ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕОРІЯ ЗАХИСТУ ІНФОРМАЦІЇ

Освітньо-професійна програма «Комп'ютерна інженерія»

другого рівня вищої освіти

за спеціальністю 123 Комп'ютерна інженерія

галузі знань 12 Інформаційні технології

кваліфікація Магістр з комп'ютерної інженерії

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

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Теорія захисту інформації**
Рік викладання	2022-2023 навчальний рік
Розробники	Смірнова Тетяна Віталіївна, кандидат технічних наук, доцент 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
Викладачи	Лектор – Смірнова Тетяна Віталіївна, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/2021/08/30/smirnova-tatiana/ https://www.scopus.com/authid/detail.uri?authorId=57219108044 https://scholar.google.com/citations?hl=ru&user=4t-bqj0AAAAJ https://orcid.org/0000-0001-6896-0612 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 «Теорія захисту інформації» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=631
E-mail:	У описі курсу «Теорія захисту інформації» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=631
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 «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 освітньої компоненти ОП «Комп'ютерна інженерія» 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.

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій магістра з комп'ютерної інженерії**:

– СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

– СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

– СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів

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**:

– РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.

– РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

– РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

– РН9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

– РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Денна форма навчання	Заочна форма навчання
	Кількість годин	Кількість годин
Рекомендації щодо семестру вивчення	1 семестр	1 семестр
Спеціальність	123 «Комп'ютерна інженерія»	123 «Комп'ютерна інженерія»
Кількість кредитів / годин	4/120	4/120
Кількість змістових модулів	2	2
Нормативна / вибіркова	вибіркова	вибіркова
лекції	28	4
лабораторні	14	2
самостійна робота	78	114
Вид підсумкового контролю : залік	-	-

7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, бажано отримання на першому (бакалаврському) рівні вищої освіти знань з наступних дисциплін: «Вища математика», «Алгоритми та методи обчислень», «Базові методології та технології програмування», «Бази даних», «Інженерія програмного забезпечення», «Системне програмне забезпечення», «Комп'ютерні мережі».

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	
SQLPro Studio https://apps.microsoft.com/store/detail/sqlpro-studio/9N621PXMDGBM?hl=uk-ua&gl=ua	вільне	
Code::Blocks IDE, версія 20.03, ліцензія GNU GPLv3 https://www.codeblocks.org/	вільне	
Mono C# версії 4.2, 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/ru/vs/community/	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

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. Нормативна база захисту інформації та криптографія							
Тиж.1 (за розкладом) (2 год.)	**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	Лекція / *Face to face*	Презентація	[1-6] [31]	Самостійно опрацювати матеріал: Дослідити нормативну базу захисту інформації. (4 год.)	4 бали	Самостійна робота до 2 тижня включно

Тиж.2 (за розкладом) (2 год.)	**Тема 1. Нормативна база захисту інформації** 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	Лекція / *Face to face*	Презентація	[1-6] [31]	Самостійно опрацювати матеріал: Дослідити нормативно-правову базу щодо захисту інформації в Україні. (4 год.)	4 бали	Самостійна робота до 2 тижня включно
Тиж.1,2 (за розкладом) 2 год.)	**Тема 1. Нормативна база захисту інформації** Закони України стосовно захисту інформації	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати БД нормативної бази захисту інформації. (3 год.)	8 балів	Самостійна робота до 2 тижня включно
Тиж.3 (за розкладом) (2 год.)	**Тема 2. Сучасні алгоритми криптографії** Симетрична криптографія. Фактори від яких залежить безпека, забезпечувана традиційною криптографією . Області застосування. Платформи. Додаткові вимоги. Мережа Фейштеля. DES. ДСТУ 28147:2009. AES. ДСТУ 7624:2014 (Калина).	Лекція / *Face to face*	Презентація	[7] [31]	Самостійно опрацювати матеріал: Застосування існуючих закордонних та українських сучасних симетричних алгоритмів шифрування (4 год.)	4 бали	Самостійна робота до 4 тижня включно
Тиж.4 (за розкладом) (2 год.)	**Тема 2. Сучасні алгоритми криптографії** Несиметрична (асиметрична, з відкритим ключем) криптографія. Основні вимоги до алгоритмів асиметричного шифрування. Основні способи використання алгоритмів з відкритим ключем. Алгоритм RSA. Алгоритм Діффі-Хеллмана. ДСТУ4145:2002	Лекція / *Face to face*	Презентація	[1-6] [31]	Самостійно опрацювати матеріал: Застосування існуючих закордонних та українських сучасних асиметричних алгоритмів шифрування (4 год.)	4 бали	Самостійна робота до 4 тижня включно

Тиж.3,4 (за розкладом) (2 год.)	**Тема 2. Сучасні алгоритми криптографії** Симетричні алгоритми шифрування.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Класичні алгоритми шифрування. (3 год.)	8 балів	Самостійна робота до 4 тижня включно
Тиж.5 (за розкладом) (2 год.)	**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	Лекція / *Face to face*	Презентація	[1-6] [31]	Самостійно опрацювати матеріал: Дослідити існуючі генератори випадкових чисел. (4 год.)	4 бали	Самостійна робота до 6 тижня включно
Тиж.6 (за розкладом) (2 год.)	**Тема 3. Генератори випадкових чисел та автентифікація** 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	Лекція / *Face to face*	Презентація	[1-6, 10] [31]	Самостійно опрацювати матеріал: Дослідити існуючі сучасні підходи до автентифікації (4 год.)	4 бали	Самостійна робота до 6 тижня включно

Тиж.5,6 (за розкладом) (2 год.)	**Тема 2. Сучасні алгоритми криптографії** Асиметричні алгоритми шифрування	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Застосування сучасних асиметричних алгоритмів шифрування. (3 год.)	10 балів	Самостійна робота до 6 тижня включно
Максимальна кількість балів за змістовим модулем 1						50 балів	
Змістовний модуль 2. Захист інформації в комп'ютерних мережах							
Тиж.7 (за розкладом) (2 год.)	**Тема 4. Ґеш-функції, MAC-коди та цифровий підпис**. Ґеш-функції й коди автентифікації повідомлень – MAC. Ґеш-функції. Вимоги до ґеш-функцій. Прості ґеш-функції. Криптоаналіз ґеш-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 ґеш-функції. HMAC. ДСТУ ISO/IEC 9797:2015	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів побудови ґеш-функцій й кодів автентифікації повідомлень – MAC (4 год.)	3 бали	Самостійна робота до 8 тижня включно

Тиж.8 (за розкладом) (2 год.)	**Тема 4. Ґеш-функції, MAC-коди та цифровий підпис**. 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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів цифрового підпису. (4 год.)	3 бали	Самостійна робота до 8 тижня включно
Тиж.7,8 (за розкладом) (2 год.)	**Тема 4. Ґеш-функції, MAC-коди та цифровий підпис**. Генератори псевдовипадкових чисел. Ґеш-функції.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Застосування сучасних генераторів псевдовипадкових чисел та ґеш-функцій. (3 год.)	6 балів	Самостійна робота до 8 тижня включно
Тиж.9 (за розкладом) (2 год.)	**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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Застосування розподілу ключів (4 год.)	3 бали	Самостійна робота до 10 тижня включно

Тиж.10 (за розкладом) (2 год.)	**Тема 5 Розподіл ключів та технічний захист інформації** 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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Застосування сучасних методів знімання та технічного захисту інформації (4 год.)	3 бали	Самостійна робота до 10 тижня включно

Тиж.9,10 (за розкладом) (2 год.)	**Тема 4. Ґеш-функції, MAC-коди та цифровий підпис**. Автентифікація користувача і електронний цифровий підпис	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Застосування електронного цифрового підпису для автентифікації користувачів (3 год.)	6 балів	Самостійна робота до 10 тижня включно
Тиж.11 (за розкладом) (2 год.)	**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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів криптоаналізу асиметричних алгоритмів на еліптичних кривих (4 год.)	3 бали	Самостійна робота до 12 тижня включно

Тиж.12 (за розкладом) (2 год.)	**Тема 6. Криптоаналіз та мережева безпека** 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. Режими роботи антивірусів	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Дослідження функцій сучасного антивірусу (4 год.)	3 бали	Самостійна робота до 12 тижня включно
Тиж.11,12 (за розкладом) (2 год.)	**Тема 6. Криптоаналіз та мережева безпека** Криптоаналіз.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Застосування алгоритмів криптоаналізу (3 год.)	6 балів	Самостійна робота до 12 тижня включно

Тиж.13 (за розкладом) (2 год.)	**Тема 7. Адміністрування, безпека операційних систем, стеганографія та біометрія.** 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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Формування та застосування політики безпеки (4 год.)	3 бали	Самостійна робота до 14 тижня включно

Тиж.14 (за розкладом) (2 год.)	**Тема 7. Адміністрування, безпека операційних систем, 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	Лекція / *Face to face*	Презентація	[6, 9] [31]	Самостійно опрацювати матеріал: Застосування методів стеганографії та методів біометрії (4 год.)	3 бали	Самостійна робота до 14 тижня включно
Тиж.13,14 (за розкладом) (2 год.)	**Тема 7. Адміністрування та стеганографія.** Програмні закладки. Клавіатурний шпигун. Стеганографія.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Застосування програмних закладок та клавіатурних шпигунів. Реалізація стеганографічних методів (4 год.)	8 бали	Самостійна робота до 14 тижня включно
Максимальна кількість балів за змістовим модулем 2						50 балів	
Максимальна кількість балів за заліку						0 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: 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, максимальна оцінка за який складає 0 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Теорія захисту інформації»

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	3	3	6	3	3	6	3	3	6	3	3	8		
50									50												0	100

Примітка: Т1, Т2,…,Т7 – 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
90-100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
1-34	F	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, A) – 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, B) – 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, C) – заслуговує студент, який:

– в загальному роботу виконав, але відповідає на заліку 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 заліку 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.

12. Рекомендована література

Базова

1. Смірнова Т.В., Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., 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., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.
4. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
5. 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.
6. 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.
7. 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.
8. 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.
9. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. 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.
11. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 с.
12. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 с.
13. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 с.
14. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 с.
15. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 с.
16. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 с.

Допоміжна

17. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399. **(Scopus)**. Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85133613188&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
18. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184. **(Scopus).** Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85118101973&origin=AuthorNamesList&txGid=9fba77a9424db54ff3b099e4400c22bb
19. Smirnova, T., Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and SystemsVolume 152, 2021, Pages 85-98. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85090914783&origin=resultslist
20. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., «Метод розрахунку критичності галузевих інформаційно-телекомунікаційних систем». *Наукоємні технології* № 2(54), 2022. С. 94-104. Режим доступу: https://jrnl.nau.edu.ua/index.php/SBT/article/view/16757 **(Фахове видання. Категорія «Б»)**
21. Смірнова Т.В., Гнатюк С.О., Юдін О.Ю., Сидоренко В.М., Жаксигулова Д.Д., «Експериментальне дослідження моделі розрахунку кількісного критерію оцінювання захищеності інформаційно-телекомунікаційних систем критичної інфраструктури держави» *Кібербезпека: освіта, наука, техніка*. № 4(16). 2022. С. 6-18. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/359/298 **(Фахове видання. Категорія «Б»)**
22. Смірнова Т.В., Якименко Н.М., Смірнов О.А., 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»)**
23. Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., Смірнов О.А. «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»**)
24. Смірнова Т.В., Якименко Н.М., Улічев О.С., Конопліцька-Слободенюк О.К., Смірнов С.А., «Дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Кібербезпека: освіта, наука, техніка*. № 3(15). С. 85-92. 2022. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/337 **(Фахове видання. Категорія «Б»)**
25. Смірнова Т.В., Бурмак Ю.А., Улічев О.С., Усік П.С., Доренський О.П., «Стійка функція шифрування удосконаленого модуля криптографічного захисту інформації в інформаційно-комунікаційних системах» *Кібербезпека: освіта, наука, техніка*. № 1(13). С. 183-201. 2021. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/346 **(Фахове видання. Категорія «Б»)**
26. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Бурмак Ю.А., Оспанова Д.М., «Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах». *Кібербезпека: освіта, наука, техніка*. № 2(14). С. 176-185. 2021. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/329 **(Фахове видання. Категорія «Б»)**

27. Смірнова Т.В., Смірнов О.А., Смірнов С.А., Поліщук Л.І., 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).**
28. Смірнова Т.В., Смірнов О.А., Смірнов С.А., Поліщук Л.І., Конопліцька-Слободенюк О.К.,. 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 **(Фахове видання).**

Методичне забезпечення

29. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнов С.А. «Теорія захисту інформації». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 53 с.
30. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнов С.А. «Теорія захисту інформації». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 53 с.

Інформаційні ресурси

31. Курс «Теорія захисту інформації» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=631
32. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
33. Онлайн-курси Coursera. – URL: https://www.coursera.org
34. Академія Cisco. – URL: https://www.netacad.com
35. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
36. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
37. Пошукова система. – URL:https://www.google.com/
38. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com