



ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ



Назва курсу	<u>Методи штучного інтелекту для захисту інформації в комп'ютерних системах</u>
Викладачі	Лектор: Олексій СМІРНОВ доктор технічних наук, професор завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету https://kbpz.kntu.kr.ua/kafedra/smirnov-oleksii-anatoliiovych1 https://www.webofscience.com/wos/author/record/129613 https://www.scopus.com/authid/detail.uri?authorId=57208667815 https://scholar.google.com.ua/citations?user=-eNGlFoAAAAJ http://orcid.org/0000-0001-9543-874X https://www.researchgate.net/profile/Smirnov-Oleksii Асистент: Оксана КОНОПЛИЦЬКА-СЛОБОДЕНЮК викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету https://kbpz.kntu.kr.ua/kafedra/konoplitska-slobodenyuk-oksana-kostiantynivna https://scholar.google.com.ua/citations?user=I6VRWKcAAAAJ
Залучені розробники	Роман ТКАЧУК (Roman TKACHUK) Senior Systems Engineer at EPAM Ukraine

	Наталія КОЗИРОВА, інженер-програміст в ТОВ "Центр програмного забезпечення СОФТКОМ"
Контактний тел.	службовий: (0522)390-449 – робочі дні з 8³⁰ до 14²⁰ мобільні телефони / месенджери надано у описі курсу «Методи штучного інтелекту для захисту інформації в комп'ютерних системах» на сервері дистанційної освіти ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1029
E-mail:	smirnovoa@kntu.kr.ua konoplicka-slobodenyukok@kntu.kr.ua
Рівень вищої освіти	Доктор філософії (PhD)
Обсяг та ознаки дисципліни	Вибіркова навчальна дисципліна Змістових модулів – 2 Форма контролю: залік. Загальна кількість кредитів – 4, годин – 120. Формат: очний (offline / face to face) / дистанційний (online). Мова викладання: українська.
Консультації	Консультації проводяться відповідно до Графіку, розміщеному в інформаційному ресурсі moodle.kntu.kr.ua; у режимі відеоконференцій Zoom, через електронну пошту, месенджери за домовленістю.
Пререквізити	Враховуючи послідовність накопичення знань та інформації, дисципліна вивчається після викладання наступних дисциплін: «Інформаційні технології в науковій діяльності», «Математичне і комп'ютерне моделювання процесів та систем».

1. Мета і завдання дисципліни

Метою викладання дисципліни «Методи штучного інтелекту для захисту інформації в комп'ютерних системах» є формування у аспірантів набуття здатності продукувати нові ідеї, розв'язувати комплексні науково-прикладні задачі та/або проблеми в галузі професійної та/або дослідницько-інноваційної діяльності за рахунок застосування та/або розробки методів штучного інтелекту для захисту інформації в комп'ютерних системах у сфері комп'ютерних наук, що передбачає глибоке переосмислення наявних та створення нових цілісних знань професійної практики.

У результаті вивчення дисципліни аспірант повинен забезпечити наступні **результати навчання**: вміти реалізовувати побудову коректного експериментального протоколу для задачі кібербезпеки; порівнювати supervised та unsupervised підходів на CIC-IDS2017/UNSW-NB15; класифікувати шкідливе ПЗ за статичними ознаками з готового дата сету; генерувати evasion-атаки на власний детектор і оцінювати adversarial training; реалізовувати RAG-систему для аналізу інцидентів на основі бази знань MITRE ATT&CK; реалізовувати практичний red teaming: prompt injection та jailbreak на тестовій LLM-системі; детектувати синтетичний текст/аудіо: порівнювати методи.

2. Результати навчання

У результаті вивчення навчальної дисципліни аспірант повинен **знати**: Ландшафт загроз і методологія досліджень штучного інтелекту в кібербезпеці; Машинне навчання для виявлення вторгнень і аномалій; Аналіз шкідливого програмного забезпечення засобами глибокого навчання; Adversarial machine learning; LLM та агентні системи в SOC і threat intelligence; Безпека LLM-систем і red teaming; Генеративний штучний інтелект в атаках: дипфейки, фішинг, соціальна інженерія.

вміти: реалізовувати побудову коректного експериментального протоколу для задачі кібербезпеки; порівнювати supervised та unsupervised підходів на CIC-IDS2017/UNSW-NB15; класифікувати шкідливе ПЗ за статичними ознаками з готового дата сету; генерувати evasion-атаки на власний детектор і оцінювати adversarial training; реалізовувати RAG-систему для аналізу інцидентів на основі бази знань MITRE ATT&CK; реалізовувати практичний red teaming: prompt injection та jailbreak на тестовій LLM-системі; детектувати синтетичний текст/аудіо: порівнювати методи.

набути соціальних навичок (soft-skills):

- командна робота під час застосування та/або розробки методів штучного інтелекту для захисту інформації в комп'ютерних системах у сфері комп'ютерних наук;
- ефективна професійна комунікація;
- самостійне навчання та пошук технічної інформації;
- критичне мислення та аналіз технічних рішень;

- управління власним часом і планування виконання завдань;
- презентація та захист результатів виконаних проектів;
- відповідальність за якість програмного продукту та дотримання професійної етики.

3. Політика курсу та академічна доброчесність

Очікується, що аспіранти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення.

Під час освітнього процесу в Центральнотукаїнському національному технічному університеті аспіранти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення вибіркоких навчальних дисциплін та формування індивідуального навчального плану ЗВО; Кодексу академічної доброчесності ЦНТУ.

4. Програма навчальної дисципліни

Змістовний модуль 1. Ландшафт загроз і методологія досліджень ШІ в кібербезпеці. Машинне навчання для виявлення вторгнень і аномалій. Аналіз шкідливого ПЗ засобами глибокого навчання.

Лекція 1. Ландшафт загроз і методологія досліджень ШІ в кібербезпеці

Таксономії атак та захисту (MITRE ATT&CK, MITRE ATLAS, NIST AI RMF), огляд літератури, коректна постановка експерименту, метрики та типові методологічні помилки в наукових роботах (data leakage, нереалістичні датасети).

Лабораторна робота 1. Побудова коректного експериментального протоколу для задачі кібербезпеки.

Лекція 2. Машинне навчання для виявлення вторгнень і аномалій

IDS/NDR, supervised та unsupervised підходи, автоенкодери, часові ряди. Датасети (CIC-IDS2017, UNSW-NB15), дисбаланс класів, concept drift, проблема відтворюваності та розриву між лабораторними і реальними результатами.

Лабораторна робота 2. Порівняння supervised та unsupervised підходів на CIC-IDS2017/UNSW-NB15.

Лекція 3. Аналіз шкідливого ПЗ засобами глибокого навчання

Статичний і динамічний аналіз, представлення бінарних файлів та байт-кодів, графові неймережі для графів викликів, embedding-моделі для коду, кластеризація сімейств malware.

Лабораторна робота 3. Класифікація шкідливого ПЗ за статичними ознаками з готового датасету.

Змістовний модуль 2. Adversarial machine learning. LLM та агентні системи в SOC і threat intelligence. Безпека LLM-систем і red teaming. Генеративний ШІ в атаках: динфейки, фішинг, соціальна інженерія.

Лекція 4. Adversarial machine learning

Evasion-атаки, poisoning, backdoor у моделях, model extraction, membership inference. Методи захисту (adversarial training, certified robustness) та їх обмеження на прикладі детекторів шкідливого ПЗ і мережевого трафіку.

Лабораторна робота 4. Генерація evasion-атаки на власний детектор і оцінка adversarial training.

Лекція 5. LLM та агентні системи в SOC і threat intelligence

RAG для аналізу інцидентів, автоматизація triage, генерація правил Sigma/YARA, витяг IoC зі звітів, автономні агенти в захисті. Оцінка якості, галюцинації та довіра до висновків моделі.

Лабораторна робота 5 . RAG-система для аналізу інцидентів на основі бази знань MITRE ATT&CK.

Лекція 6. Безпека LLM-систем і red teaming

Prompt injection (прямий і непрямий), jailbreak, витік даних, OWASP Top 10 for LLM, безпека агентів з доступом до інструментів, методики та автоматизація red teaming, оцінка ризиків.

Лабораторна робота 6. Практичний red teaming: prompt injection та jailbreak на тестовій LLM-системі.

Лекція 7. Генеративний ШІ в атаках: дипфейки, фішинг, соціальна інженерія

Використання генеративних моделей зловмисниками, детекція синтетичного контенту (аудіо, відео, текст), водяні знаки та походження контенту (C2PA), обмеження сучасних детекторів.

Лабораторна робота 7. Детекція синтетичного тексту/аудіо: порівняння методів.

5. Критерії та засоби оцінювання

Методи контролю: спостереження за навчальною діяльністю аспірантів, усне опитування, тестовий контроль.

Форма підсумкового контролю: **залік**.

Критерієм успішного навчання є досягнення аспірантом мінімальних порогових рівнів оцінок за кожним результатом навчання.

Забезпечення об'єктивності оцінювання аспірантів здійснюється шляхом застосування накопичувальної системи нарахування балів оцінювання результатів навчання з кожної теми освітнього компоненту впродовж семестру та результатів підсумкового контролю.

Протягом семестру аспірант може отримати максимум 100 балів, у тому числі: перший рубіжний контроль – 50 балів, другий рубіжний контроль – 50 балів.

По поточному контролю аспірант може набрати бали за активність на лекційних заняттях, виконання лабораторної роботи, виявлення рівня підготовки аспірантів із зазначеної теми під час опитування, тестування, презентації індивідуальних завдань, вирішення практичних задач та кейсів тощо.

Підсумковий контроль у формі заліку передбачає підсумкову оцінку рівня досягнення програмних результатів навчання.

Схема нарахування балів з навчальної дисципліни

Змістовий модуль 1						Змістовий модуль 2								Залік	Сума
Т1		Т2		Т3		Т4		Т4		Т5		Т7			
Л1	ЛР1	Л2	ЛР2	Л3	ЛР3	Л4	ЛР4	Л5	ЛР5	Л6	ЛР6	Л7	ЛР7		
8	8	8	8	8	10	8	5	8	5	8	5	8	3		
50						50								0	100

Примітка: Т – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

Оцінювання результатів навчання з дисципліни здійснюється за кредитно-накопичувальною системою та проводиться за 100-бальною шкалою. Поточний контроль реалізується протягом семестру і передбачає систематичне оцінювання навчальної діяльності аспіранта. Він поділяється на два змістовні модулі, кожен з яких оцінюється максимально у 50 балів. У межах модулів враховується:

- робота аспіранта на лекційних заняттях;
- виконання та захист лабораторних робіт;
- рівень засвоєння теоретичного матеріалу.

Лабораторні роботи є обов'язковими складовими навчального процесу. До оцінювання допускаються лише ті роботи, які виконані в повному обсязі. Обов'язковою умовою є їх захист, під час якого аспірант повинен продемонструвати розуміння виконаних завдань, пояснити отримані результати та відповісти на запитання викладача.

Виконання лабораторних робіт повинно здійснюватися у встановлені терміни. Роботи, подані або захищені із запізненням без поважної причини, підлягають зниженню оцінки.

При незгоді аспіранта з поточною оцінкою, він може підняти свій бал на заліку Максимальна кількість балів за залік становить 40 балів. Залік передбачає перевірку:

- здатності застосовувати знання для розв'язання практичних завдань;
- розуміння основних понять і закономірностей дисципліни;
- здатності застосовувати знання для розв'язання практичних завдань;
- логічності, повноти та обґрунтованості відповідей.

Підсумкова оцінка з дисципліни визначається як сума балів, отриманих за два модульні рубежі (до 50 балів) та залік, при незгоді аспіранта з поточною оцінкою (до 40 балів).

Критерії оцінювання роботи на лекціях, здійснюється за накопичувальним принципом. За кожне лекційне заняття аспірант може отримати максимально 8 балів.

Максимальна кількість балів за лекцію	4
– підготовка до заняття (опрацювання теоретичного матеріалу)	+2
– участь в обговоренні	+2
– відповіді на запитання викладача	+4

Критерії оцінювання лабораторних робіт. Лабораторна робота оцінюється лише за умови її повного виконання та захисту. За кожну лабораторну роботу аспірант може отримати максимально 3, 5, 8 або 10 балів (в залежності від лабораторної роботи).

Максимальна кількість балів за лабораторну роботу	3	5	8	10
– високий рівень. завдання виконано повністю і без помилок, аспірант демонструє глибоке розуміння матеріалу, аргументовано пояснює результати, усно відповів на контрольні запитання, обґрунтував наукову складову	3	5	8	10
– достатній рівень. завдання виконано повністю, але наявні незначні помилки або неточності	2,25	3,75	6	7,5
– середній рівень. завдання виконано повністю, однак аспірант демонструє поверхнєве розуміння матеріалу	1,5	2,5	4	5
– низький рівень. робота виконана формально, без належного розуміння	0,75	1,25	2	2,5

При підсумовуванні балів, за наявності дробових значень, бали округляються у більший бік

Критерії оцінювання заліку. При незгоді аспіранта з поточною оцінкою, він може підняти свій бал на заліку Заліковий білет складається з 2-х теоретичних питань та одного практичного. Оцінювання відбувається наступним чином.

	Кількість балів
Не надана відповідь на жодне питання	0
Надана неповна відповідь тільки на одне питання	0-5
Надана повна відповідь тільки на одне питання	5-10
Надана неповна відповідь тільки на два питання	11-15
Надана повна відповідь на одне питання та неповна на друге	16-20
Надана неповна відповідь на три питання	16-20
Надана повна відповідь на одне питання та неповне на інші два	21-24
Надана повна відповідь на два питання та неповна на третє	25-29
Надана повна відповідь на всі три питання, але є певні погрішності	30-34
Надана повна відповідь на всі три питання	35
Надана повна відповідь на всі три питання та усна співбесіда з аспірантами, їх відповідями на додаткові запитання	36-40

Відповідність шкали оцінювання ЄКТС національній системі оцінювання визначена у розділі 8 Положення про організацію освітнього процесу в ЦНТУ: таблиця 1, стор. 33 www.kntu.kr.ua/file/content/424/polozhennia-pro-orhanizatsiyu-osvitnoho-protsesu-v-tsntu.pdf

Шкала оцінювання: національна та ЄКТС

Оцінка за шкалою ЄКТС	Визначення	Оцінка		
		За національною системою (екзамен, диф. залік, курс. проект, курс. робота, практика)	За національною системою (залік)	За 100 бальною шкалою ЦНТУ
A	ВІДМІННО – відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	Зараховано	90-100
B	ДУЖЕ ДОБРЕ – вище середнього рівня з кількома помилками	4 (добре)	Зараховано	82-89
C	ДОБРЕ – в загальному правильна робота з певною кількістю грубих помилок			74-81
D	ЗАДОВІЛЬНО – непогано, але зі значною кількістю недоліків	3 (задовільно)	Зараховано	64-73
E	ДОСТАТНЬО – виконання задовольняє мінімальні критерії			60-63
FX	НЕЗАДОВІЛЬНО – потрібно попрацювати перед тим, як перескласти	2 (незадовільно)	Незараховано	35-59
F	НЕЗАДОВІЛЬНО – необхідна серйозна подальша робота			1-34

6. Методичне забезпечення

1. Смірнов О.А., Коноплицька-Слободенюк О.К., Ткачук Р.О., Козірова Н.Л., Смірнова Т.В., Буравченко К.О., Смірнов С.А. «Методи штучного інтелекту для захисту інформації в комп'ютерних системах». Методичні вказівки до виконання лабораторних робіт для аспірантів денної форми навчання галузі F Інформаційні технології. – Кропивницький: ЦНТУ – 2025. – 34 с. Режим доступу:
2. Смірнов О.А., Коноплицька-Слободенюк О.К., Ткачук Р.О., Козірова Н.Л., Смірнова Т.В., Буравченко К.О., Смірнов С.А. «Методи штучного інтелекту для захисту інформації в комп'ютерних системах». Методичні вказівки до виконання контрольних робіт для аспірантів заочної форми навчання галузі F Інформаційні технології. – Кропивницький: ЦНТУ – 2025. – 34 с. Режим доступу:

7. Рекомендовані джерела інформації:

Основні

3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А., Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка. – К.: Видавничий центр “Кафедра”, 2025. – 320 с. ISBN 978-966-2711-74-5. Режим доступу: <https://opac.kntu.kr.ua/bib/9160> (бібліотека ЦНТУ)
4. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/12524>
5. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп’ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/9799>
6. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп’ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
7. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко – Львів: «Магнолія 2006». 2025 – 448 с. Режим доступу: <https://opac.kntu.kr.ua/bib/8739> (бібліотека ЦНТУ)
8. Основи формування державної системи кібернетичної безпеки: монографія / В.Л. Бурячок – Львів: «Магнолія 2006». 2025 – 432 с. Режим доступу: <https://opac.kntu.kr.ua/bib/8693> (бібліотека ЦНТУ)
9. Прикладні аспекти інформаційної та кібернетичної безпеки держави: Аналіз мережевого трафіку:: навч. посіб. / [Ю.В. Борсуковський, В.Ю. Борсуковська, В.Л. Бурячок та ін.]; М-во освіти і науки України, Університет Грінченка – Львів: «Магнолія 2006». 2025 – 222 с. Режим доступу: <https://opac.kntu.kr.ua/bib/8729> (бібліотека ЦНТУ)
10. Безпека вебдодатків: навч. посібн. / О.В. Пірог. – Електронні дані. – Житомир: Житомирська політехніка, 2025. – 290 с. Режим доступу: <https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8813/Пірог%20О.В.%20Безпека%20вебдодатків.%20Навчальний%20посібник-2025.pdf>
11. Етичний хакінг [Електронний ресурс]: навч.-практ. посібник / О. В. Мілов, О. В. Шматко, С. В. Мілевський, О. Г. Король; за заг. ред. С. П. Євсєєва. – Електрон. текст. дані. – Харків – Львів: "Новий Світ – 2000", 2025. – 100 с. – (Серія "Кібербезпека та штучний інтелект"). Режим доступу: <https://repository.kpi.kharkov.ua/handle/KhPI-Press/93087>

12. Безпека інформаційно-комунікаційних систем: підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. – Київ: Київський столичний університет імені Бориса Грінченка, 2025. – 1016 с. Режим доступу: <https://elibrary.kubg.edu.ua/id/eprint/51358/>
13. С. О. Кравчук «Протидія хакерським атакам в мобільних інфокомунікаціях». К.: НТУ «КПІ». 2025. 813 с.
14. Безпека Java-додатків: навчальний посібник / В. О. Любчак, В. В. Савостян, П. Д. Козолуп. – Суми: Сумський державний університет, 2023. – 72 с. Режим доступу: <https://essuir.sumdu.edu.ua/.../1234.../93738/1/Liubchak.pdf>
15. Основи операційних систем: навч. посібн. / О. С. Головня. – Електронні дані. – Житомир: «Житомирська політехніка», 2023. – 126 с. Режим доступу: <https://eztuir.ztu.edu.ua/.../%d0%93%d0%be%d0%bb%d0%be%d0...>
16. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. Режим доступу: <http://eztuir.ztu.edu.ua/123456789/8092>
17. Золотухіна О.А., Негоденко О.В., Резник С.Ю., Разіна С.Я.. «Якість та тестування інформаційних систем».К.: ДУТ. - 2020. Режим доступу: <https://duikt.edu.ua/ua/lib/1/category/2127/view/2177>
18. Горбань Г. В. Операційна система Linux: навч. посіб. / Г. В. Горбань, І. О. Кандиба. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2019. – 276 с. Режим доступу: <https://dspace.chmnu.edu.ua/jspui/handle/123456789/325>
19. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 p.
20. NIST AI Risk Management Framework (NIST AI 100-1, 2023) – Офіційний фреймворк від Національного інституту стандартів і технологій США для розробки, оцінки та управління ризиками штучного інтелекту. Режим доступу: <https://www.nist.gov/itl/ai-risk-management-framework>
21. MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) – База знань та матриця тактик і технік атак (з регулярно оновлюваним каталогом загроз для ML та LLM-систем). Режим доступу: <https://atlas.mitre.org/>
22. OWASP Top 10 for Large Language Model Applications (2023–2025) – Перелік критичних вразливостей систем на базі LLM (Direct/Indirect Prompt Injection, Sensitive Information Disclosure тощо). Режим доступу: <https://owasp.org/projects/top-10-for-large-language-model-applications>
23. C2PA Technical Specification v1.3 (2023) – Стандарт Coalition for Content Provenance and Authenticity щодо криптографічної перевірки походження цифрового контенту та боротьби з дипфейками. Режим доступу: https://c2pa.org/specifications/specifications/1.3/specs/C2PA_Specification.html
24. Ferrag, M. A., et al. (2024). Large Language Models for Cyber Security: A Systematic Literature Review. Режим доступу: <https://arxiv.org/abs/2405.04760>
25. Motlagh, F. A., et al. (2024). Large Language Models in Cybersecurity: State-of-the-Art. Режим доступу: <https://arxiv.org/abs/2402.00891>

26. Greshake, K., et al. (2023). Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. Режим доступу: <https://arxiv.org/abs/2302.12173>
27. Perez, F., & Ribeiro, I. (2022). Ignore This Title and Hack Them Instead: XRDS Survey on Prompt Injection Attacks. Режим доступу: <https://arxiv.org/abs/2211.09527>

Допоміжна

28. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105032602547>
29. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105026847051>
30. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105014300075>
31. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105014301897>
32. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., Imoize, A.L. «Advancing metaverse security with cryptographic innovations». *Advanced Metaverse Wireless Communication Systems*. pp 351-386. 2024 https://doi.org/10.1049/PBTE112E_ch13 **(Scopus)**. Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85217796661>
33. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241. Available: https://ceur-ws.org/Vol-3909/#Paper_18.pdf **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/85217281478>
34. Lakhno, V., Malyukov, V., Smirnov, O., Bebashko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *Smart Innovation, Systems and Technologies*, 2025. vol 389. pp 377-389. Springer, Singapore. https://doi.org/10.1007/978-981-97-2147-4_26

- (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85208027785>
35. Kuznetsov, O., Kuznetsova, Y., Frontoni, E., Arnesano, M., Smirnov, O. «Performance analysis of symmetric encryption algorithms for time-critical cybersecurity application». *CEUR Workshop Proceedings*, 3826, 2024. pp. 82-93. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85210258994>
36. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Hrebeniuk, A. «Smart contracts for automated compliance in healthcare cybersecurity». *Cybersecurity in Emerging Healthcare Systems*. 2024. pp. 263–303. https://doi.org/10.1049/PBHE064E_ch9. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85209979506>
37. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402. DOI: 10.1201/9781003457428-16. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85201885928>
38. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylanska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». *Lecture Notes on Data Engineering and Communications Technologies*, 2023. vol 180. Springer, Cham. pp. 288-298. https://doi.org/10.1007/978-3-031-36115-9_27 (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85188231470t>
39. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». *CEUR Workshop Proceedings*, 2023, 3628, pp. 93-105. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85184379056>
40. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». *CEUR Workshop Proceedings*, Volume 3624, 2023, pp. 330-339. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85184153182>
41. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85176927818>
42. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, KL., Vuppapalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85134768958>

43. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. **Springer**, Cham. 2022, pp. 2463-2477. **(Scopus)**. Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85109040660>
44. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346. **(Scopus)**. Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85096438116>
45. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136. **(Scopus)**. Режим доступу: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85086314545>
46. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Коноплицька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686. Режим доступу: <https://doi.org/10.28925/2663-4023.2026.34.1360> **(Фахове видання. Категорія «Б»)**
47. Смірнов, О., Ткачук, Р., Козірова, Н., Константинова, Л., Коноплицька-Слободенюк, О., Якименко, Н., Смірнов, С.. «Дослідження застосування векторних баз даних у генеративному штучному інтелекті». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 1 № 33, 667-682. Режим доступу: <https://doi.org/10.28925/2663-4023.2026.33.1248> **(Фахове видання. Категорія «Б»)**
48. Смірнов О., Заріцький В., Буравченко К., Коноплицька-Слободенюк О., Константинова Л., Якименко Н., Смірнов С. «Оптимізація розпізнавання облич за допомогою CUDA прискореної бібліотеки dlib». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 4, № 32, С. 573-582. Режим доступу: <https://doi.org/10.28925/2663-4023.2026.32.1154> <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/1154> **(Фахове видання. Категорія «Б»)**
49. Смірнова Т.В., Усік П.С., Лисенко І.А., Буравченко К.О., Смірнов О.А. «Методологія підтримки технологічних процесів у критичній інфраструктурі з забезпеченням безпеки інформації на основі хмарних технологій». *Безпека інформації*. 2025. Том 31 № 1. С. 49-60. Режим доступу: <https://doi.org/10.18372/2225-5036.31.20638> **(Фахове видання. Категорія «Б»)**
50. Смірнова Т.В., Буравченко К.О., Добринчук О.А., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. № 12(43), ч. II.

- С. 36-54. Режим доступу: [https://doi.org/10.32515/2664-262X.2025.12\(43\).2.36-54](https://doi.org/10.32515/2664-262X.2025.12(43).2.36-54) (Фахове видання. Категорія «Б»)
51. Лисенко, І., Минайленко, Р., Смірнов, С., Буравченко, К., Якименко, Н., Смірнов, О. «Дослідження інструментів штучного інтелекту для інтелектуального аналізу даних». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2025, № 3(31), С. 227–241. Режим доступу: <https://doi.org/10.28925/2663-4023.2025.31.1022> (Фахове видання. Категорія «Б»)
52. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025. DOI: 10.28925/2663-4023.2025.29.930. Режим доступу: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/930>
53. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448. Режим доступу: <https://doi.org/10.28925/2663-4023.2025.27.763> <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/763> (Фахове видання. Категорія «Б»)
54. Смірнова Т.В., Константинова Л.В., Коноплицька-Слободенюк О.К., Козлов Я.О., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження сучасного стану SIEM-систем». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2024. № 1(25), С. 6-18. Режим доступу: <https://doi.org/10.28925/2663-4023.2024.25.618> <https://csecurity.kubg.edu.ua/index.php/journal/article/view/646> (Фахове видання. Категорія «Б»)
55. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27. Режим доступу: <https://doi.org/10.28925/2663-4023.2024.24.627> <https://csecurity.kubg.edu.ua/index.php/journal/article/view/588> (Фахове видання. Категорія «Б»)
56. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131. Режим доступу: <https://doi.org/10.28925/2663-4023.2024.23.111131> <https://csecurity.kubg.edu.ua/index.php/journal/article/view/564> (Фахове видання. Категорія «Б»)
57. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Коноплицька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. *Кібербезпека: освіта,*

- наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87. Режим доступу: <https://doi.org/10.28925/2663-4023.2019.3.6387>. (Фахове видання).
58. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Коноплицька-Слободенюк О.К., Смірнова Т.В. GERT-моделі технології хмарного антивірусного захисту. Кібербезпека: освіта, наука, техніка. – Том 2 № 2. – Київ: КУ ім. Бориса Грінченка. – 2018. – С. 7-30. .Режим доступу: <https://doi.org/10.28925/2663-4023.2018.2.730>

Інформаційні ресурси

59. Курс «Методи штучного інтелекту для захисту інформації в комп'ютерних системах» на сервері дистанційної освіти ЦНТУ. – URL: <https://moodle.kntu.kr.ua/course/view.php?id=7125>
60. Онлайн-курси Coursera. – URL: <https://www.coursera.org>
61. Онлайн-курс «Основи машинного навчання та штучного інтелекту». – URL: <https://www.coursera.org/learn/fundamentals-of-machine-learning-and-artificial-intelligence>
62. Онлайн-курс «Генеративний штучний інтелект». – URL: <https://www.coursera.org/learn/introduction-to-generative-ai>
63. Онлайн-курс «Генеративний ШІ для всіх». – URL: <https://www.coursera.org/learn/ai-for-everyone>
64. Онлайн-курс «Безпека штучного інтелекту». – URL: <https://www.coursera.org/learn/ai-security>
65. Онлайн-курс «Дослідження варіантів використання та сфер застосування штучного інтелекту». – URL: <https://www.coursera.org/learn/exploring-artificial-intelligence-use-cases-and-applications>
66. Онлайн-курс «ШІ в національній безпеці: інтеграція штучного інтелекту в діяльність державного сектору». – URL: <https://www.coursera.org/learn/ai-national-security>
67. Академія Cisco. – URL: <https://www.netacad.com>
68. Он-лайн ресурс з кібербезпеки. – URL: <https://www.itsecurityguru.org/>
69. Он-лайн ресурс з кібербезпеки. – URL: <https://www.scmagazine.com/security-weekly-blog>
70. Он-лайн ресурс з кібербезпеки. – URL: <https://thehackernews.com/>
71. Он-лайн ресурс з кібербезпеки. – URL: <https://www.infosecurity-magazine.com/>
72. Он-лайн ресурс з кібербезпеки. – URL: <https://www.csoononline.com/>
73. Он-лайн ресурс з кібербезпеки. – URL: <https://www.tripwire.com/state-of-security>
74. Он-лайн ресурс з кібербезпеки. – URL: <https://www.schneier.com/>
75. Он-лайн ресурс з інформаційних технологій. – URL: <https://dou.ua/>
76. Пошукова система. – URL: <https://www.google.com/>
77. Он-лайн ресурс перегляду відеоуроків. – URL: <https://www.youtube.com>

