



**ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кафедра кібербезпеки та програмного забезпечення



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕОРІЯ ЗАХИСТУ ІНФОРМАЦІЇ

вибіркова дисципліна

другого рівня вищої освіти

Кропивницький

1. Загальна інформація

Назва дисципліни	Теорія захисту інформації
Розробники	Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету Скрипник Дмитро Анатолійович, спеціаліст з експлуатації програмних комплексів ІТ головного офісу / Адміністратор системи / Senior DevOps напрямку платіжні системи АТ КБ «Приватбанк» Коноплицька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Викладачі	Лектор – Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення, 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&hl=ru http://orcid.org/0000-0001-9543-874X https://www.researchgate.net/profile/Smirnov_Oleksii Асистент – Коноплицька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення, https://kbpz.kntu.kr.ua/kafedra/konopliitska-slobodenyuk-oksana-kostiantynivna?view https://scholar.google.com.ua/citations?user=I6VRWKcAAAAJ&hl=ru
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8 ³⁰ до 14 ²⁰ Мобільні телефони / Viber / Telegram надано у описі курсу «Теорія захисту інформації» на сервері дистанційної освіти ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1079
E-mail:	dr.smirnovoa@gmail.com ksuha80@gmail.com
Консультації	Очні консультації згідно розкладу консультацій Вівторок та Середа з 14 ²⁰ до 15 ⁴⁰ Онлайн консультації засобами електронної пошти, месенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Курс «Теорія захисту інформації» призначений для набуття теоретичних знань та практичних навичок з питань забезпечення захисту інформації. Включає в себе набуття наступних теоретичних знань: основні визначення та положення теорії захисту інформації; нормативно-правову базу щодо захисту інформації в Україні; стандарти у галузі захисту інформації; симетричну криптографію; несиметричну (асиметричну, з відкритим ключем) криптографію; генератори випадкових чисел; автентифікацію; геш-функції й коди автентифікації повідомлень – MAC; цифровий підпис; розподіл ключів; технічні засоби знімання й захисту інформації; криптоаналіз; введення в мережеву безпеку Інтернет; віруси й антивіруси; адміністративний рівень інформаційної безпеки; безпеку операційних систем; стеганографію; біометричні методи захисту інформації. Та набуття наступних практичних навичок й вмінь, які полягають у можливості програмно реалізовувати наступні проекти: База даних щодо

законів України стосовно захисту інформації; Симетричні алгоритми шифрування; Асиметричні алгоритми шифрування; Генератори псевдовипадкових чисел. Геш-функції; Автентифікація користувача і електронний цифровий підпис; Криптоаналіз; Програмні закладки. Клавіатурний шпигун. Стеганографія. Відповідно означене є предметом навчальної дисципліни «Теорія захисту інформації», як вибіркової освітньої компоненти другого (магістерського) рівня вищої освіти.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Теорія захисту інформації» є формування у здобувачів вищої освіти ґрунтовних теоретичних знань, практичних умінь та навичок, необхідних для застосування в професійній діяльності у сфері захисту інформації.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні **результати навчання**: вміти програмно реалізовувати наступні проекти: База даних щодо законів України стосовно захисту інформації; Симетричні алгоритми шифрування; Асиметричні алгоритми шифрування; Генератори псевдовипадкових чисел. Геш-функції; Автентифікація користувача і електронний цифровий підпис; Криптоаналіз; Програмні закладки. Клавіатурний шпигун. Стеганографія.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Денна форма навчання	Заочна форма навчання
	Кількість годин	Кількість годин
Кількість кредитів / годин	4/120	4/120
Кількість змістових модулів	2	2
Нормативна / вибіркова	вибіркова	вибіркова
Вид підсумкового контролю : залік	-	-

7. Технічне і програмне забезпечення / обладнання

Програмне забезпечення	Вільне ПЗ чи ні	Матеріально-технічне забезпечення
Ліцензійне офісне ПЗ: наявні у розпорядженні в ЦНТУ хмарні сервіси Microsoft 365: Word, Excel, PowerPoint, Outlook, хмарні служби для спільної роботи Microsoft Teams, OneDrive та ін.	ліцензія	Лекційні заняття проводяться у ауд. 500 обладнаною мультимедійним проектором Epson EB-X41. Лабораторні роботи виконуються у лабораторіях кафедри кібербезпеки та програмного забезпечення, (ауд 501, 505, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету.
OpenOffice, ліцензія LGPL,	вільне	
Google Chrome, ліцензія EULA	вільне	
Веб-портал «Законодавство України», https://zakon.rada.gov.ua/	вільне	
Веб-портал «Електронна бібліотека нормативних документів» http://online.budstandart.com/ua/catalog/klassifikator-minregionstroya/10_dstu_derzhavnyi_23691.html	вільне	
Веб-портал «Стандарти ISO/IEC» https://www.iso.org/standards.html	вільне	
SQLPro Studio https://apps.microsoft.com/store/detail/sqlpro-studio/9N621PXMDBGMB?hl=uk-ua&gl=ua	вільне	
Code::Blocks IDE, ліцензія GNU GPLv3 https://www.codeblocks.org/	вільне	
Mono C#, ліцензія GPL, LGPL, MIT https://www.mono-project.com/	вільне	
Visual Studio Community 2022, Ліцензійна угода: https://visualstudio.microsoft.com/ru/license-terms/vs2022-ga-community/ Мови програмування: C#, Visual Basic, F#, C++, HTML, JavaScript, TypeScript, Python та інші. https://visualstudio.microsoft.com/vs/community/	вільне	

8. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : <http://www.kntu.kr.ua/doc/dobro.pdf>

На першій лекції здобувачам освіти доводяться положення Статті 42. Академічна доброчесність, Закону України «Про освіту»

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральнотехнічному національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

9. Програма навчальної дисципліни

Тема 1. Нормативна база захисту інформації

Закон України «Про освіту». Стаття 42. Академічна доброчесність.

Основні визначення та положення теорії захисту інформації. Закон України (ЗУ) «Про інформацію». ЗУ «Про науково-технічну інформацію». ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах». ЗУ «Про доступ до публічної інформації». ЗУ «Про державну таємницю». ЗУ «Про основні засади забезпечення кібербезпеки України». Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.

Загрози, яким підлягає інформація. Стратегії реалізації загроз. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту.. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки. Основні принципи побудови систем захисту безпеки.

Нормативно-правова база щодо захисту інформації в Україні. Статі Кримінального кодексу, які передбачують покарання за розголошення таємниці. Нормативно-правові акти, що регламентують діяльність Держспецзв'язку за сферами. Стандарти у галузі захисту інформації

Тема 2. Сучасні алгоритми криптографії

Симетрична криптографія. Фактори від яких залежить безпека, забезпечувана традиційною криптографією . Области застосування. Платформи. Додаткові вимоги. Мережа Фейштеля. DES. ДСТУ 28147:2009. AES. ДСТУ 7624:2014 (Калина).

Несиметрична (асиметрична, з відкритим ключем) криптографія. Основні вимоги до алгоритмів асиметричного шифрування. Основні способи використання алгоритмів з відкритим ключем. Алгоритм RSA. Алгоритм Діффі-Хеллмана. ДСТУ 4145:2002

Тема 3. Генератори випадкових чисел та автентифікація

Генератори випадкових чисел. Вимоги до випадкових чисел. Джерела випадкових чисел. Генератори псевдовипадкових чисел. Криптографічно створені випадкові числа. Режим Output Feedback DES. ANSI X9.17. ДСТУ ISO/IEC 18031:2015. ДСТУ ISO/IEC 20543:2021

Автентифікація. Протоколи автентифікації. Використання симетричного шифрування. Протокол Нидхема й Шредера. Протокол Деннинга. Протокол автентифікації з використанням квитка. Використання шифрування з відкритим ключем. Протокол автентифікації з використанням автентифікаційного сервера. Протокол автентифікації з використанням KDC. Однобічна автентифікація. Використання симетричного шифрування. Використання шифрування з відкритим ключем. ДСТУ ISO/IEC 9798:2015

Тема 4. Геш-функції, MAC-коди та цифровий підпис.

Геш-функції й коди автентифікації повідомлень – MAC.

Геш-функції. Вимоги до геш-функцій. Прості геш-функції. Криптоаналіз геш-функцій. Використання ланцюжка зашифрованих блоків. SHA-1 і MD5. SHA-2. SHA-3. ДСТУ 7564:2014 (Купина). ДСТУ ISO/IEC 10118:2015.

Коди автентифікації повідомлень – MAC. Вимоги до MAC. MAC на основі алгоритму симетричного шифрування. MAC на основі геш-функції. HMAC. ДСТУ ISO/IEC 9797:2015

Цифровий підпис. Вимоги до цифрового підпису. Прямі й арбітражні цифрові підписи. Технології арбітражного цифрового підпису. Симетричне шифрування, арбітр бачить повідомлення. Симетричне шифрування, арбітр не бачить повідомлення. Шифрування відкритим ключем, арбітр не бачить повідомлення. Стандарт цифрового підпису DSS. Стандарт цифрового підпису ДСТУ 4145-2002. ДСТУ ISO/IEC 14888:2019

Тема 5 Розподіл ключів та технічний захист інформації

Розподіл ключів. Алгоритми розподілу ключів з використанням третьої довіреної сторони. PKI. X.509. ДСТУ ISO/IEC 11770:2019. ISO/IEC 27099:2022

Технічні засоби знімання й захисту інформації. Методи й засоби несанкціонованого одержання інформації з технічних каналів отримання інформації. Засоби проникнення. Пристрої прослуховування приміщень. Пристрої для прослуховування проводових телефонних ліній. Методи й засоби підключення до проводових ліній зв'язку та віддаленого одержання інформації. Дистанційний спрямований мікрофон. Системи схованого відеоспостереження. Акустичний контроль приміщень через засоби проводового телефонного зв'язку. Перехоплення електромагнітних випромінювань. Методи прослуховування мобільного зв'язку.

Технічні методи й засоби захисту інформації. Класифікація технічних засобів захисту. Технічні засоби захисту території й об'єктів. Акустичні засоби захисту. Особливості захисту від радіозакладок. Захист ліній проводового зв'язку. Екранування приміщень. Захист від прослуховування мобільного зв'язку. СКУД. CCTV. Пожежна сигналізація

Тема 6. Криптоаналіз та мережева безпека

Криптоаналіз. Диференціальний і лінійний криптоаналіз. Атака "зустріч посередині". Атаки на варіанти зі зменшеним числом раундів.

Криптоаналіз блокових симетричних шифрів. Криптоаналіз AES.. Криптоаналіз ДСТУ 7624:2014 (Калина).

Криптоаналіз алгоритмів з відкритим ключем. Криптоаналіз RSA. Криптоаналіз систем на еліптичних кривих

Введення в мережну безпеку Інтернет. Віруси й антивіруси. Класи мережевих атак. Атаки, пов'язані з розсиланням вірусів, хробаків, кроликів, троянських коней. Атаки протоколів SMTP, IMAP, POP3 і NNTP. Атаки FTP, Telnet, Finger, TFTP. Атаки сканування. DoS/DDoS-атаки. Дефекти програмного забезпечення. Соціальна інженерія. Операційна система. Уразливості й латки. Наслідки заражень комп'ютерними вірусами. Класифікація вірусів. Методи захисту від шкідливих програм. Організаційні методи. Політика безпеки. Технічні методи. Класифікація антивірусів. Режим роботи антивірусів

Тема 7. Адміністрування, безпека операційних систем

Адміністративний рівень інформаційної безпеки. Політика безпеки. BS 7799 (ISO/IEC 17799/ ISO/IEC 27002). Програма безпеки. Синхронізація програми безпеки з життєвим циклом систем. ДСТУ ISO/IEC 27000.

Безпека операційних систем. Механізми безпеки Windows Server 2022. Механізми безпеки Windows 10/11

Тема 8. Стеганографія та біометрія

Стеганографія. Сучасне застосування стеганографії. Класифікація стегосистем. Безключові стегосистем. Стегосистеми із секретним ключем. Стегосистеми з відкритим ключем. Класифікація методів приховання інформації. Текстові стеганографи. Методи перекручування формату текстового документа. Синтаксичні методи. Семантичні метод. Методи генерації стеганограм. Приховання даних у зображенні й відео. Широкополосні методи. Статистичні методи. Методи перекручування. Структурні методи. Приховання інформації у звуковому середовищі. Статичні методи біометрії. Динамічні методи біометрії. ДСТУ ISO/IEC 24745:2015

10. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

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

Особливість методів контролю навчальної дисципліни полягає у проведенні на початку лабораторних робіт летючих контрольних робіт (5-10 хв.) по передуючому лекційному матеріалу для визначення поточного рівня знань здобувачів освіти.

Форма підсумкового контролю: залік.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Теорія захисту інформації» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт), для оцінювання якої призначається 100 балів, та заліку.

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті.

11. Рекомендована література

Базова

1. 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., Корчинський 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>
2. 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>
3. 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>
4. 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.
5. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дресєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с
6. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп’ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.
7. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
8. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп’ютерна інженерія». За ред. С.В. Кавуна. Гриф “Навчальний посібник” надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5760. – Кіровоград: КНТУ 2012. – 442 с.
9. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Основи захисту інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп’ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова Гриф “Навчальний посібник” надано у відповідності з листом Міністерства освіти і науки України від 16.12.2010 року № 1/11-11486. – Кіровоград: КНТУ 2011. – 322 с.

10. Смірнов О.А., Кузнецов О.О., Євсєєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5762. – Кіровоград: КНТУ 2012. – 315 с.
11. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/8855>
12. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.
13. Смірнов О.А., Кавун С.В., Коваленко О.В., Дреєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.
14. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 1.12.2011 року № 1/11-11258. – Кіровоград: КНТУ 2012. – 454 с.
15. Смірнов О.А., Коваленко О.В., Кожанова А.С., Левашко О.Л., Константинова Л.В. Основи системного програмування. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. Коваленка О.В., Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки України від 26.02.2013 року № 1/11-4368. – Кіровоград: КНТУ 2013. – 257с.
16. 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>
17. 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>
18. 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>
19. 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>
20. 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>
21. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзасва, М.В. Ворохоб. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 1016 с. Режим доступу: <https://elibrary.kubg.edu.ua/id/eprint/51358/>
22. С. О. Кравчук «Протидія хакерським атакам в мобільних інфокомунікаціях». К.: НТУ «КПІ». 2025. 813 с.
23. 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>

24. 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%...>
25. 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>
26. 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>
27. 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>
28. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 p.
29. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 p.
30. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.
31. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.
32. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
33. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
34. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
35. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
36. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
37. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p.
38. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
39. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
40. Alex Matrosov, Eugene Rodionov, Sergey Bratus. Rootkits and Bootkits. No Starch Press. 2019. 450 p.

Допоміжна

41. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224. **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105014300735>
42. 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>
43. 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>
44. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Kozhakhmetova, D. «Optimized Simulated Annealing for Efficient Generation of Highly Nonlinear S-Boxes». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 146-174 <https://doi.org/10.1201/9781003546153> **(Scopus)**. Режим доступу: <https://www.scopus.com/pages/publications/105010780501>

45. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Bekeshova, G. «Enhanced Cryptographic Security through Advanced S-Box Optimization: A Hybrid Heuristic Approach». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. pp. 56-78. <https://doi.org/10.1201/9781003546153> (Scopus). Режим доступа: <https://www.scopus.com/pages/publications/105010780521>
46. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Abduraimova, B. «Enhancing Cryptographic Strength: A Novel Approach to S-Box Generation Using Modified Simulated Annealing». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. pp. 79-116. <https://doi.org/10.1201/9781003546153> (Scopus). Режим доступа: <https://www.scopus.com/pages/publications/105010779198>
47. Kuznetsov, O., Derevianko, Y., Frontoni, E., Arnesano, M., Smirnov, O. «Factorial Representation of S-Boxes: A Novel Approach to Cryptographic Analysis and Optimization». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. pp. 117-145. <https://doi.org/10.1201/9781003546153> (Scopus). Режим доступа: <https://www.scopus.com/pages/publications/105010779619>
48. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Shaikhanova, A., Khruskov, B. «Innovative Cost Functions for Optimizing Cryptographic S-Box Generation». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. pp. 29-55. <https://doi.org/10.1201/9781003546153> (Scopus). Режим доступа: <https://www.scopus.com/pages/publications/105010780326>
49. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., Zvieriev, V. «Comparative Research on Cryptocurrency Efficiency: An Objective Analysis of Key Metrics». *International Journal of Computing* 23(4), 2024. pp. 563-573 <https://doi.org/10.47839/ijc.23.4.3755> (Scopus). Режим доступа: <https://www.scopus.com/pages/publications/85217945318>
50. Kuznetsov O., Frontoni E., Kuznetsova K., Smirnov O., Kostenko V. «Blockchain applications in metaverse environments: new horizons». *Advanced Metaverse Wireless Communication Systems*. pp. 255-293. 2024 https://doi.org/10.1049/PBTE112E_ch10 (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85217740464&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=f1a8fb668b59ee5fa9c1c2a3f49a1924
51. 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 доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85217796661&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=b347f7be578e3e35a904d816a59f23c4
52. 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 доступа: <https://www.scopus.com/pages/publications/85217281478>
53. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, 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&origin=resultslist>
54. 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&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=dc97f04b93df404b65e2af8016ee9afa
55. Kuznetsov, O., Poluyanenko, N., Frontoni, E., Arnesano, M., Smirnov, O. «Evolutionary approach to S-box generation: Optimizing nonlinear substitutions in symmetric ciphers». *CEUR Workshop Proceedings*, 3829, 2024. pp. 1-11. (Scopus). Режим доступа:

- https://www.scopus.com/record/display.uri?eid=2-s2.0-85210257663&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=f2d4a2b82c9c6fe62448854e25427c1b
56. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Hrebenuk, 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&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=934a7ca808348b5290ebfb9ee60896b0
57. 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&origin=resultslist>
58. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447. DOI: 10.1201/9781003457428-17 **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85201858596&origin=resultslist>
59. 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-s2.0-85188231470&origin=resultslist>
60. 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&origin=resultslist>
61. 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&origin=resultslist>
62. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, 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&origin=resultslist>
63. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85175701031&origin=resultslist&sort=plf-f>
64. 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, K.L., Vuppapapati, 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&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1,FEATURE_EXPORT_REDESIGN:1
65. 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 доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85109040660&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4efdd02a212c90c07ca42f56dcb309f2

66. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w> (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85131801425&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
67. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021*, Cracow, Poland, 22-25 September 2021. P. 414-418 (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85124794482&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=dbf957fe0a817be8dcfcce2557bb4f0d&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
68. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260. (Scopus). Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85124008010&origin=resultslist&sort=plf-f>
69. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020*, Kharkiv, 6 October 2020-9 October 2020, P. 358-362. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85114388319&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=030a5fa3ef0a593fa1705f0c73130f01
70. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings Volume 2805*, 2020, Pages 44-58. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85100870219&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=aaa2da42a20c8ce0a011a2f45fcf2acf
71. Smirnov O., Kuznetsov A., Potii O., Poluyanenko N., Stelnyk I., Mialkovsky D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096919335&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=612e931a8e3eb73102c95ce1ccc90d0d
72. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings. Volume 2740*, 2020, Pages 102-114. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096412796&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=feb5eedf8c0626618743ca09212f9cd6
73. 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 доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096438116&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=1e91df71a9e62824506812d4d2f72e33
74. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings Volume 2654*, 2020, Pages 122-131. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091266964&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4ec5a65377ecac53f41fcbfc796f1d95
75. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings Volume 2654*, 2020, Pages 1-14. (Scopus). Режим доступа: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091288576&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=e0ddd0fb568a6aa6581297e6d8a10f99

76. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. **Springer**, Cham. 2021, pp 66-84. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85090900682&origin=AuthorNamesList&txGid=f48206584d421b66d484d464eef6ae71>
77. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 *IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85087880477&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm>
78. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I., Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 *IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 166-171. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85087899476&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm>
79. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 *IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 172-177. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85087876353&origin=resultslist&sort=plf-f&src=s&sid=3b1b7490cfd07f8a6eb2e90ad30c8c6d&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=4&citeCnt=0&searchTerm>
80. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. **Springer**, Cham. 2021. pp 557-587. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85087208231&origin=resultslist&sort=plf-f&src=s&sid=c4094ccaebdad4549a0820b2d8742aa3&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm>
81. 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 доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85086314545&origin=resultslist&sort=plf-f&src=s&sid=4f00231d7103e01bb1909823c51f297e&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm>
82. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». *International Journal of Computer Network and Information Security (IJCNIS)*. Vol. 12, No. 3, 2020. PP.33-43. **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85086029655&origin=resultslist&sort=plf-f&src=s&sid=0b320faf9bef84b1358467c5f8080eff&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm>
83. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», *CEUR Workshop Proceedings Volume 2608*, 2020, Pages 646-660., **(Scopus)**. Режим доступа: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85085516340&origin=resultslist&sort=plf-f&src=s&sid=34535eee1c1d23f4f421db6a0c97e825&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm>

84. 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>
85. 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»**)
86. 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»**)
87. 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»**)
88. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98. Режим доступу: <http://journals.nupp.edu.ua/sunz/article/view/2615> (**Фахове видання. Категорія «Б»**)
89. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022. Режим доступу: <http://journals.khnu.km.ua/vestnik/?cat=65> (**Фахове видання. Категорія «Б»**)
90. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89. Режим доступу: <http://journals.nupp.edu.ua/sunz/article/view/2449/1918> (**Фахове видання. Категорія «Б»**)
91. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». *CEUR Workshop Proceedings Volume 2732*, 2020, Pages 214-227. Режим доступу: <http://ceur-ws.org/Vol-2732/20200214.pdf> (**Закордонне фахове видання**)
92. 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. <https://doi.org/10.28925/2663-4023.2019.3.6387> Режим доступу: http://nbuv.gov.ua/UJRN/cest_2019_3_7 (**Фахове видання**).
93. 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. <https://doi.org/10.28925/2663-4023.2018.2.730> .Режим доступу: http://nbuv.gov.ua/UJRN/cest_2018_2_3 63-87. <https://doi.org/10.28925/2663-4023.2019.3.6387>. Режим доступу: http://nbuv.gov.ua/UJRN/cest_2019_3_7

Методичне забезпечення

94. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А. «Теорія захисту інформації». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 (F) Інформаційні технології. – Кропивницький: ЦНТУ – 2025. – 61 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/12361>
95. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А. «Теорія захисту інформації». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 (F) Інформаційні технології. – Кропивницький: ЦНТУ – 2025. – 61 с. Режим доступу: <http://dspace.kntu.kr.ua/jspui/handle/123456789/12364>

Інформаційні ресурси

96. Курс «Теорія захисту інформації» на сервері дистанційної освіти ЦНТУ. – URL: <https://moodle.kntu.kr.ua/course/view.php?id=1079>
97. Онлайн-курси Prometheus. – URL: <https://prometheus.org.ua/>
98. Онлайн-курси Coursera. – URL: <https://www.coursera.org>
99. Академія Cisco. – URL: <https://www.netacad.com>
100. Он-лайн ресурс з інформаційних технологій. – URL: <https://habr.com>
101. Он-лайн ресурс з інформаційних технологій. – URL: <https://dou.ua/>
102. Пошукова система. – URL: <https://www.google.com/>
103. Он-лайн ресурс перегляду відеоуроків. – URL: <https://www.youtube.com>