НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

Відділення енергетики та енергетичних технологій НАН України

Наукова рада «Кібербезпека в енергетиці»

ПЛАН РОБОТИ
МІЖВІДОМЧОГО МІЖРЕГІОНАЛЬНОГО
НАУКОВО-ПРАКТИЧНОГО СЕМІНАРУ

"Кібербезпека та захист інформації"
на 2026 р.

Київ 2026

Базові підрозділи:	Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ Державний університет інформаційно-комунікаційних технологій
Науковий керівник Співголова	чл.-кор. НАН України (відділення енергетики та енергетичних технологій), д.т.н., проф. Мохор Володимир Володимирович, MokhorVV@nas.gov.ua
Науковий керівник Співголова	чл.-кор. НАН України (відділення інформатики), д.т.н., проф. Корченко Олександр Григорович agkorchenko@gmail.com
Вчений секретар	к.т.н., проф. Хохлачова Юлія Євгеніївна yuliiahohlachova@gmail.com
Керівник Вінницького відділення	д.т.н., проф. Яремчук Юрій Євгенович yurevyar@gmail.com
Керівник Дніпровського відділення	д.т.н., проф. Корнієнко Валерій Іванович korniienko.v.i@nmu.one
Керівник Закарпатського відділення	д.ф.-м.н., проф. Різак Василь Михайлович vrizak@uzhnu.edu.ua
Керівник Львівського відділення	д.т.н., проф. Дудикевич Валерій Богданович vdudykev@gmail.com
Керівник Одеського відділення	д.т.н., проф. Кобозєва Алла Анатоліївна alla_kobozeva@ukr.net
Керівник Тернопільського відділення	д.т.н., проф. Касянчук Михайло Миколайович, kasyanchuk@ukr.net
Керівник Харківського відділення	д.т.н., проф. Євсеєв Сергій Петрович Serhii.Yevseiev@gmail.com
Керівник Хмельницького відділення	д.т.н., проф. Говорущенко Тетяна Олександрівна hovorushchenko@khmnu.edu.ua
Керівник Чернігівського відділення	д.т.н., професор Ткач Юлія Миколаївна tkachym@icloud.com

ВІННИЦЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Яремчук Ю.Є.
Вчений секретар: канд. техн. наук, доцент Карпінець В.В.
Місце проведення семінару:
Вінницький національний технічний університет,
м. Вінниця, вул. Хмельницьке шосе, 95, ВНТУ, другий навчальний корпус, ауд. 2304.

Початок роботи – 15^{00}

14.01	1. Нормативне забезпечення та особливості захисту об'єктів критичної інфраструктури в сучасних умовах. Юрій Яремчук (ВНТУ) 2. Метод захисту від лазерних систем акустичної розвідки. Віталій Катаєв (ВНТУ)
11.02	1. Новий підхід до вбудовування ЦВЗ. Василь Карпінець (ВНТУ) 2. Перспективи використання та впровадження Zero Trust Architecture. Ірина Бондаренко, Дар'я Пінчук (ВНТУ)
11.03	1. Методи формування захищеного каналу для управління дронами в умовах застосування засобів РЕБ. Анатолій Шиян (ВНТУ) 2. Забезпечення звукоізоляції та запобігання витоку інформації в умовах конфіденційних переговорів. В'ячеслав Гуменюк (ВНТУ)
08.04	1. Підвищення захищеності інформації від витоку через закладні пристрої. Павло Павловський (ВНТУ) 2. Вдосконалення біометричної автентифікації користувача з використанням розпізнавання міміки обличчя на основі нейронної мережі. Анастасія Кірчанова, Юрій Яремчук (ВНТУ)
13.05	1. Удосконалений метод виявлення та запобігання фішинговим загрозам у веборієнтованих інформаційних системах. Дмитро Присяжний (ВНТУ) 2. Методи захисту баз даних у хмарних сховищах AWS. Віталій Білоус (ВНТУ)
10.06	1. Динамічний аналіз впливу загроз на безпеку системи. Ольга Салієва, Юрій Яремчук (ВНТУ) 2. Удосконалення методу розпізнавання нечіткого голосу людей, що мають вади вимовляння деяких звуків, на основі нейромережі. Олександр Ніколайчук (ВНТУ)
09.09	1. Моделі управління ризиками для підвищення захищеності об'єктів критичної інфраструктури. Лілія Нікіфорова, Анатолій Шиян (ВНТУ) 2. Вдосконалений метод дослідження комп'ютерних інцидентів. Микола Римаренко (ВНТУ)
14.10	1. Адаптивне управління інцидентами у хмарному середовищі за допомогою когнітивних агентів. Анатолій Грицак (ВНТУ) 2. Підвищення завадостійкості шифрованого аналогового відеосигналу БПЛА на основі методу з автоматичною зміною частоти каналу. Дмитро Соколовський, Василь Карпінець (ВНТУ)
11.11	1. Ідентифікація вторгнень у комп'ютерну систему на основі генетичних алгоритмів.

	Кирило Безпалий, Юрій Яремчук (ВНТУ) 2. Аналіз соціальних мереж для виявлення прихованих спільнот і трендів. Ірина Бондаренко, Анастасія Магденко (ВНТУ)
09.12	1. Особливості застосування тепловізорів для пошуку закладних пристроїв на реальних об'єктах інформаційної діяльності. Віталій Катаєв (ВНТУ) 2. Удосконалення системи виявлення мережевих атак на основі гібридного підходу машинного навчання з динамічним налаштуванням порогових значень. Вадим Вакуліч (ВНТУ)
16.12	Підсумкове засідання відділення семінару.

ДНІПРОВСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Корнієнко В.І.
Вчений секретар: ст. викладач Тимофєєв Д.С.
Місце проведення семінару:
Національний технічний університет "Дніпровська політехніка",
м. Дніпро, пр. Дмитра Яворницького, 19. Національний технічний університет "Дніпровська політехніка", ауд. 19, корп. 3.

Початок роботи – 15^{00}

15.01	1. Методи побудови правил контролю доступу на основі ролей для SAP On-Premise. Левенець Д.Д., Жукова О.А. (Національний технічний університет "Дніпровська політехніка") 2. Методика формування комплексних вимог безпеки при розробці програмного забезпечення. Кручінін О.В., Лукашевич А.Р. (Національний технічний університет "Дніпровська політехніка")
05.02	1. Метод OSINT для визначення цифрової ідентичності особи. Кручінін О.В., Магдєєв В.С. (Національний технічний університет "Дніпровська політехніка") 2. Методика виявлення прихованих каналів DNS-тунелювання на базі машинного навчання. Сафаров О.О., Ободовський Я.Ю. (Національний технічний університет "Дніпровська політехніка")
12.03	1. Програма навчання з протидії кіберзагрозам для персоналу енергетичної компанії. Святошенко В.О., Пилько Я.І. (Національний технічний університет "Дніпровська політехніка") 2. Методи підвищення захищенності протоколу підключення IoT пристроїв Matter Герасіна О.В., Семачкін О.Д. (Національний технічний університет "Дніпровська політехніка")
02.04	1. Обгрунтування методу активного захисту інформації від витоку каналами ПЕМВН з інверсним шумовим сигналом. Мілінчук Ю.А., Стасюк П.Р. (Національний технічний університет «Дніпровська політехніка») 2. Система моніторингу стану комплексу технічного захисту інформації. Корнієнко В.І., Терин М.О. (Національний технічний університет «Дніпровська політехніка»)

30.04	1. Використання методів стохастичної гри в процесі протидії інсайдерським атакам. Тимофєєв Д.С., Тищенко К.С. (Національний технічний університет «Дніпровська політехніка») 2. Розробка захищеної цифрові архітектури для високочастотних RFID-міток. Магро В.І., Швець Д.С. (Національний технічний університет «Дніпровська політехніка»)
14.05	1. Система біометричної голосової автенти-фікації з агентною архітектурою для безпечного управління Kubernetes кластером. Корнієнко В.І., Корнєєв О.Ю. (Національний технічний університет «Дніпровська політехніка») 2. Автоматизація тестування на проникнення з використанням інструментів генеративного штучного інтелекту. Тимофєєв Д.С., Кузнецов Б.В. (Національний технічний університет «Дніпровська політехніка»)
11.06	1. Методика автоматизованого тестування на проникнення систем керування контентом (CMS) WordPress. Мєшков В.І., Санжара Є.В. (Національний технічний університет «Дніпровська політехніка») 2. Моніторинг цілісності конфігурації робочих станцій локальної мережі. Ковальова Ю.В., Яненко О.В. (Національний технічний університет «Дніпровська політехніка»)
10.09	1. Захист інформації з обмеженим доступом від впливу ненавмисних електромагнітних завад при обробці технічними засобами. Магро В.І., Козловський М.В. (Національний технічний університет «Дніпровська політехніка») 2. Розробка комплексу засобів захисту інформації з обмеженим доступом із використанням GSM-каналів зв’язку. Герасіна О.В., Коваленко А.В., (Національний технічний університет «Дніпровська політехніка»)
01.10	1. Інтегрована система екранування захищених приміщень об'єктів інформаційної діяльності. Ковальова Ю.В., Павленко А.І. (Національний технічний університет «Дніпровська політехніка») 2. Методика підтримки прийняття рішень щодо забезпечення безпеки цифрових ланцюгів постачання програмного забезпечення. Святошенко В.О., Єрмаков О.В. (Національний технічний університет «Дніпровська політехніка»)
12.11	1. Підвищення стійкості паролів користувачів на основі статистичних характеристик української мови. Сафаров О.О., Косяченко С.Р. (Національний технічний університет «Дніпровська політехніка») 2. Дослідження звукоізоляційних властивостей захисних конструкцій об’єктів інформаційної діяльності. Магро В.І., Іванюк В.В. (Національний технічний університет «Дніпровська політехніка»)
03.12	1. Дослідження впливу режимів роботи відеотракту на рівні побічних електромагнітних випромінювань персонального комп’ютера. Корнієнко В.І., Гончарова А.Д. (Національний технічний університет «Дніпровська політехніка») 2. Комплексний аудит інформаційної безпеки веб-порталу дилерського автосалону.

	Жукова О.А., Хрипко Д.О. (Національний технічний університет «Дніпровська політехніка»)
17.12	Підсумкове засідання відділення семінару.

ЗАКАРПАТСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. фіз.-мат. наук, професор Різак В. М.
Вчений секретар: канд. фіз.-мат. наук, доцент Попович Н. І.
Місце проведення семінару:
Ужгородський національний університет,
м. Ужгород, вул. Волошина, 54, фізичний факультет, ауд. 251.

Початок роботи – 14^{00}

30.01	1.Система виявлення та ідентифікації БПЛА в реальному часі за акустичним слідом. Різак В. М. (УжНУ) 2.Telegram-бота для контролю доступу та безпеки персонального комп'ютера. Боценюк Л. Р. Розробка (УжНУ)
27.02	1.Вибір ключів в RSA алгоритмі шифрування та діапазон можливостей атаки Вінера на шифр Пагіря М. М. (УжНУ) 2.Аналіз сучасних тенденцій та досліджень у технологіях електронного голосування Матвіїв Ю. Ю. (УжНУ) 3.Кібербезпека вбудованих систем: виклики та рішення Войтович Б. В. (УжНУ)
27.03	1.Проблема невироджених інтерполяційних ланцюгових дробів та їх застосування в задачах криптографії. Мисло Ю. М. (УжНУ) 2.Моделювання загроз для IoT-пристроїв із застосуванням інфраструктури кіберполігону кафдери ТЕІБ УжНУ Маліцький Б. В. (УжНУ)
24.04	1.Застосування генераторів псевдовипадкових послідовностей в кібербезпеці Гапак О. М. (УжНУ) 2.Захист електронного документообігу в умовах розвитку квантових обчислень: концепція та реалізація Старцев А. (УжНУ)
29.05	1.Термічна стабільність наношарів інформаційних біомолекул для застосування в системах молекулярної криптографії Попович Н. І. (УжНУ) 2.Сучасні технології та підходи у сфері автоматизації розгортання інформаційної інфраструктури під час освітнього процесу Черепов О. С. (УжНУ)
25.09	1.Перспективи практичного використання нелінійних оптичних властивостей плівкових структур на основі бактеріородопсину у системах технічного захисту інформації Трикур І. І. (УжНУ)

	2.Стеганографічні методи приховування інформації у відео на платформах YouTube та TikTok Пирогов О. О. (УжНУ)
30.10	1.Big Data в управлінні міжнародною логістикою Яковець В. В. (УжНУ) 2.Центр IoT-досліджень при кафедрі ТЕІБ УжНУ. Ігнатоля П. (УжНУ) 3.Інтелектуальні технології захисту інформаційних ресурсів в комп'ютерних системах Безвершенко Є. І. (УжНУ)
27.11	1.Гібридний метод шифрування кольорових зображень на основі матриць Адамара та хаотичних систем Фролов А. О. (УжНУ) 2.Квантово-хімічне моделювання фотоциклу бактеріородопсину для створення захищених біофізичних систем зберігання даних Скиба І.В. (УжНУ)
18.12	Підсумкове засідання відділення семінару

КИЇВСЬКЕ ВІДДІЛЕННЯ

Керівник: чл.-кор. НАН України, д.т.н., професор Корченко О.Г.
Вчений секретар: канд. техн. наук, професор Хохлачова Ю.Є.
Місце проведення семінару:
Державний університет інформаційно-комунікаційних технологій,
м. Київ, вул. Солом'янська, 7, ауд. 423.
Державний торговельно-економічний університет,
м. Київ, вул. Кіоту, 19, корпус В, ауд. 514.

Початок роботи – 15^{00}

15.01	1. Антенна система для локалізації несанкціонованих радіовипромінювань Данилов І.Д., Пепа Ю.В. (ДУІКТ) 2. Аналіз поляризаційних ознак приховування інформації в радіовипромінюваннях Пепа Ю.В. (ДУІКТ) 3. Алгоритмичний підхід до оцінки впливу радіозакладних джерел нефлуктуаційних перешкод на цілісність дискретних сигналів з багатопозиційною фазовою маніпуляцією Бондаренко Є.В., Туровський О.Л. (ДУІКТ)
29.01	1. Метод захисту інформації на об'єктах критичної інфраструктури Собчук А.В., Біляєв Д.А. (ДУІКТ) 2. Кіберзагрози технічним каналам передачі інформації транспортної інформаційно-комунікаційної мережі Хворстяний Р.В. (ДУІКТ) 3. Метод протидії атакам на канали зв'язку Дробик О.В., Ровда В.В. (ДУІКТ)
12.02	1. Як ШІ робить фішинг правдоподібнішим і що з цим робити Цюцюра С.В., Цюцюра М.І. (ДТЕУ) 2. Безпечна розробка (Secure SDLC) для IT-команд, що не мають власного CISO

	Хлапонін Ю.І., Мних А.С. (ДТЕУ) 3. Типові помилки конфігурацій хмарних середовищ і способи їх автоматизованого виявлення Палагута К.О., Жирова Т.О., Котенко Н.О. (ДТЕУ)
26.02	1. Перспективи та напрямки розбудови системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова Чабан Б.В., Котенко А.М. (ДУІКТ) 2. Механізми підвищення ефективності розслідування кіберінцидентів на острові побудови оцінки ризиків Орлов Р.Р. (ДУІКТ) 3. Захист персональних даних у системі інформаційної безпеки сучасного суспільства Лозова І.Л., Різак М.В. (ДУІКТ)
26.03	1. Системний підхід до організації кіберзахисту інформаційних ресурсів закладів вищої освіти Шестак Я.І., Цюцюра М.І. (ДТЕУ) 2. Побудова моделі параметрів для оцінювання кіберстійкості Хохлачова Ю.Є. (ДТЕУ) 3. Кіберстійкість критичної інфраструктури в умовах гібридних загроз Десятко А.М., Токар В.В. (ДТЕУ)
30.04	*Виїзне засідання у Київський національний університет імені Тараса Шевченка* 1. Захист хмарних сервісів і віртуальної інфраструктури підприємства Щебланін Ю.М. (КНУ ім. Т. Шевченка) 2. Метод формування системи антитерористичного захисту об'єктів критичної інфраструктури Меленті Є.О. (Національна академія Служби безпеки України) 3. Метод захисту даних від несанкціонованого доступу Наконечний В.С. (КНУ ім. Т. Шевченка) 4. Метод побудови захищених каналів зв'язку Толюпа С.В. (КНУ ім. Т. Шевченка) 5. Методи обробки інцидентів інформаційної безпеки з використанням штучного інтелекту Бучик С.С. (КНУ ім. Т. Шевченка) 6. Метод захисту акустичної інформації при конференційних перемовах Лаптєв О.А. (КНУ ім. Т. Шевченка) 7. Метод протидії атакам на децентралізовані мережі Пархоменко І.І. (КНУ ім. Т. Шевченка) 8. Концептуальні основи побудови системи забезпечення протидії інформаційним впливам у соціальних мережах Браіловський М.М. (КНУ ім. Т. Шевченка) 9. Метод визначення стійкості систем захисту інформації від кібератак Лаптєв С.О. (КНУ ім. Т. Шевченка) 10. Методи захисту інформації в програмно-орієнтовиних мережах мережах SDN Даков С.Ю. (КНУ ім. Т. Шевченка) 11. Метод застосування штучного інтелекту для виявлення та нейтралізації кібератак у критичній інфраструктурі Білоконь І.В. (КНУ ім. Т. Шевченка) 12. Метод мінімізація втрат інформації в центрах обробки даних Шестак Я.В. (КНУ ім. Т. Шевченка)

	13. Метод підвищення завадостійкості бездротового зв'язку системи визначення вибухонебезпечних предметів Торошанко О.С. (КНУ ім. Т. Шевченка) 14. Алгоритм генерації асинхронного ключа на базі криптомодуля ATECC608A для гібридної системи визначення вибухонебезпечних предметів Дуднік А.С. (КНУ ім. Т. Шевченка) 15. Застосування операторів, породжених підсумовуванням рядів Фур'є, та їх інтерполяційних аналогів у виявленні несанкціонованого впливу на сигнали Барабаш О.В., Макарчук А.В. (НТУ України «Київський політехнічний інститут ім. І. Сікорського») 16. Спільна база пам'яті для мультиагентних систем на основі графів траєкторій Мусієнко А.П., Ворвуль Д.М. (НТУ України «Київський політехнічний інститут ім. І. Сікорського») 17. Програмне забезпечення для забезпечення живучості енергетичних підсистем Smart Energy Свинчук О.В., Дацюк О. А. (НТУ України «Київський політехнічний інститут ім. І. Сікорського») 18. Метод керування малим літальним апаратом в умовах невизначеності параметрів його стану Корнага Я.І., Базака Ю.А., Марченко О.І. (НТУ України «Київський політехнічний інститут ім. І. Сікорського») 19. Метод вибору кількості вхідних параметрів для оптимізації за допомогою нейромереж Корнага Я.І., Базака Ю.А., Гальченко І.О. (НТУ України «Київський політехнічний інститут ім. І. Сікорського»)
28.05	1. «Кібергігієна у військових формуваннях України» Артемов В.Ю. Національна академія СБ України 2. Передача шифрованих даних розподіленими мережевими лініями зв'язк Левкуша О.В., Пепа Ю.В. (ДУІКТ) 3. Метод захисту інформації на об'єктах критичної інфраструктури Собчук А.В. (ДУІКТ)
25.06	*Виїзне засідання у Державний університет «Київський авіаційний університет»* 1. Адаптивна ймовірнісна модель формування показника кіберстійкості цифрових інфраструктур до багатовекторних атак Козловський В.В. (ДУ «КАІ») 2. Інтелектуальна методика прогнозування реалізації кіберзагроз у системах цифрового управління в умовах динамічної невизначеності Міщенко А.В. (ДУ «КАІ») 3. Методологія поведінкового виявлення прихованої несанкціонованої активності на основі багатомасштабних патернів користувацької динаміки Лазаренко С.В. (ДУ «КАІ») 4. Методи та засоби боротьби з несанкціонованим доступом та копіюванням програмного забезпечення Скворцов С.О. (ДУ «КАІ») 5. Інтегрована модель попереджувального виявлення кібератак на основі кумулятивної еволюції показників мережевої активності Вишневська Н.С. (ДУ «КАІ») 6. Ймовірнісна архітектура гарантування кіберстійкості цифрових сервісів в умовах високоінтенсивних кіберзагроз Білоненко В.Ю. (ДУ «КАІ») 7. Методика адаптивного визначення ефективності кіберзахисних стратегій в умовах невизначеності інформаційного середовища

	Костюк І.Ю. (ДУ «КАІ») 8. Інтелектуальний метод адаптивного визначення ефективності кіберзахисних стратегій Цвьок Д.Р. (Міністерство цифрової трансформації) 9. Інтегральна модель формування індексу кіберризику на основі агрегованих поведінкових та інфраструктурних характеристик Кудренко С.О. (ДУ «КАІ») 10. Адаптивна методика прогнозування фаз еволюції кібератак у багаторівневих кіберфізичних середовищах Алькема В.В. (ДУ «КАІ») 11. Інтегрована модель синхронізації подій цифрової інфраструктури для прогнозування деградаційних процесів і ризику дестабілізації Макєєв І.Г. (ДУ «КАІ») 12. Ймовірнісна модель виявлення координованих атак через кореляційні взаємозв'язки між подіями безпеки Німіч О.В. (ДУ «КАІ») 13. Методика визначення впливу цифрової трансформації підприємства на його кіберстійкість Залевський Б.М. (ДУ «КАІ») 14. Адаптивна модель визначення чутливості хмарних платформ до складних багатовекторних атак із динамічним масштабуванням загроз Баланюк Ю.В. (ДУ «КАІ») 15. Інтелектуальна система інтерпретації інформаційних потоків для ідентифікації стану кіберзахищеності в реальному часі Моркляник Б.В. (ДУ «КАІ») 16. Модель динамічної оптимізації кіберзахисних стратегій у середовищах із високою варіативністю інформаційних параметрів Корж Р.О., Козловська Д.В. (ДУ «КАІ») 17. Байєсівсько-марківська методика визначення ймовірності критичних відмов у телекомунікаційних системах під впливом атак Торошанко А.І. (ДУ «КАІ») 18. Адаптивна самонавчальна архітектура кіберзахисту з проактивним реагуванням на нові класи атак Комар О.М. (ДУ «КАІ») 19. Модель динамічного пріоритизаційного ранжування кіберризиків на основі еволюційної поведінки загроз Тертус Я.В. (ДУ «КАІ») 20. Ймовірнісно-структурна методика визначення взаємозалежності між цифровою зрілістю організації та її кіберстійкістю Веклич О.К. (ДУ «КАІ») 21. Методика адаптивного визначення ефективності кіберзахисних стратегій в умовах невизначеності інформаційного середовища Мірненко В.І. (АО "Українська оборонна промисловість") 22. Модель прогнозування кумулятивного впливу складних атак у кіберфізичних системах критичної інфраструктури Чернявський С.С. (НА ВСУ) 23. Інтелектуальна мультиагентна архітектура кіберзахисту з адаптивним сценарним реагуванням у цифровій економіці Лисецький Ю.М. (ДУ «КАІ»)
27.08	*Виїзне засідання у Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут (ВІТІ)*

	1. Варіант перетворення сигналів стохастичних флуктуацій у бітову послідовності підвищеної ентропії для оцінки криптографічної стійкості Тлустий А.О. (ВІТІ) 2. Електричні кола як джерело витоку інформації в сучасних радіо-електронних системах Погребняк С.В. (ВІТІ) 3. Напрямки удосконалення керівних документів щодо організації захисту інформації в інформаційно-комунікаційному просторі Болотюк Ю.В. (ВІТІ) 4. Оцінка ефективності вогневого засобу при застосуванні системи автоматичної стабілізації Поляк І.Є. (ВІТІ) 5. Можливості використання штучного інтелекту для динамічного керування процесами модуляції та кодування Романенко В.В. (ВІТІ) 6. Обґрунтування вибору методу експертних оцінок для визначення надійності радіоелектронного обладнання в умовах обмеженої вхідної інформації Ланко А.В. (ВІТІ) 7. Автоматизація процесів обміну захищеною інформацією між структурними підрозділами військових формувань Лапа В.І. (ВІТІ) 8. Застосування середовища Pyton при організації процесу форсованих випробувань Мацаєнко А.М., Кузавков Г.В. (ВІТІ) 9. Методи захисту інформації в спеціальних інформаційно-комунікаційних системах Зарубенко А.О. (ВІТІ) 10. Методика ідентифікації пристроїв-генераторів псевдовипадкових послідовностей в інформаційно-комунікаційних системах Климович С.О. (ВІТІ)
10.09	1. Оцінка ефективності застосування фрактальних сигналів у генераторах радіозавад Петренко А.Б., Пепа Ю.В. (ДУІКТ) 2. Захист IoT-пристроїв на базі мікроконтролерів з підтримкою апаратного шифрування Рижаков М.М., Іванченко і.С. (ДУІКТ) 3. Застосування дискретного перетворення Фур'є для запобіганню витоку інформації матеріально-речовим каналом Котенко А.М. (ДУІКТ)
24.09	1. Моделювання блокуючого фільтру витоку інформації ланцюгами заземлення Пепа Ю.В. (ДУІКТ) 2. Забезпечення інформаційної безпеки приватного підприємства Німченко Т.В., Темніков В.О. (ДУІКТ) 3. Моделювання сигналів і шумів в інформаційних оптико-електронних системах Пепа Ю.В., Герасимчук В.С. (ДУІКТ)
15.10	1. Модель виявлення загроз на основі генеративно-змагальних мереж Вербіненко В.О., Зибін С.В. (ДУІКТ) 2. Методологія використання OSINT у виявленні кіберзагроз. Могилевич В.Д. (ІСЗЗІ КПІ ім. Ігоря Сікорського) 3. Особливості розробки цільових профілів безпеки інформаційно-комунікаційних систем в рамках авторизації систем з безпеки Загиней А.Ю. (ДУІКТ)

29.10	1. Комплексне управління інформаційною безпекою магістральних оптоволоконних мереж провайдерів 2. Криворучко О.В., Чорноус О.С. (НУБІП)Безпечна віртуалізація IT-інфраструктури ЗВО. Сучасний стан та перспективи розвитку Чорноус С.М., Касаткін Д.Ю. (НУБІП) 3. Вибір стратегій протистояння EDos атакам у рамках стохастичної диференціальної гри Лахно В.А. (НУБІП)
26.11	1. Огляд моделей поширення шкідливого програмного забезпечення в банківських додатках Грищук О.М. (Національний університет оборони України) 2. Кібербезпека криптовалют: теорія та практика Грищук Р.В. (Військова академія (м. Одеса)) 3. Розвинення теоретичних засад забезпечення кібербезпеки критичних інформаційно-керуючих систем на основі формальних методів і засобів Шкарупило В.В. (ІПМЕ) 4. Інструменти моделювання атак для виявлення вразливостей пов'язаних з соціальною інженерією Висоцька О.О. (КАІ), Давиденко А.М. (ІПМЕ)
24.12	Підсумкове засідання відділення семінару

ЛЬВІВСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Дудикевич В.Б.
Секретар: докт. техн. наук, професор Пархуць Л.Т.
Місце проведення семінару:
Національний університет «Львівська політехніка»,
м. Львів, вул. Князя Романа, 1, ауд. 202.

Початок роботи – 16^{00}

12.02	1. Авторизація користувачів через застосування доказів із нульовим розголошенням та технології блокчейн. Побережник В.О. (НУ «Львівська політехніка») 2. Розробка методології автоматизованої концепції перевірки відповідності стандартам кібербезпеки хмарної інфраструктури підприємства. Марценюк Є.В. (НУ «Львівська політехніка»)
12.03	1. From Agent Autonomy to Secure Governance: Implementing Security as Code with AI Agentic Framework for Kubernetes. Вахула О.П. (НУ «Львівська політехніка») 2. Аналіз API активностей і журналів подій за допомогою ML/NLP. Котляров О.Ю. (НУ «Львівська політехніка») 3. Комплексна архітектура системи захисту віртуальних мереж на основі інтеграції SIEM, EDR та SOAR-підходів. Абібулаєв А.Р. (НУ «Львівська політехніка»)
09.04	1. Безперервна перевірка стану системи: eBPF як сенсор в архітектурі нульової довіри. Глущенко П.К. (НУ «Львівська політехніка») 2. Preparing IT Infrastructure for the Quantum Age: Post-Quantum SSH. Воробець П.А. (НУ «Львівська політехніка») 3. Аналіз типових атак на бездротові системи з акцентом на атаки Replay/Relay. Лобан Г.А. (НУ «Львівська політехніка»)

14.05	1. Використання методів штучного інтелекту в автоматизованому тестуванні безпеки. Максимович М.В. (НУ «Львівська політехніка») 2. Удосконалення методології автоматизації тестування на проникнення за допомогою методів машинного навчання. Журавчак А.Ю. (НУ «Львівська політехніка») 3. Аналіз спектральних аномалій у просторі DCT(Discrete Cosine Transform) та інших частотних доменах Мединський О.Р. (НУ «Львівська політехніка»)
11.06	1. Інтелектуальна спостережуваність для багатохмарних DevOps-конвеєрів з використанням системного трасування та передбачуваного виявлення аномалій на основі eBPF та LLM. Журавчак Ю.Ю. (НУ «Львівська політехніка») 2. Способи виявлення обфускації шкідливого програмного коду за поєднанням статичних і поведінкових ознак. Четвертуха Н.Р. (НУ «Львівська політехніка») 3. Розробка моделі захисту інформації у відкритих джерелах на основі методу компартменталізації Івкова В.С. (НУ «Львівська політехніка»)
12.09	1. Розробка засобів організації політик і конфігурацій як основи технічного виконання вимог стандартів на різних рівнях IT-інфраструктури. Сведенюк О.В. (НУ «Львівська політехніка») 2. Методи виявлення медіаконтенту згенерованого штучним інтелектом. Джалюк Н.О. (НУ «Львівська політехніка»)
08.10	1. Аналіз переваг RBA фреймворку для виявлень атак APT. Опанович М.Ю. (НУ «Львівська політехніка») 2. Методи та засоби для обробки, локалізації та протидії цифровим протоколам керування безпілотними системами та наземними комплексами. Неділенко В.І. (НУ «Львівська політехніка») 3. Технологія знешкодження та реконструкції контенту як інструмент попередження прихованих загроз у моделі нульової довіри. Яцев А.В. (НУ «Львівська політехніка»)
12.11	1. Тенденції використання засобів штучного інтелекту для прогнозування кіберврразливостей. Єрьомкін М.М. (НУ «Львівська політехніка») 2. Аналіз стійкості стеганоалгоритмів у віртуальній реальності до виявлення нейронними мережами Гасілін Д.Л. (НУ «Львівська політехніка»)
10.12	1. Криптостійкий гібридний генератор псевдовипадкових послідовностей на основі нелінійних булевих функцій. Кіх М.В. (НУ «Львівська політехніка») 2. Архітектура системи тестування загроз у великих мовних моделях. Кольченко В.В. (НУ «Львівська політехніка»)
24.12	Підсумкове засідання відділення семінару

ОДЕСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Кобозєва А.А.
Вчений секретар: докт. техн. наук, професор Казакова Н.Ф.
Місце проведення семінару:
м. Одеса, Одеський національний морський університет,
вул. Мечникова, 34, Новий корпус, ауд.401.
м. Одеса, Одеський національний університет ім. І.І. Мечнікова,
вул. Всеволода Змієнка, 2, адм. корпус, ауд. 7
Початок роботи – 15^{00}

17.02	1. Врахуванням специфіки цифрових зображень, згенерованих за допомогою штучного інтелекту, в методі вибору стеганографічного контейнера. Сокальський С.О. (Національний університет «Одеська політехніка») 2. Використання теорії графів для забезпечення надійності сприйняття стеганоповідомлення при організації прихованого каналу зв'язку Кобозєва А.А. (ОНМУ) 3. Нормована відокремленість максимального сингулярного числа блоку цифрового зображення як показник доцільності його стеганоперетворення. Бобок І.І. (Національний університет «Одеська політехніка»)
14.04	1. Застосування недвійкових афінних перетворень для підвищення криптографічної якості S-блоків Соколов А.В., (Національний університет «Одеська юридична академія»), Радуш В.В. (Національного університету «Одеська політехніка») 2. Методологія статистичного випробування сучасних алгоритмів шифрування, призначених для обміну даними в розподілених комп'ютерних системах Щербина Ю.В. (Національний університет «Одеська юридична академія»)
29.05	1. Виявлення порушення цілісності відео послідовності в режимі реального часу Лебедєва О.Ю. (ОНМУ) 2. Виявлення обробки цифрових контентів засобами графічних редакторів Трифонова К.О. (ОНМУ)
26.09	1. Передумови дослідження ефективності застосування кількісної оцінки кіберживучості систем критичного призначення (Байєсівська Адаптація Біноміальної Схеми Випробувань) Казакова Н.Ф. (Одеський національний університет ім. І.І. Мечнікова) 2. Загальні проблеми селективної стеганографії Григоренко С.М. (Національний університет «Одеська політехніка»)
29.09	1. Метод виявлення фотомонтажу цифрового зображення на основі аналізу частотної області Яворська К.О. (ОНМУ) 2. Способи виявлення аномальної активності в інформаційних системах на основі гібридних моделей Big Data-аналітики Фразе-Фразенко О.О. (Одеський національного університету ім. І.І. Мечнікова) 3. Застосування машинного навчання для підвищення ефективності стеганографічного методу з кодовим управлінням Соколов А.В., Євдокимов Д.В. (Національний університет «Одеська юридична академія»)
01.12	1. Оцінка пропускної спроможності прихованого каналу зв'язку Бобок І.І. (Національний університет «Одеська політехніка») 2. Удосконалення теоретичних основ методів виявлення порушень цілісності цифрового зображення Зоріло, В.В. (ОНМУ)
15.12	Підсумкове засідання відділення семінару

ХАРКІВСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Євсеєв С.П.
Вчений секретар: докт. техн. наук, професор Олейніков А.М.
Місце проведення семінару:
Національний технічний університет «Харківський політехнічний інститут», м. Харків, вул. Кирпичова, 2, корпус У-2, Кіберполігон.

Початок роботи – 14^{00}

27.01	1. Моделі валідації вразливостей систем безпеки Денисюк В. М. (НТУ “ХПІ”) 2. Моделі забезпечення безпеки безперервності банківських бізнес-процесів Уманський О. Г. (НТУ “ХПІ”) 3. Моделі класифікації атак на об'єкти критичної інфраструктури Світличний Д. О. (НТУ “ХПІ”)
27.03	1. Моделі класифікації атак на нейронні мережі Дністровський В. В. (НТУ “ХПІ”) 2. Методи моніторингу об'єктів захисту інформації на основі технології Data Mining Литвиненко Б. В. (НТУ “ХПІ”)
24.04	1. Моделі та методи безпеки соціокіберфізичних систем Жигалов М.О. (НТУ “ХПІ” 2. Моделі та методи безпеки об’єктів смарт технологій” Печериця Д.В. (НТУ “ХПІ”)
29.05	1. Методологія синтезу моделі штучного інтелекту для систем в кібербезпеці Сокол В. Є. (НТУ “ХПІ”) 2. Методологія формування захисту системи спеціального зв’язку Томашевський Б. П. (НТУ “ХПІ”)
26.06	1. “Методи стеганографічного візуального захисту документів з обмеженим доступом” Сітченко О. А. (НТУ “ХПІ”) 2. Метод підвищення прихованості даних на основі LDPC-кодів Дунаєв С. В. (НТУ “ХПІ”) 3. Нейромережеві моделі багатоконтурних систем безпеки Трофименко Р. В. (НТУ “ХПІ”)
31.07	1. Методи виявлення вразливостей з урахуванням семантики засобами нейронних мереж Єграшин О. О. (НТУ “ХПІ”) 2. Нейромережеві методи виявлення шкідливого коду в операційних системах Лінукс Яшунін Ю. В. (НТУ “ХПІ”)
28.08	1. Метод підвищення автентичності даних в смарт технологіях Стеценко В.О. (НТУ “ХПІ”) 2. Методи виявлення атак на системи штучного інтелекту Хоменко І. О. (НТУ “ХПІ”)
25.09	1. Моделі обміну особистими даними на основі блокчейну Букатич І.В. (НТУ “ХПІ”) 2. Моделі динаміки трафіку для виявлення кібератак Кудрявцев Є. І. (НТУ “ХПІ”)
30.10	1. Розробка методів код-безкодових виявлень інформаційно-психологічних впливів Валєєв В. А. (НТУ “ХПІ”)

	2. Розробка методів інформаційної скритності в технологіях 6G Вегієв Р. С. (НТУ “ХПІ”)
27.11	1. Нейромережева система кіберзахисту mesh IoT-мереж з криптоавтентифікацією вузлів Верколаб Г. С. (НТУ “ХПІ”) 2. Методи захисту нейронних мереж від ворожих атак у системах штучного інтелекту Євсеєв Д. С. (НТУ “ХПІ”) 3. Розробка багатоконтурної системи захисту в технологіях 6G Пасько О. І. (НТУ “ХПІ”)
18.12	1. Моделі комплексної системи захисту інформаційних ресурсів в інтернет-сервісах Кальницький Д. В. (НТУ “ХПІ”) 2. Моделі безпеки взаємодії агентів у соціокіберфізичних системах Покаліцин В. В. (НТУ “ХПІ”)
18.12	Підсумкове засідання відділення семінару

ТЕРНОПІЛЬСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Касянчук М.М.
Вчений секретар: канд. техн. наук, доцент Загородна Н.В.
Місце проведення семінару:
Західноукраїнський національний університет,
м. Тернопіль, вул. О.Теліги, 8, кафедра кібербезпеки;
Тернопільський національний технічний університет імені Івана Пулюя,
м. Тернопіль, вул. Руська, 56, кафедра кібербезпеки.

Початок роботи – 14^{00}

15.01	1. Механізм капсулювання ключа (KEM) на основі криптосистеми McEliece-RRNS. Яцків В.В. (ЗУНУ) 2. Ефективні алгоритми факторизації для криптографічних перетворень. Івасьєв С.В. (ЗУНУ) 3. Методи та засоби криптографічного захисту інформації на основі ієрархічної СЗК. Якименко І.З. (ЗУНУ)
19.02	1. Методика оцінки якості безпеки вебдодатку. Загородна Н.В. (ТНТУ) 2. Оцінювання ризиків безпеки кібер-фізичних систем. Козак Р.О., Скоренький Ю.Л. (ТНТУ) 3. Виклики в галузі кібербезпеки. Карпінський М.П. (ТНТУ)
12.03	1. Афінні шифри в системі залишкових класів. Голембйовський М.П., Касянчук М.М. (ЗУНУ) 2. Методи та засоби криптографічного захисту інформації на основі поліноміальної СЗК. Якименко І.З. (ЗУНУ) 3. Алгоритми захисту від фішингових атак. Бабала Л.В., Сапіташ В.І., Рибінський В.О. (ЗУНУ)
16.04	1. Виявлення аномалій у мережевому трафіку методами штучного інтелекту. Стадник М.А. (ТНТУ)

	2. Програмні засоби "приманка" для дослідження аномалій в інфраструктурі організації. Козак Р.О., Лобур Т.Б. (ТНТУ) 3. Внутрішній аудит інформаційної безпеки: методи, етапи та оцінка ефективності. Лечаченко Т.А. (ТНТУ)
14.05	*Виїзне засідання у Тернопільський національний педагогічний університет імені Володимира Гнатюка (м. Тернопіль, вул. Винниченка, 10, кафедра інформатики та методики її навчання)* 1. Проєктування захищених і стійких інформаційних систем. Лень А.В., Шмигер Г.П. (ТНПУ) 2. Хмарні інфраструктури й кібербезпека: технічні механізми захисту даних у розподілених системах. Іваницький Р.І. Вовкодав О.В. (ТНПУ) 3. Захист інформації в умовах розвитку штучного інтелекту: технічні ризики та нові вектори кіберзагроз. Карабін О.Й., Мартинюк С.В. (ТНПУ) 4. Порівняльний аналіз сучасних бібліотек гомоморфного шифрування для безпечних хмарних обчислень. Кулина С.В. (ЗУНУ)
18.06	1. Алгоритми виявлення та реагування на інциденти для систем моніторингу безпеки. Нетребяк М.Р. (ЗУНУ) 2. Методи і засоби шифрування даних на основі афінного перетворення базисних чисел системи залишкових класів. Момотюк О.В., Касянчук М.М. (ЗУНУ) 3. Розробка вебзастосунку на основі системи аналізу технік і тактик крипто атак. Марчук С.І. (ЗУНУ)
17.09	1. Автоматизована ідентифікація клікабельних фішингових елементів в UI1. Ярема О.М. (ТНТУ) 2. Застосування методів симуляції в задачах кібербезпеки: переваги та обмеження. Козак Р.О. (ТНТУ) 3. Витік даних через помилки та приховані елементи у об'єктних моделях вебсторінок. Загородна Н.В., Ярема О.М. (ТНТУ)
15.10	1. Методи побудови асиметричних криптосистем в області комплексних чисел. Алілуйко А.М., Дзюбановська Н.В. (ЗУНУ) 2. Постквантове анаморфне шифрування: методи та інтеграція в KEM. Яцків В.В. (ЗУНУ) 3. Технології багатовимірної атрибуції загроз на основі OSINT-розвідданих. Бараннік Б.О., Цубера О.М., Царьков А. (ЗУНУ)
12.11	1. Захист від атак на структуру нейронної мережі. Карпінський М.П. (ТНТУ) 2. Авторизація з безпеки ІКС особливості та виклики. Лечаченко Т.А. (ТНТУ) 3. Шифрування в системі залишкових класів: тенденції досліджень та майбутні виклики. Касянчук М.М. (ЗУНУ)
10.12	1. Методи та інструменти доказу з нульовим розголошенням на основі СЗК. Цаволик Т.Г. (ЗУНУ)

	2. Механізми впливу, техніки реалізації та методи оцінювання ефективності соціоінженерних атак. Давлетова А.Я. (ЗУНУ) 3. Python-орієнтована бібліотека для пошуку квадратичних лишків у криптосистемі Рабіна. Бабала Л.В., Висоцький А.М. (ЗУНУ)
22.12	Підсумкове засідання відділення семінару.

ХМЕЛЬНИЦЬКЕ ВІДДІЛЕННЯ

Керівник: докт. техн. наук, професор Говорущенко Т.О.
Вчений секретар: канд. техн. наук, доцент Кльоц Ю.П.
Місце проведення семінару:
Хмельницький національний університет,
м. Хмельницький, вул. Інститутська, 11/1, ХНУ, навчальний корпус № 4, ауд. 4-239.

Початок роботи – 15^{00}

14.01	1. Муляр І.В. Використання IoT для приховування даних у потоках сенсорів з використанням стеганографії. 2. Білоус П.Р. Метод дослідження мережевої топології через графічну модель потоків даних та визначення критичних вузлів для формування політик безпечної маршрутизації. 3. Дрозд А.І.Метод виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів 4. Лисий А.М.Метод захисту спеціалізованих комп'ютерних систем від несанкціонованого вторгнення
11.02	1.Петляк Н.С. Модель автоматизованого пошуку вразливостей корпоративної мережі. 2.Багрій М.О. Метод виявлення та попередження вторгнень через динамічну адаптацію сигнатур. 3. Сєргєєв Є.В. Метод виявлення вразливостей в програмному забезпеченні комп'ютерних систем 4. Бохонько О.О. Метод ідентифікації кібератак соціальної інженерії
11.03	1.Пирч О.В. Методи та особливості виявлення аномалій у мережевому трафіку малої інтенсивності. 2.Купчик Н.С. Модель управління ризиками кібербезпеки фінансової організації з автоматичною побудовою мапи загроз. 3. Віжевський П.В. Метод виявлення витоку даних в корпоративних мережах згідно еволюційних алгоритмів 4. Семенюк Б.В. Метод виявлення комп'ютерних атак в корпоративних мережах
08.04	1.Тітова В.Ю. Технологія автоматизації щоденних зведених звітів про мережеві події та інциденти, які мають вплив на рівень захищеності корпоративної мережі. 2.Савченко С.В. Модель аудиту конфігурацій безпеки хмарної платформи Google Cloud. 3. Паюк В.П. Метод самодіагностування мікроконтролерних вбудованих систем технологічних ліній 4. Стецюк Ю.В. Метод синтезу мультикомп'ютерних систем обліку даних з обмеженим доступом в корпоративних мережах
13.05	1.Кльоц Ю.П. Аналіз підходів до виявлення аномалій у трафіку ISP-мереж. 2.Вишневський Д.Я. Використання машинного навчання для прогнозування поведінки зловмисників у корпоративних мережах.

	3. Козельський О.В. Метод створення мультикомп'ютерних систем з подвійною аутентифікацією потоків даних в корпоративних мережах 4. Поплавський С.Ю. Метод виявлення зловмисного програмного забезпечення в мобільних пристроях
10.06	1. Чешун В.М. Метод розслідування кіберінцидентів у державних інформаційних системах. 2. Вовкович М.О. Модель виявлення фішингових доменів за допомогою аналізу DNS-запитів. 3. Глухенький О.А. Метод виявлення зловмисного програмного забезпечення в кіберфізичних системах 4. Аскеров В.В. Метод безпечного керування фінансовими даними на основі технології блокчейн 5. Лигун О.О. Метод виявлення зловмисних дроперів в комп’ютерних системах
08.07	1. Інноваційні практики побудови комплексних систем захисту інформації у зв'язку із змінами вимог нормативних документів Держспецзв'язку. Зарицька О.А. (Хмельницький національний університет) 2. Застосування блокчейн-технологій для забезпечення цілісності журналів аудиту безпеки. 3. Чернов С.В. (Хмельницький національний університет) 4. Качур А.В. Метод забезпечення безпеки систем доданої реальності 5. Клейн О.М. Метод організації великих даних в масивах з компактним індексом
12.08	1. Мостовий С.В. Аналіз вразливостей протоколів динамічної маршрутизації. 2. Нігловський О.О.Інструменти моніторингу витоку конфіденційних даних у відкритих джерелах. 3. Продеус М.С. Метод виявлення й ідентифікації кібератак, спрямованих на порушення доступності у мережах Інтернету речей 4. Ковальчук В.К. Інформаційна технологія виявлення вразливостей в комп’ютерних системах 5. Прокоф'єв І.Г. Інформаційна технологія аналізу та оцінювання якості програмного коду з використанням компонентів штучного інтелекту
09.09	1. Стецюк М.В. Метод виявлення багатовекторних атак за допомогою графових нейронних мереж у IoT мережах. 2. Волинець Є.І. Моделювання поведінки користувачів для підвищення ефективності систем багатофакторної автентифікації. 3. Сорочинський О.Ю. Інформаційна технологія виявлення зловмисних кодів у програмному забезпеченні 4. Головко І.Г. Інформаційна технологія захисту вихідного коду з використанням штучного інтелекту 5. Денисюк Д.О. Інформаційна технологія виявлення аномальних кодів в фото-об’єктах вебресурсів
14.10	1. Анікін В.А. Метод побудови багатошарової симетричної криптосистеми із застосуванням сталих криптографічних примітивів. 2. Берчук В.В. Метод побудови політик доступу у хмарних середовищах із застосуванням Zero Trust Architecture. 3. Олійник П.Г. Метод оцінювання захищеності даних та інформації в корпоративних мережах 4. Шудрик А.О. Метод забезпечення безпеки інформації в корпоративних мережах 5. Гуральник О.Б. Метод оброблення критичної інформації в корпоративних мережах
11.11	1. Джулій В.М. Метод виявлення дезінформації за допомогою OSINT-інструментів.

	2. Чорненький С.В. Порівняння засобів глибинного аналізу трафіку (DPI) для ідентифікації зловмисних потоків у мережах провайдерів. 3. Возний К.Ю. Методи синтезу мереж інтелектуальних приманок і пасток для виявлення комп'ютерних атак 4. Головатюк А.О. Метод виявлення поліморфного програмного забезпечення бот-мереж в комп'ютерних системах 5. Марценков О.І. Метод виявлення аномалій в мережному трафіку комп'ютерних систем
09.12	1. Петрушак В.С. Вимірювання характеристик шумоподібного сигналу від РЕП на основі ГКН. 2. Мельник М.М. Методи виявлення аномального трафіку на рівні вузлів маршрутизації мереж провайдерів. 3. Мартинюк Д.В. Метод синтезу ізольованих середовищ для виявлення мережних вірусів 4. Ісаєв Т.С. Метод автоматичного оновлення моделей виявлення загроз в комп'ютерних системах
23.12	Підсумкове засідання відділення семінару.

ЧЕРНІГІВСЬКЕ ВІДДІЛЕННЯ

Керівник: докт. пед. наук, професор Ткач Ю.М.
Вчений секретар: канд. техн. наук, доцент Петренко Т.А.
Місце проведення семінару:
Національний університет «Чернігівська політехніка»,
м. Чернігів, вул. Шевченка 95, корп. 1, ауд. 106.

Початок роботи – 15^{00}

29.01	1. Безпека смарт-контрактів у мережі Ethereum Ващенок Д. (НУ «Чернігівська політехніка») 2. Використання ШІ як додаткового помічника у запобіганні та ліквідації повторних кібератак Вертебний І. (НУ «Чернігівська політехніка») 3. Рішення для виявлення витоку даних (DLP): практичне застосування Symantec DLP та McAfee Total Protection Дятел І. (НУ «Чернігівська політехніка») 4. Методи наукового аналізу вразливостей інформаційних систем при проведенні Penetration Testing. Райчинець О. (НУ «Чернігівська політехніка»)
26.02	1. Аналіз механізмів протидії дезінформаційним кампаніям в українському кіберпросторі в умовах гібридної війни Калінін В. (НУ «Чернігівська політехніка») 2. Аналіз вразливостей REST API у сучасних веб-застосунках. Комар В. (НУ «Чернігівська політехніка») 3. Аналіз механізмів SQL-атак та програмна реалізація методів запобігання їм у веб-додатках Корнієнко А. (НУ «Чернігівська політехніка») 4. Організація моніторингу інформаційної безпеки за допомогою IBM QRadar Зінченко О. (НУ «Чернігівська політехніка»)
26.03	1. Реалізація протоколу Zero Trust з використанням Azure AD Conditional Access Малько В. (НУ «Чернігівська політехніка»)

	2. Аналіз, виявлення та мінімізація ризиків, пов'язаних із помилками конфігурації в управлінні ідентифікацією та доступом (IAM) у хмарних середовищах AWS Масановець Ю. (НУ «Чернігівська політехніка») 3. Аналіз вразливостей і методів захисту пристроїв IoT у побутовому середовищі Мотузка Б. (НУ «Чернігівська політехніка») 4. Застосування LLM у кіберзахисті Бакун Б. (НУ «Чернігівська політехніка»)
30.04	1. Забезпечення безпеки в AWS із використанням AWS Security Hub і GuardDuty Нехай О. (НУ «Чернігівська політехніка») 2. Ризики розвитку штучного інтелекту: виклики та стратегії протидії Одноколов В. (НУ «Чернігівська політехніка») 3. Аналіз основних загроз інформаційній безпеці у корпоративних мережах Озява О. (НУ «Чернігівська політехніка») 4. Психологічні моделі маніпуляції в онлайн-комунікації. Ткач Ю. (НУ «Чернігівська політехніка»)
28.05	1. Дослідження ефективності алгоритмів AES, ChaCha20 та RSA у захисті мобільних застосунків Попсуй П. (НУ «Чернігівська політехніка») 2. Система менеджменту інформаційної безпеки підприємства Величко В. (НУ «Чернігівська політехніка») 3. Дослідження когнітивних алгоритмів перебудови частоти у MATLAB на базі USRP B210 Семендяй С. (НУ «Чернігівська політехніка») 4. Формування культури інформаційної безпеки підприємства як складової культури захищеності Сафронова О. (НУ «Чернігівська політехніка») 5. Використання Cisco SecureX для SOC-автоматизації Калашнікова Ю. (НУ «Чернігівська політехніка»)
25.06	1. Розробка програмного модуля для шифрування та захисту конфіденційних даних у хмарних середовищах Солопова Т. (НУ «Чернігівська політехніка») 2. Інструмент для виявлення вразливих місць у вебдодатку Супряга А. (НУ «Чернігівська політехніка») 3. AI-підхід до прогнозування кіберзагроз на основі поведінкових шаблонів користувачів Тимощенко І. (НУ «Чернігівська політехніка») 4. Використання архітектури Zero Trust в хмарних технологіях Содиль М. (НУ «Чернігівська політехніка»
24.09	1. Виявлення аномалій у мережевому трафіку з використанням алгоритмів машинного навчання Шеремет С. (НУ «Чернігівська політехніка») 2. Використання штучного інтелекту в забезпеченні інформаційної безпеки організацій Маринченко А. (НУ «Чернігівська політехніка») 3. Використанням Zero Trust-архітектури для захисту інформації в "хмарі" Руденок О. (НУ «Чернігівська політехніка») 4. Захист інформації в ІКС Носатенко Ю. (НУ «Чернігівська політехніка»)
29.10	1. Загрози та виклики кібербезпеки в епоху IoT Андрушко Д. (НУ «Чернігівська політехніка»)

	2. Технічні засоби виявлення та нейтралізації пристроїв несанкціонованого зняття інформації Євстаф'єв С. (НУ «Чернігівська політехніка») 3. Міграція до SASE: Вивчення шляхів відмови від застарілого мережевого периметра на користь хмарних рішень Запека І. (НУ «Чернігівська політехніка») 4. Комплексна система захисту інформації автоматизованої системи другого класу підприємства. Олексієнко О. (НУ «Чернігівська політехніка») 5. Психологічні моделі маніпуляції в онлайн-комунікації. Сикилідна Д. (НУ «Чернігівська політехніка»)
26.11	1. Система управління інцидентами ІБ підприємства. Кирієнко М. (НУ «Чернігівська політехніка») 2. Розгортання захищеної мережі за допомогою технічних засобів та технологій fortine Костенко Л. (НУ «Чернігівська політехніка») 3. Принципи роботи сучасних криптографічних шифраторів у системах захисту інформації. Лутченко В. (НУ «Чернігівська політехніка») 4. Система управління інформаційними ризиками на підприємстві Горбик Н. (НУ «Чернігівська політехніка»)
31.12	1. Використання ШІ в IP-телефонії для покращення клієнтського досвіду Медушенко В. (НУ «Чернігівська політехніка») 2. КСЗІ АС-1 Ридзель А. (НУ «Чернігівська політехніка») 3. Система захисту від атак на основі honeypot Свирид В. (НУ «Чернігівська політехніка») 4. Система менеджменту ІБ акціонерного банку Сургучов В. (НУ «Чернігівська політехніка»)
31.12	Підсумкове засідання відділення семінару.

План роботи семінару затверджений
науковою радою «Кібербезпека в енергетиці» НАН України
30 грудня 2025 року (протокол № 5)