ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОГРАМНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Рівень вищої освіти другий (магістерський)
Галузь знань Інформаційні технології

Розглянуто на засіданні кафедри
Протокол №17 від 29 червня 2022 року

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Програмний захист інформації**
Рік викладання	2022-2023 навчальний рік
Викладач	Лектор – Смірнов Олексій Анатолійович, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення, http://kbpz.kntu.kr.ua/Смірнов-Олексій-Анатолійович 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/Конопліцька-Слободенюк-Оксана-Костя/ 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 «Програмний захист інформації» на сервері дистанційної освіти ЦНТУ.
E-mail:	У описі курсу «Програмний захист інформації» на сервері дистанційної освіти ЦНТУ.
Консультації	*Очні консультації* згідно розкладу консультацій *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Курс «Програмний захист інформації» призначений для набуття теоретичних знань та практичних навичок з питань забезпечення захисту інформації. Включає в себе: вивчення основних понять теорії захисту інформації; вивчення способів криптографічного перетворення інформації; отримання необхідних теоретичних знань побудови систем захисту інформації; отримання навиків адміністрування систем захисту інформації набуття практичних навичок з формування бази даних щодо законів України стосовно захисту інформації; реалізовувати симетричні алгоритми шифрування; реалізовувати асиметричні алгоритми шифрування; реалізовувати генератори псевдовипадкових чисел; реалізовувати ґеш-функції; реалізовувати автентифікацію користувача і електронний цифровий підпис; проводити криптоаналіз; реалізовувати програмні закладки; реалізовувати клавіатурний шпигун. Відповідно означене є предметом навчальної дисципліни «Програмний захист інформації» як освітньої компоненти ОП «Комп'ютерні науки» другого (магістерського) рівня вищої освіти.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Програмний захист 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'ютерних наук:

– ЗК13. Здатність спілкуватися з нефахівцями своєї галузі (з експертами з інших галузей)

– СК1: Знати принципи функціонування та технології віртуалізації серверних систем, архітектури та стандарти комунікаційних засобів розподілених обчислень, протоколи захисту інформації, яка циркулює в інформаційно-комунікаційних системах.

– СК2: Знати класифікацію хмарних обчислень на рівні систем та технологій , особливості та характерні ознаки звичайного хостингу веб-ресурсів, оренди віртуальних приватних машин та систем хмарних обчислень.

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:

– ПР1. Здатність формулювати та вирішувати дослідницьке завдання, для його вирішення збирати, оброблювати та систематизувати інформацію та формулювати висновки.–

– ПР4: Здатність робити презентації за професійною тематикою різного обсягу та складності рідною та іноземною мовами як для фахівців, так і для нефахівців.

– ПР 6: Здатність демонструвати знання з віртуалізації серверних систем, протоколів захисту інформації та використання отриманих знань у вирішенні практичних завдань.

– ПР7: Здатність демонструвати знання з існуючих математичних методів, алгоритмів обробки даних, методів оптимізації та їх використання для рішення професійних завдань, в тому числі для управління і прийняття управлінських рішень.

– ПР 8: Обізнаність у існуючих інформаційних технологіях для вирішення професійних задач фахівців у ІТ-галузі та здатність до їх обґрунтованого вибору, налаштування та подальшої експлуатації.

– ПР 13: Здатність ефективно працювати в групі, в тому числі і на лідерських позиціях з метою вирішення різноманітних дослідницьких та практичних завдань.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Рекомендації щодо семестру вивчення	1 семестр
Спеціальність	122 «Комп'ютерні науки»
Кількість кредитів / годин	4/120
Кількість змістових модулів	2
Нормативна / вибіркова	вибірковаа
лекції	28
лабораторні	14
самостійна робота	48
Вид підсумкового контролю : екзамен	30

7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, бажано отримання на першому (бакалаврському) рівні вищої освіти знань з наступних дисциплін: «Вища математика. Теорія ймовірності та математична статистика», «Алгоритми та методи обчислень», «Програмування», «Організація баз даних», «Інженерія програмного забезпечення», «Системне програмне забезпечення», «Комп'ютерні мережі».

8. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

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

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** Основні визначення та положення теорії захисту інформації. Закон України «Про інформацію». Основні принципи інформаційних відносин. Право на інформацію. Основні види інформації. Доступ до відкритої інформації. Інформація з обмеженим доступом. Закон України «Про державну таємницю». Закон України «Про захист інформації в автоматизованих системах». 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 . Основні принципи побудови систем захисту безпеки	Лекція / *Face to face*	Презентація	[1-5] [23]	Самостійно опрацювати матеріал: Дослідити нормативну базу захисту інформації. (2 год.)	2 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 Карного 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] [23]	Самостійно опрацювати матеріал: Дослідити нормативно-правову базу щодо захисту інформації в Україні. (2 год.)	2 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	[21, 23]	Самостійно опрацювати матеріал: Реалізувати БД нормативної бази захисту інформації. (3 год.)	6 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	Лекція / *Face to face*	Презентація	[6] [23]	Самостійно опрацювати матеріал: Застосування існуючих закордонних та українських сучасних симетричних алгоритмів шифрування (2 год.)	2 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	[1-5] [23]	Самостійно опрацювати матеріал: Застосування існуючих закордонних та українських сучасних асиметричних алгоритмів шифрування (2 год.)	2 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	[21, 23]	Самостійно опрацювати матеріал: Класичні алгоритми шифрування. (3 год.)	6 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	Лекція / *Face to face*	Презентація	[1-5] [23]	Самостійно опрацювати матеріал: Дослідити існуючі генератори випадкових чисел. (2 год.)	2 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	Лекція / *Face to face*	Презентація	[1-5, 9] [23]	Самостійно опрацювати матеріал: Дослідити існуючі сучасні підходи до автентифікації (2 год.)	2 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	[21, 23]	Самостійно опрацювати матеріал: Застосування сучасних асиметричних алгоритмів шифрування. (3 год.)	6 балів	Самостійна робота до 6 тижня включно
Максимальна кількість балів за змістовим модулем 1						30 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. . Вимоги до ґеш-функцій. Прості ґеш-функції. Криптоаналіз ґеш-функцій. Використання ланцюжка зашифрованих блоків. SHA-1 і MD5. SHA-2. ДСТ 3411. Коди автентифікації повідомлень – MAC. Вимоги до MAC. MAC на основі алгоритму симетричного шифрування. MAC на основі ґеш-функції. HMAC	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів побудови ґеш-функцій й кодів автентифікації повідомлень – MAC (2 год.)	1 бал	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 ДСТ 3410.	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів цифрового підпису. (2 год.)	1 бал	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	[21, 23]	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.	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Застосування розподілу ключів (2 год.)	1 бал	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 телефонних ліній. Методи й засоби підключення. Методи й засоби віддаленого одержання інформації. Дистанційний спрямований мікрофон. Системи схованого відеоспостереження. Акустичний контроль приміщень через засоби телефонного зв'язку. Перехоплення електромагнітних випромінювань. 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 зв'язку. Екранування приміщень	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Застосування сучасних методів зняття та технічного захисту інформації (2 год.)	1 бал	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	[21, 23]	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 алгоритмів з відкритим ключем. Криптоаналіз RSA	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Огляд існуючих алгоритмів криптоаналізу асиметричних алгоритмів на еліптичних кривих (2 год.)	1 бал	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	[5, 8] [23]	Самостійно опрацювати матеріал: Дослідження функцій сучасного антивірусу (2 год.)	1 бал	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	[21, 23]	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 та стеганографія.** Адміністративний рівень інформаційної безпеки. Політика безпеки. BS 7799:1995. Програма безпеки. Синхронізація програми безпеки з життєвим циклом систем	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Формування та застосування політики безпеки (2 год.)	1 бал	Самостійна робота до 14 тижня включно
Тиж.14 (за розкладом) (2 год.)	**Тема 7. Адміністрування та стеганографія.** 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	Лекція / *Face to face*	Презентація	[5, 8] [23]	Самостійно опрацювати матеріал: Застосування методів стеганографії (2 год.)	1 бал	Самостійна робота до 14 тижня включно
Тиж.13,14 (за розкладом) (2 год.)	**Тема 7. Адміністрування та стеганографія.** Програмні закладки. Клавіатурний шпигун	Лабораторна робота / *Face to face*	Методичні рекомендації	[21, 23]	Самостійно опрацювати матеріал: Застосування програмних закладок та клавіатурних шпигунів (2 год.)	4 бали	Самостійна робота до 14 тижня включно
Максимальна кількість балів за змістовим модулем 2						30 балів	
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.

Форма підсумкового контролю: екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Програмний захист 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 60 балів, та екзамену, максимальна оцінка за який складає 40 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Програмний захист інформації»

Поточний контроль та самостійна робота																				Екзамен	Сума
Змістовий модуль 1									Змістовий модуль 2												
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		
2	2	6	2	2	6	2	2	6	1	1	6	1	1	6	1	1	6	1	1	4		
30									30												40	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, 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, 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 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.

12. Рекомендована література

Базова

1. 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.
2. 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.
3. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
4. 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'ютерні науки». 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.
5. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Програмний захист інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерні науки» 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.
6. 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'ютерні науки». 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.
7. 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.
8. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
9. 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.

Допоміжна

10. 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.
11. 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

12. 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
13. 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
14. 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
15. 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
16. 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.
17. 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
18. 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
19. 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

20. 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

21. Смірнов О.А., Мелешко Є.В.,Конопліцька-Слободенюк О.К., Хох В.Д., Смірнов С.А. Програмний захист інформації. / Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання за спеціальностями «Комп'ютерна інженерія», «Комп'ютерні науки» – Кропивницький: ЦНТУ – 2017. – 53 с.
22. Смірнов О.А., Мелешко Є.В.,Конопліцька-Слободенюк О.К., Хох В.Д., Смірнов С.А. Програмний захист інформації. / Методичні вказівки до виконання лабораторних робіт для студентів заочної форми навчання за спеціальностями «Комп'ютерна інженерія», «Комп'ютерні науки» – Кропивницький: ЦНТУ – 2017. – 53 с.

Інформаційні ресурси

23. Курс «Програмний захист інформації» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=185
24. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/
25. Онлайн-курси Coursera. – URL: https://www.coursera.org
26. Академія Cisco. – URL: https://www.netacad.com
27. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
28. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
29. Пошукова система. – URL:https://www.google.com/
30. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com