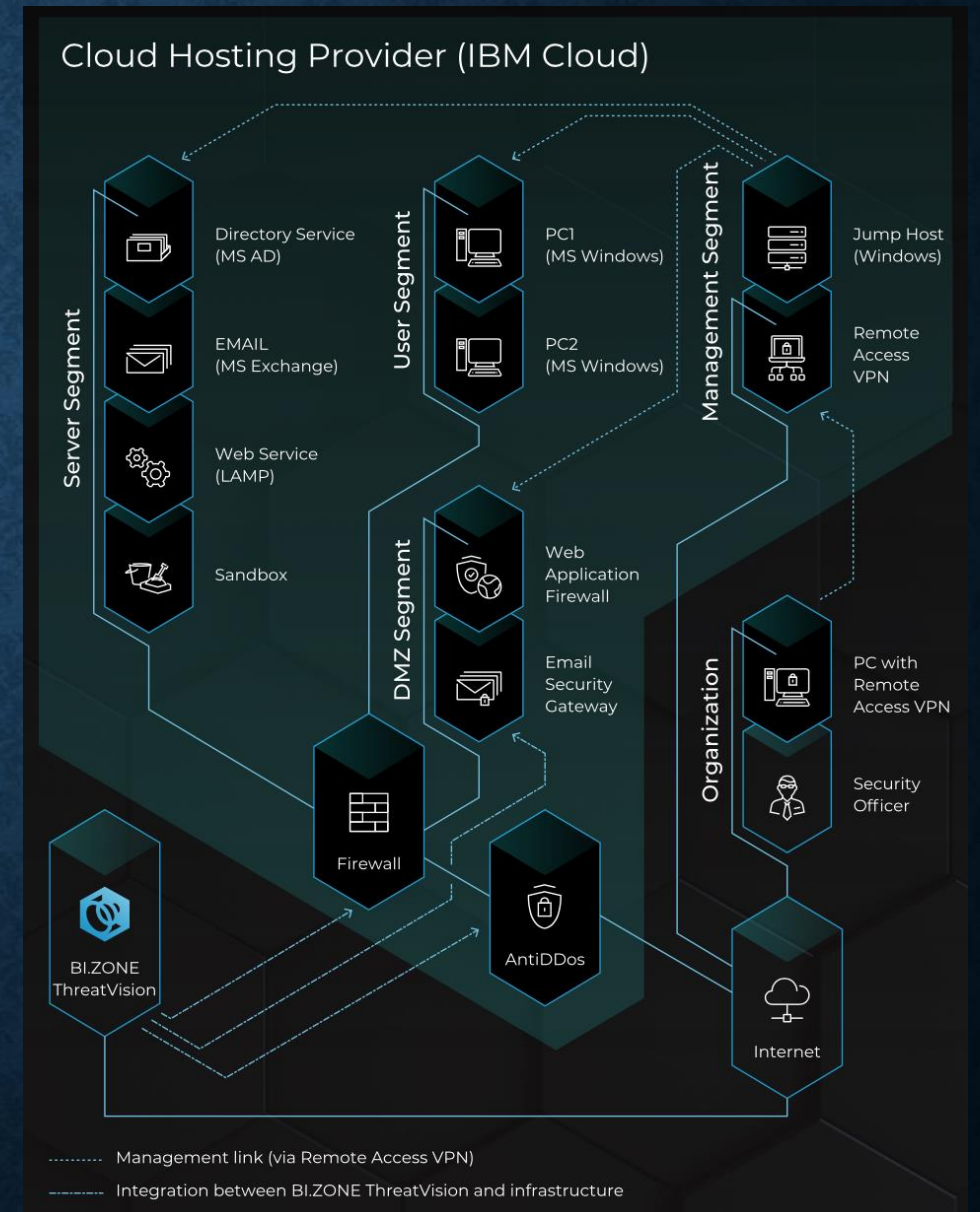
моделювати процеси нападу та захисту інформаційних систем об'єктів критичної інфраструктури;



ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

оцінювати рівень захищеності
електронних ресурсів та апаратно-
програмних засобів інформаційних
систем;

ВІДНОВЛЕННЯ	RC	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ
ВИЗНАЧЕННЯ	ID	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ
ЗАХИСТ	PR	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ
ВИЯВЛЕННЯ	DE	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ
РЕАГУВАННЯ	RS	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ
ВІДНОВЛЕННЯ	RC	КАТЕГОРІЇ	ПІДКАТЕГОРІЇ	ІНФОРМАЦІЙНІ ПОСИЛАННЯ



ФУНКЦІОНУВАННЯ ПОЛІГОНУ ДОЗВОЛЯЄ:

аналізувати ефективність кібервпливу на інформаційні системи об'єктів критичної інфраструктури.

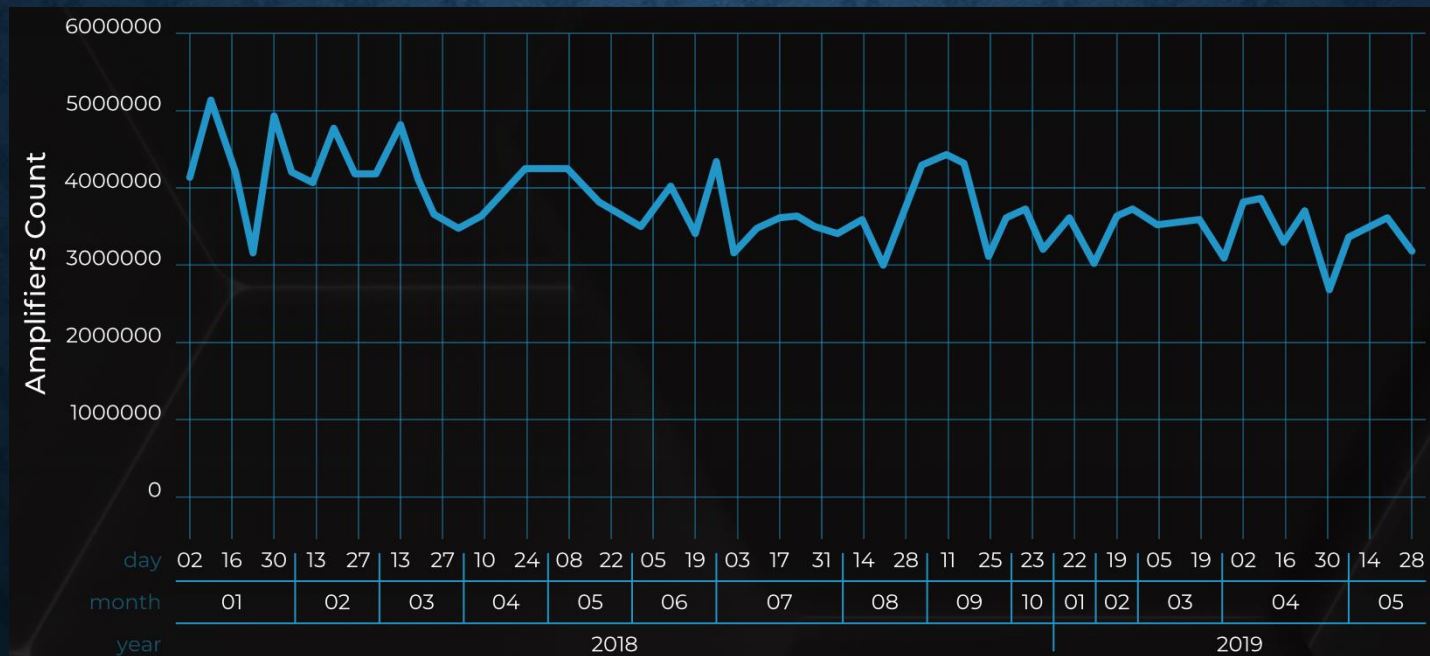


Fig. 2. Dynamics of DNS amplifiers

Обладнання ННЛКБ

Лабораторія має дві навчальні аудиторії та обладнана 24 сучасними робочими місцями на базі комп'ютерного обладнання DELL Optiplex 780



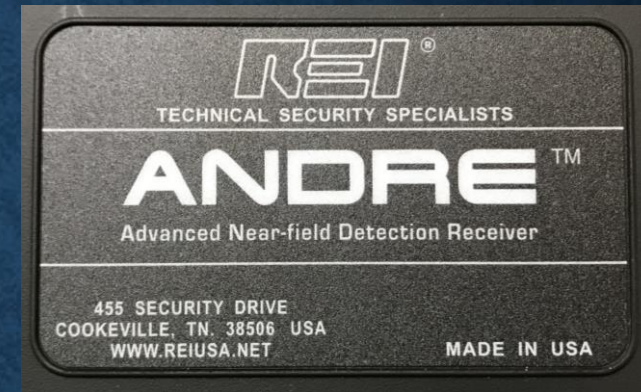
Обладнання ННЛКБ

Для вивчення сучасних мережевих технологій в лабораторії змонтовано нову телекомунікаційну шафу з обладнанням комутації та маршрутизації MikroTik



Обладнання ННЛКБ

Для виявлення приховано встановлених електронних пристроїв використовується багатофункціональний пошуковий прилад ANDRE, виробництва США



Обладнання ННЛКБ

Для захисту об'єктів від витоку інформації з обмеженим доступом застосовується продукція науково-виробничого підприємства «РІАС». Серед обладнання лабораторії представлені прилади радіочастотного та акустичного шуму, прилади захисту інформації в аналогових телефонних лініях



Обладнання ННЛКБ

Досліджувати акустоелектричні канали витоку інформації студенти мають змогу за допомогою універсальних напіваавтоматичних приладів «Бумеранг-2Г»

