ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВСТУП ДО КІБЕРБЕЗПЕКИ

Освітньо-професійна програма «Комп'ютерна інженерія»

першого рівня вищої освіти

за спеціальністю 123 Комп'ютерна інженерія

галузі знань 12 Інформаційні технології

Розглянуто на засіданні кафедри
Протокол №13 від 31 березня 2022 року

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Вступ до кібербезпеки**
Рік викладання	2022-2023 навчальний рік
Розробники	Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету Скрипник Дмитро Анатолійович, DevOps Engineer/DevSecOps Engineer (Security Engineer), MIF Projects Конопліцька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Викладач	Лектор – Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення, http://kbpz.kntu.kr.ua/smirnov-oleksii/ https://www.scopus.com/authid/detail.uri?authorId=57208667815 https://scholar.google.com.ua/citations?user=-eNGlFoAAAAJ&hl=ru https://publons.com/researcher/1753507/oleksii-smirnov/ http://orcid.org/0000-0001-9543-874X https://www.researchgate.net/profile/Smirnov_Oleksii Асистент – Конопліцька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення, http://kbpz.kntu.kr.ua/konoplickay-oksana/ 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 «Вступ до кібербезпеки» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=685
E-mail:	У описі курсу «Вступ до кібербезпеки» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=685
Консультації	*Очні консультації* згідно розкладу консультацій Вівторок та Середа з 14^{20} до 15^{40} *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger/Viber/Telegram) у робочі дні

2. Анотація дисципліни

Курс «Вступ до кібербезпеки» призначений для набуття теоретичних знань та практичних навичок з питань забезпечення кібербезпеки. Включає в себе набуття наступних теоретичних знань: законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки; міжнародні стандарти в галузі інформаційної та /або кібербезпеки; інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці; методи і засоби обробки інформації; операційні системи; моделі безпеки в інформаційній та/або кібербезпеці; захист інформації, що обробляється та зберігається в ІКС; програмні та програмно-апаратні комплекси ЗЗІ; відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; моніторинг процесів функціонування ІКС; механізми безпеки комп'ютерних мереж; проектування, створення, супровід КСЗІ; моделі загроз та моделі порушника; оцінка захищеності інформації в ІКС; управління

інформаційною та/або кібербезпекою; аудит інформаційної та/або кібербезпеки; симетричні криптосистеми; асиметричні криптосистеми; криптографічні протоколи; цифрова стеганографія; технічний захист інформації. Та набуття наступних практичних навичок й вмінь з кібербезпеки, для чого вміти: Розгортати операційну систему для проведення аудиту кібербезпеки комп'ютерних мереж та систем. Використовувати інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі. Досліджувати уразливості системи або мережі за допомогою спеціалізованого сканера уразливостей – Nessus. Визначати уразливості веб-ресурсів та веб-застосунків. Користуватися сканером уразливостей – Vega. Шукати уразливості та чуттєву інформацію у відкритих ресурсах за допомогою засобу Maltego. Користуватися сніферами. Користуватися засобом дослідження уразливостей безпровідних мереж Wi-Fi – Aircrack-ng. Розгортати pen-test станції. Підготовлювати до роботи Metasploit та postgresql. Збирати інформацію за допомогою Metasploit. Шукати уразливості за допомогою Metasploit. Користуватися енкодером. Експлоатувати уразливості. Користуватися пост-експлоатацією. Відповідно означене є предметом навчальної дисципліни «Вступ до кібербезпеки».

3. Мета і завдання дисципліни

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

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій**:

– Здатність застосовувати знання у практичних ситуаціях.

– Знання та розуміння предметної області та розуміння професії.

– Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

– Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

– Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

– Здатність застосовувати методи та засоби криптографічного та технічного захисту.

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 **програмні результати навчання**:

– готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки;

– розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем;

– виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.

– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій;

- розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;

- здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах;

– виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно-телекомунікаційних системах.

- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;

– забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

– виконувати розробку експлуатаційної документації на комплексів засобів захисту.

– вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

– проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки;

– забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;

– аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;

– аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації;

– виявляти небезпечні сигнали технічних засобів;

– вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами;

– визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;

– інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

– обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності;

– впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин	
Рекомендації щодо семестру вивчення	2022-2023 р. – 3 семестр 2022-2023 р. – 4 семестр	
Спеціальність	123 «Комп’ютерна інженерія»	
Кількість кредитів/годин	6/180	
Кількість змістових модулів	3 семестр – 2 модулі 4 семестр – 2 модулі	
Нормативна/вибіркова	вибіркова	
лекції	42	3 семестр – 28 4 семестр – 14
лабораторні	28	3 семестр – 14 4 семестр – 14
самостійна робота	80	3 семестр – 48 4 семестр – 32
Вид підсумкового контролю	3 семестр – залік. 4 семестр – екзамен – 30.	

7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, дисципліну краще вивчати після дисциплін: «Вища математика», «Базові методології та технології програмування».

8. Технічне і програмне забезпечення/обладнання

Програмне забезпечення	Вільне ПЗ чи ні	Матеріально-технічне забезпечення
OpenOffice версії 4.1.7, ліцензія LGPL,	вільне	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.
Google Chrome, версія 80.0.3987.162, 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	
Kali Linux ліцензія GNU GPL https://www.kali.org/	вільне	
VirtualBox версії 6.1.38 ліцензія GNU GPL 2 https://www.virtualbox.org/	вільне	
Nmap версії 7.93 https://nmap.org/	вільне	
Nessus версії 8.2.3 ліцензія: безкоштовно протягом 7 днів https://www.tenable.com/try	умовно вільне	
Vega ліцензія: безкоштовно https://subgraph.com/vega/	вільне	
Maltego версії 4.2.11 ліцензія: безкоштовна однорічна ліцензія Maltego для академічних і некомерційних дослідників https://www.maltego.com/academic-non-profit/	умовно вільне	
WireShark версії 3.7.1. ліцензія GNU GPL 2+ https://www.wireshark.org/	вільне	
Aircrack-ng версії 1.5.2. ліцензія GNU GPL https://aircrack-ng.org/	вільне	
Metasploit версії 6.0.1 ліцензія GNU GPL https://www.metasploit.com/	вільне	

9. 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: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському 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.

10. Навчально-методична карта дисципліни

3 семестр

Тиждень, дата, академічні години	Тема, основні питання *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Самостійна робота Завдання, обсяг годин	Вага оцінки	Термін виконання
Змістовний модуль 1. Українське та міжнародне законодавство в галузі інформаційної та /або кібербезпеки, методи і засоби обробки інформації, операційні системи, моделі безпеки							
Тиж.1 (за розкладом) (2 год.)	**Тема 1. Українське та міжнародне законодавство в галузі інформаційної та /або кібербезпеки** Закон України «Про освіту». Стаття 42. Академічна доброчесність. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки: (ЗУ про інформацію, 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.)	Лекція / *Face to face*	Презентація	[1-7] [31-40] [118]	Самостійно опрацювати матеріал: Розглянути законодавчо-нормативну базу, щодо забезпечення кібербезпеки в Україні. (2 год.)	4 бали	Самостійна робота до 2 тижня включно

Тиж.2 (за розкладом) (2 год.)	**Тема 1. Українське та міжнародне законодавство в галузі інформаційної та /або кібербезпеки** Міжнародні стандарти в галузі інформаційної та /або кібербезпеки: (Регламенти ЄС в галузі кібербезпеки. ДСТУ ISO 27001)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити міжнародні стандарти в галузі інформаційної та /або кібербезпеки (2 год.)	4 бали	Самостійна робота до 2 тижня включно
Тиж.1,2 (за розкладом) (2 год.)	**Тема 1.** Розгортання операційної системи для проведення аудиту кібербезпеки комп'ютерних мереж та систем	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Розгорнути операційну системи для проведення аудиту кібербезпеки комп'ютерних мереж та систем (3год.)	8 балів	Самостійна робота до 2 тижня включно
Тиж.3 (за розкладом) (2 год.)	**Тема 2. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці та методи і засоби обробки інформації** Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці. (Мережева модель OSI. Основні протоколи стеку TCP/IP. Віртуалізація (принципи, гіпервізори). Архітектура комп'ютерів.)	Лекція / *Face to face*	Презентація	[1-7] [9-12] [118]	Самостійно опрацювати матеріал: Дослідити інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці (2 год.)	4 бали	Самостійна робота до 4 тижня включно

Тиж.4 (за розкладом) (2 год.)	**Тема 2. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці та методи і засоби обробки інформації** Методи і засоби обробки інформації: (Економне кодування: кодування методом Шеннона-Фано, алгоритм Хаффмана. Завадостійкі коди: Принципи завадостійкого кодування. Основні характеристики завадостійких кодів. Класифікація завадостійких кодів. Математичний опис процесу кодування і декодування, Блочні лінійні коди. Коди Хеммінга, Циклічні коди. Укорочені циклічні коди. Коди Боуза-Чоудхурі-Хоквінгема. Коди Ріда-Соломона. Код Файра)	Лекція / *Face to face*	Презентація	[1-7] [17] [118]	Самостійно опрацювати матеріал: Дослідити методи і засоби обробки інформації (2 год.)	4 бали	Самостійна робота до 4 тижня включно
Тиж.3,4 (за розкладом) (2 год.)	**Тема 2.** Інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Розгорнути інструменти прихованого збору технічної інформації з комп'ютерної системи або мережі (3 год.)	8 балів	Самостійна робота до 4 тижня включно

Тиж.5 (за розкладом) (2 год.)	**Тема 3. Операційні системи та моделі безпеки в інформаційній та/або кібербезпеці** Операційні системи: (Архітектура операційних систем. Процеси і потоки в операційних системах. Керування пам'яттю в операційних системах. Файлові системи. Захисні механізми операційних систем (Unix, Windows Server 2022, Windows 10/11))	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити захисні механізми операційних систем (2 год.)	4 бали	Самостійна робота до 6 тижня включно
Тиж.6 (за розкладом) (2 год.)	**Тема 3. Операційні системи та моделі безпеки в інформаційній та/або кібербезпеці** Моделі безпеки в інформаційній та/або кібербезпеці: (ДСТУ ISO/IEC 15408. Модель порушника. Модель загроз. Модель вразливостей)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити моделі безпеки в інформаційній та/або кібербезпеці (2 год.)	4 бали	Самостійна робота до 6 тижня включно
Тиж.5,6 (за розкладом) (2 год.)	**Тема 3.** Дослідження уразливостей системи або мережі за допомогою спеціалізованого сканера уразливостей – Nessus	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Провести дослідження уразливостей системи або мережі за допомогою спеціалізованого сканера уразливостей – Nessus (3 год.)	10 балів	Самостійна робота до 6 тижня включно
Максимальна кількість балів за змістовим модулем 1						50 балів	

Змістовний модуль 2. Захист інформації, що обробляється та зберігається в ІКС, програмні та програмно-апаратні комплекси ЗЗІ, відновлення та моніторинг процесів функціонування ІКС, механізми безпеки комп'ютерних мереж, проектування, створення, супровід КСЗІ, моделі загроз та моделі порушника, оцінка захищеності інформації в ІКС							
Тиж.7 (за розкладом) (2 год.)	**Тема 4 Захист інформації, що обробляється та зберігається в ІКС, програмні та програмно-апаратні комплекси ЗЗІ** Захист інформації, що обробляється та зберігається в інформаційно-телекомунікаційних системах (ІКС): (Процедури ідентифікації, автентифікації, авторизації користувачів. Захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші). Резервування інформації та компонентів ІКС).	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити питання захисту інформації, що обробляється та зберігається в ІКС (2 год.)	4 бал	Самостійна робота до 8 тижня включно
Тиж.8 (за розкладом) (2 год.)	**Тема 4 Захист інформації, що обробляється та зберігається в ІКС, програмні та програмно-апаратні комплекси ЗЗІ** Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ): (Антивіруси, міжмережеві екрани. IDS, IPS. Системи контролю та управління доступом)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити програмні та програмно-апаратні комплекси ЗЗІ (2 год.)	4 бал	Самостійна робота до 8 тижня включно

Тиж.7,8 (за розкладом) (2 год.)	**Тема 4** Визначення уразливостей веб ресурсів та веб застосунків. Сканер уразливостей – Vega	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Визначити уразливості веб ресурсів та веб застосунків сайту http://kbpz.kntu.kr.ua/ за допомогою сканеру уразливостей – Vega (3 год.)	4 балів	Самостійна робота до 8 тижня включно
Тиж.9 (за розкладом) (2 год.)	**Тема 5. Відновлення та моніторинг процесів функціонування ІКС** Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження: (Організаційно-технічні заходи відновлення функціонування ІКС. Журнал аудиту подій. Політики резервного копіювання даних).	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Розглянути питання відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження (2 год.)	4 бал	Самостійна робота до 10 тижня включно
Тиж.10 (за розкладом) (2 год.)	**Тема 5. Відновлення та моніторинг процесів функціонування ІКС** Моніторинг процесів функціонування ІКС: (Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу. Система візуалізації та управління подіями (SIEM). Аналіз подій)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Розглянути питання моніторингу процесів функціонування ІКС (2 год.)	4 бал	Самостійна робота до 10 тижня включно

Тиж.9,10 (за розкладом) (2 год.)	**Тема 5.** Пошук уразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Провести пошук уразливостей та чуттєвої інформації у відкритих ресурсах за допомогою засобу Maltego (3 год.)	4 балів	Самостійна робота до 10 тижня включно
Тиж.11 (за розкладом) (2 год.)	**Тема 6. Механізми безпеки комп'ютерних мереж та проектування, створення, супровід КСЗІ.** Механізми безпеки комп'ютерних мереж: (Віртуальні приватні мережі (VPN). Протоколи автентифікації RADIUS. Протоколи SSL/TLS.)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити механізми безпеки комп'ютерних мереж (2 год.)	4 бал	Самостійна робота до 12 тижня включно
Тиж.12 (за розкладом) (2 год.)	**Тема 6. Механізми безпеки комп'ютерних мереж та проектування, створення, супровід КСЗІ.** Проектування, створення, супровід КСЗІ: (Проведення аудиту інформаційної безпеки (ІБ) та визначення її рівня на основі звіту з аудиту ризиків ІБ. Вибір методів та засобів забезпечення необхідного рівня ІБ)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити механізми проектування, створення, супровід КСЗІ. (2 год.)	4 бал	Самостійна робота до 12 тижня включно

Тиж.11,12 (за розкладом) (2 год.)	**Тема 6.** Сніфери	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Використовуючи сніффер Wireshark та інформацію з сайту anti-trojan.org/port_opened.html (можливо використовувати й інші ресурси, основним критерієм є актуальність інформації) побудуйте фільтр(захвату або відображення) для перехвату пакетів що можуть йти з шпигунського програмного забезпечення. Після проаналізуйте трафік у декількох мережах(мінімум три). Додайте у звіт інформацію про трафік який було отримано у кожній з мереж. Використовуючи Wireshark проаналізуйте трафік що генерує ваш комп'ютер при зверненні на популярні сайти (використовуйте фільтри, інформацію про них додайте у звіт, поясніть чому ви використали саме їх), ваші спостереження додайте у звіт. Використовуючи сніффер Etherape проаналізуйте зв'язки що виникають при зверненні вашого браузеру до популярних сайтів. Спостереження додайте у звіт. (3 год.)	4 балів	Самостійна робота до 12 тижня включно

Тиж.13 (за розкладом) (2 год.)	**Тема 7. Моделі загроз та моделі порушника та оцінка захищеності інформації в ІКС** Моделі загроз та моделі порушника: (Загальні визначення й поняття моделі загроз та моделі порушника. Загрози цілісності. Загрози доступності. Загрози конфіденційності. Загрози через технічні канали. Загрози через соціальну інженерію.)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити моделі загроз та моделі порушника (2 год.)	4 бал	Самостійна робота до 14 тижня включно
Тиж.14 (за розкладом) (2 год.)	**Тема 7. Моделі загроз та моделі порушника та оцінка захищеності інформації в ІКС** Оцінка захищеності інформації в інформаційно-телекомунікаційних системах (ІКС): (Концептуальна схема оцінки безпеки інформації. Кількісна та якісна оцінки безпеки інформації)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити механізми оцінки захищеності інформації в ІКС (2 год.)	4 бал	Самостійна робота до 14 тижня включно
Тиж.13,14 (за розкладом) (2 год.)	**Тема 7.** Засіб дослідження уразливостей безпровідних мереж Wi-Fi – Aircrack-ng	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Провести дослідження уразливостей безпровідних мереж Wi-Fi за допомогою Aircrack-ng (2 год.)	6 бали	Самостійна робота до 14 тижня включно
Максимальна кількість балів за змістовим модулем 2						50 балів	
Залік							

4 семестр

Тиждень, дата, академічні години	**Тема, основні питання** *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	**Форма діяльності (заняття) /формат**	**Матеріали**	**Література, інформаційні ресурси**	**Самостійна робота Завдання, обсяг годин**	**Вага оцінки**	**Термін виконання**
Змістовний модуль 3. Управління інформаційною та/або кібербезпекою, аудит інформаційної та/або кібербезпеки, симетричні криптосистеми							
Тиж.1,2 (за розкладом) (2 год.)	**Тема 8. Управління інформаційною та/або кібербезпекою** (Управління кіберінцидентами: Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів/кібератак. Управління ризиками в інформаційній та/або кібербезпеці: Загальна концепція управління ризиками ІБ. ISO/IEC 27005:2018, IEC 31010:2019, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30, NIST SP 800-137 (Ризики інформаційної безпеки. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику). Системи класу Incident Response Platform.)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити питання управління інформаційною та/або кібербезпекою (2 год.)	4 бали	Самостійна робота до 2 тижня включно
Тиж.1,2 (за розкладом) (2 год.)	**Тема 8.** Розгортання pen-test станції	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Розгорнути pen-test станцію (2 год.)	6 балів	Самостійна робота до 2 тижня включно

Тиж.3,4 (за розкладом) (2 год.)	**Тема 9. Аудит інформаційної та/або кібербезпеки** (Етапи проведення аудиту. Аудит на основі аналізу ризиків. Аудит на основі стандартів ІБ. Аудит на основі експертних досліджень ІС. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу.)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити питання аудиту інформаційної та/або кібербезпеки (2 год.)	4 бали	Самостійна робота до 4 тижня включно
Тиж.3,4 (за розкладом) (2 год.)	**Тема 9.** Підготовка до роботи Metasploit та postgresql	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Підготувати до роботи Metasploit та postgresql (2 год.)	6 балів	Самостійна робота до 4 тижня включно
Тиж.5,6 (за розкладом) (2 год.)	**Тема 10. Симетричні криптосистеми.** (Модель симетричної криптосистеми. Класичні методи шифрування: Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування. Блокові шифри: DES. AES. ДСТУ ГОСТ 28147-2009. ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість). Потокові шифри: RC4, STRUMOK. (ДСТУ 8845:2019) (довжина ключів, крипостійкість).)	Лекція / *Face to face*	Презентація	[1-7] [41-46] [118]	Самостійно опрацювати матеріал: Дослідити симетричні криптосистеми (2 год.)	4 бали	Самостійна робота до 6 тижня включно

Тиж.5,6 (за розкладом) (2 год.)	**Тема 10.** Збір інформації за допомогою Metasploit	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Зібрати інформацію за допомогою Metasploit (2 год.)	6 балів	Самостійна робота до 6 тижня включно
Максимальна кількість балів за змістовим модулем 3						30 балів	
Змістовний модуль 4. Асиметричні криптосистеми, криптографічні протоколи, цифрова стеганографія, технічний захист інформації							
Тиж.7,8 (за розкладом) (2 год.)	**Тема 11. Асиметричні криптосистеми.** (Модель асиметричної криптосистеми. Шифр RSA. Алгоритм Ель-Гамаля (EG). Генерація спільних секретів Діффі-Хеллмана (DH). Електронний цифровий підпис DSA. Криптографія на еліптичних кривих. Електронний цифровий підпис згідно ДСТУ 4145-2002.EC-DSA згідно ISO/IEC 15946-2)	Лекція / *Face to face*	Презентація	[1-7] [47-53] [118]	Самостійно опрацювати матеріал: Дослідити асиметричні криптосистеми (2 год.)	2 бали	Самостійна робота до 8 тижня включно
Тиж.7,8 (за розкладом) (2 год.)	**Тема 11.** Пошук уразливостей за допомогою Metasploit	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Знайти уразливості за допомогою Metasploit (2 год.)	6 балів	Самостійна робота до 8 тижня включно
Тиж.9,10 (за розкладом) (2 год.)	**Тема 12. Криптографічні протоколи.** (Протоколи захисту мережевого трафіку IPSec. Протоколи безпечної передачі даних прикладного рівня: https.)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити криптографічні протоколи (2 год.)	2 бали	Самостійна робота до 10 тижня включно

Тиж.9,10 (за розкладом) (2 год.)	**Тема 12.** Енкодери	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Використати енкодери для обходу захисту антивірусних програм (2 год.)	6 балів	Самостійна робота до 10 тижня включно
Тиж.11,12 (за розкладом) (2 год.)	**Тема 13. Цифрова стеганографія.** (Поняття цифрової стеганографії. Модель стеганосистеми та класифікація методів стеганографічного захисту. Основні вимоги до стеганосистеми. Відкриті, напівзакриті, закриті стеганосистеми. Поняття ЦВЗ, класифікація. Метод модифікації найменшого значущого біта та інші методи приховання даних у зображенні, відео та аудіо. Атаки на стеганосистеми).	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити методи та механізми цифрової стеганографії (2 год.)	2 бали	Самостійна робота до 12 тижня включно

Тиж.11,12 (за розкладом) (2 год.)	**Тема 13.** Експлоатація уразливостей	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Використати уразливість яка дає змогу віддаленої експлотації**.** Використати уразливість що дає змогу експлуатації уразливості на стороні клієнта. Додати у звіт відомості про уразливості що були використані**.** Додати у звіт відомості про можливості що були надані в результаті використання уразливостей. Додати у звіт рекомендації що до усунення цих уразливостей, та що до усунення можливості їх появи у майбутньому (2 год.)	6 балів	Самостійна робота до 12 тижня включно

Тиж.13 (за розкладом) (2 год.)	**Тема 14. Технічний захист інформації** (Технічні канали витоку інформації: Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Методи прослуховування мобільного зв'язку. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації. Методи та засоби технічного захисту інформації: Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами. Захист від прослуховування мобільного зв'язку. Система контролю та управління доступом (СКУД). Системи відеоспостереження. Пожежна сигналізація)	Лекція / *Face to face*	Презентація	[1-7] [118]	Самостійно опрацювати матеріал: Дослідити механізми технічного захисту інформації (2 год.)	2 бали	Самостійна робота до 14 тижня включно

Тиж.13,14 (за розкладом) (2 год.)	**Тема 14.** Пост-експлоатація	Лабораторна робота / *Face to face*	Методичні рекомендації	[116-118]	Самостійно опрацювати матеріал: Отримати скріншот віддаленої машини. Отримати права system на стороні системи клієнта. Виконати видалення логів подій на стороні системи клієнта. Налаштувати port-forwarding та влаштувати бекдор за допомогою NetCat. У звіті відобразити хід виконання роботи. Додати скріншоти, та вивід консолі (6 год.)	4 балів	Самостійна робота до 14 тижня включно
Максимальна кількість балів за змістовим модулем 4						30 балів	
	Підготовка до екзамену				30 год.		
Максимальна кількість балів за екзамен						40 балів	

11. 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 проведені на початку лабораторних робіт летючих контрольних робіт (5-10 хв.) по передуючому лекційному матеріалу для визначення поточного рівня знань здобувачів освіти.

Форма підсумкового контролю: 4 семестр – залік, 5 семестр – екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Вступ до кібербезпеки» 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 60 балів, та екзамену, максимальна оцінка за який складає 40 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Вступ до кібербезпеки»

3 семестр

Поточний контроль та самостійна робота																				
Змістовий модуль 1									Змістовий модуль 2											Залік	Сума
Т1			Т2			Т3			Т4			Т5			Т6			Т7				
Л1	Л2	ЛР1	Л3	Л4	ЛР2	Л5	Л6	ЛР3	Л7	Л8	ЛР4	Л9	Л10	ЛР5	Л11	Л12	ЛР6	Л13	Л14	ЛР7		
4	4	8	4	4	8	4	4	10	4	4	4	4	4	4	4	4	4	4	4	6		
50									50													100

4 семестр

Поточний контроль та самостійна робота														Екзамен	Сума
Змістовий модуль 3						Змістовий модуль 4									
Т8		Т9		Т10		Т11		Т12		Т13		Т14			
Л15	ЛР8	Л16	ЛР9	Л17	ЛР10	Л18	ЛР11	Л19	ЛР12	Л20	ЛР13	Л21	ЛР14		
4	6	4	6	4	6	2	6	2	6	2	6	2	4		
30						30								40	100

Примітка: Т1, Т2,…,Т14 – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для заліку – 4 семестр	для екзамену – 5 семестр
90-100	A	зараховано	відмінно
82-89	B		добре
74-81	C		
64-73	D		задовільно
60-63	E		
35-59	FX	не зараховано з можливістю повторного складання	незадовільно з можливістю повторного складання
1-34	F	не зараховано з обов'язковим повторним вивченням дисципліни	незадовільно з обов'язковим повторним вивченням дисципліни

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:

оцінку «відмінно» (90-100 балів, А) – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

– засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

– засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;

– вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;

– самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку « добре» (82-89 балів, В) – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

– має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

– під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, С) – заслуговує студент, який:

– в загальному роботу виконав, але відповідає на екзамені з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

– опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;

– ознайомлений з основною літературою, яка рекомендована програмою;

– допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує студент, який:

– володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку «незадовільно» (35 балів, F) – виставляється студенту, який:

– володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

– допускає грубі помилки при виконанні завдань, передбачених програмою;

– не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

12. Рекомендована література

Базова

1. Смірнов О.А., Конопліцька-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
2. 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.
3. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с
4. 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.

5. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
6. 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.
7. 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.
8. Смірнов О.А., Кузнецов О.О., Євсеєв 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.
9. Смірнов О.А., Конопліцька-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
10. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.
11. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.
12. Смірнов О.А., Євсеєв 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.
13. Смірнов О.А., Коваленко О.В., Кожанова А.С., Левошко 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.
14. Захист інформації в автоматизованих системах управління : навчальний посібник/Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
15. Остапов С. Е. Технологія захисту інформації : навчальний посібник/С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
16. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч./за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування/[О.М. Хоша ба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.
17. Абакумов, В. Г. Теорія інформації та кодування. Ч. 1 [Електронний ресурс] : навчальний посібник/В. Г. Абакумов ; НТУУ «КПІ». - Електронні текстові дані (1 файл: 3,42 Мбайт). – Київ : НТУУ «КПІ», 2011.
18. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 p.

19. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 p.
20. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.
21. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.
22. 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.
23. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
24. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
25. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
26. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
27. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p
28. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
29. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
30. Alex Matrosov, Eugene Rodionov, Sergey Bratus. Rootkits and Bootkits. No Starch Press. 2019. 450 p.
31. Закон України «Про інформацію».
32. Закон України «Про науково-технічну інформацію».
33. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
34. Закон України «Про доступ до публічної інформації».
35. Закон України «Про державну таємницю».
36. Закон України «Про основні засади забезпечення кібербезпеки України».
37. Закон України «Про оборону України».
38. Закон України «Про правовий режим воєнного стану».
39. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури.
40. Укази Президента України №151/2022 та №151/2022, якими введено в дію рішення Ради національної безпеки і оборони України від 18 березня "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану" та "Про нейтралізацію загроз інформаційній безпеці держави".
41. ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".
42. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри".
43. ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования".
44. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) "Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів".
45. ДСТУ 8845:2019 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення".
46. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри".
47. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".
48. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) "Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел".

49. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) “Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі”.
50. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.
51. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні”.
52. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) “Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих”.
53. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри”.
54. ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) “Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану геш-функцію”.
55. ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”.
56. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n-бітний блоковий шифр”.
57. ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції”.
58. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) “Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику”.
59. ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.
60. ДСТУ ISO/IEC 9798-2:2015 (ISO/IEC 9798-2:2008; Cor 3:2013, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування”.
61. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) “Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису”.
62. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію”.
63. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 5. Механізми, що використовують методи нульової обізнаності”.
64. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) “Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 6. Механізми, що використовують ручне передавання даних”.
65. ДСТУ ISO/IEC 11670-2:2015 (ISO/IEC 11670-2:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів”.
66. ДСТУ ISO/IEC 11670-3:2015 (ISO/IEC 11670-3:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів”.
67. ДСТУ ISO/IEC 11670-4:2015 (ISO/IEC 11670-4:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми , засновані на нестійких секретах”.

68. ДСТУ ISO/IEC 11670-5:2015 (ISO/IEC 11670-5:2008, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами”.
69. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT) “Інформаційні технології. Методи захисту. Генерування випадкових бітів”.
70. ДСТУ ISO/IEC 20543 “Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів”.
71. ДСТУ ISO/IEC 11670-2:2015 (ISO/IEC 11670-2:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів”.
72. ДСТУ ISO/IEC 11670-3:2015 (ISO/IEC 11670-3:2008; Cor 1:2009, IDT) “Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів”.
73. ДСТУ ISO/IEC 20085-1 “Методи захисту IT. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування”.
74. ДСТУ ISO/IEC 20085-2 “Методи захисту IT. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом’якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування”.

Допоміжна

75. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». *In: Rajakumar, G., Du, KL., Vuppalapati, 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 доступу: 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
76. 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&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4efdd02a212c90c07ca42f56dcb309f2
77. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85131801425&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
78. 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 доступу: 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
79. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85124008010&origin=resultslist&sort=plf-f
80. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85114388319&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=030a5fa3ef0a593fa1705f0c73130f01

81. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85100870219&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=aaa2da42a20c8ce0a011a2f45fcf2acf
82. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096919335&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=612e931a8e3eb73102c95ce1ccc90d0d
83. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85096412796&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=feb5eedf8c0626618743ca09212f9cd6
84. 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&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=1e91df71a9e62824506812d4d2f72e33
85. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091266964&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=4ec5a65377ecac53f41fcbfc796f1d95
86. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091288576&origin=SingleRecordEmailAlert&dgcid=raven_sc_author_ru_ru_email&txGid=e0ddd0fb568a6aa6581297e6d8a10f99
87. 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 доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85090900682&origin=AuthorNamesList&txGid=f48206584d421b66d484d464eef6ae71
88. 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 доступу: 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
89. 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 доступу: 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

90. 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 доступу: 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
91. 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 доступу: 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
92. 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&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
93. 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 доступу: 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
94. 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 доступу: 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
95. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85091704115&origin=AuthorNamesList&txGid=6047f73642b838afa9b36c54ad7e29d5
96. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85084440832&origin=resultslist&sort=plf-f&src=s&sid=78e9700b01a40be3c0799a1567340a7f&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=11&citeCnt=0&searchTerm
97. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083667464&origin=resultslist&sort=plf-f&src=s&sid=2b6a0139fad18bb19a964441b5bded76&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm

98. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083203878&origin=resultslist&sort=plf-f&src=s&sid=4e89c5e5e6bd68a6310e60ba77c04b42&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=10&citeCnt=0&searchTerm
99. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85083237488&origin=resultslist&sort=plf-f&src=s&sid=4e89c5e5e6bd68a6310e60ba77c04b42&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=9&citeCnt=0&searchTerm
100. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», *2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019).* 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85082664468&origin=resultslist&sort=plf-f&src=s&sid=5c53cd2ed9d68e904ea625555543d5f8&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm
101. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18 -21 September 2019. P.713-718. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077114956&origin=resultslist&sort=plf-f&src=s&sid=e66ec7ff6625e5acea5827784acaead6&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm
102. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019;* Metz; France; 18-21 September 2019. P. 707-712. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077116930&origin=resultslist&sort=plf-f&src=s&sid=e66ec7ff6625e5acea5827784acaead6&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=0&citeCnt=0&searchTerm.
103. Smirnov, O., Kuznetsov, A., Kiian, A., Babenko, B., Zhosan, H., Prokopovych-Tkachenko, D., «Soft Decoding Method for Turbo-Productive Codes», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019*, Lviv, Ukraine, 2-6 July, 2019, P. 129-134. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85073344541&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=1&citeCnt=0&searchTerm
104. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931997&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=2&citeCnt=0&searchTerm
105. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85069931008&origin=resultslist&sort=plf-

f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=3&citeCnt=0&searchTerm

106. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», *CEUR Workshop Proceedings* Volume 2353, CEUR-WS 2019, Pages 873-884. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85065482781&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=5&citeCnt=0&searchTerm

107. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-84938096221&origin=resultslist&sort=plf-f&src=s&sid=d686ad0e756d5334e61f7258a32f58c1&sot=autdocs&sdt=autdocs&sl=18&s=AU-ID%2857208667815%29&relpos=6&citeCnt=33&searchTerm

108. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування 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»)**

109. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування 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»)**

110. 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)**

111. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Смірнова Т.В., Конопліцька-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).**

112. Смірнов О.А., Смірнов С.А., Поліщук Л.І., Конопліцька-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

113. Смірнов О.А., Мелешко Є.В., Хох В.Д. Дослідження методів аудиту систем управління інформаційною безпекою. Системи управління, навігації та зв'язку. – Випуск 1 (41). – Полтава: ПолтНТУ. – 2017. – С. 38-42**.** Режим доступу: http://nbuv.gov.ua/UJRN/suntz_2017_1_12

114. Смирнов А.А., Смирнов С.А., Дидык А.К., Дреев А.Н. Способ контроля линий связи телекоммуникационной системы облачного антивируса. Способ контроля линий связи телекоммуникационной системы облачного антивируса. Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 121-127. Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_2_32

115. Смирнов А.А., Смирнов С.А. Дидык А.К., Дреев А.Н. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах. Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 36-39.Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/16443

Методичне забезпечення

116. Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнова Т.В., Буравченко К.О., Смірнов С.А. «Вступ до кібербезпеки». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 90 с.
117. Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнова Т.В., Буравченко К.О., Смірнов С.А. «Вступ до кібербезпеки». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 90 с.

Інформаційні ресурси

118. Курс «Вступ до кібербезпеки» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=685
119. Онлайн-курси Coursera. – URL: https://www.coursera.org
120. Академія Cisco. – URL: https://www.netacad.com
121. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
122. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
123. Пошукова система. – URL:https://www.google.com/
124. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com