ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Савенко О.С.
«1» 09 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека програм та даних

Галузь знань 12 – Інформаційні технології
Спеціальність 121 – Інженерія програмного забезпечення
Рівень вищої освіти – Перший бакалаврський
Освітньо-професійна програма – Інженерія програмного забезпечення
Обсяг дисципліни –5 кредитів ЄКТС, ***Шифр дисципліни*** – ОПП.06
Статус дисципліни: обов'язкова, ***Мова навчання*** Англійська, українська
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Обсяг дисципліни	Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
				Аудиторні заняття				Семінарські заняття	Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Разом	Лекції	Лабораторні роботи	Практичні заняття						
Очна (денна)	4	7	5	150	34	34			82				+
Разом			**5**	**150**	**34**	**34**			**82**				**1**

Робоча програма складена на основі Стандарту вищої освіти, освітньо-професійної програми підготовки бакалаврів 2023 року та навчального плану

Програма складена _____ (Підпис) к.т.н., доцент (Вчений ступінь, звання) Віра ТІТОВА (Ім'я, ПРІЗВИЩЕ)

Схвалена на засіданні кафедри кібербезпеки

Протокол № 1 від "31" серпня 2023 р.

Зав. кафедри кібербезпеки _____ (Підпис) Юрій КЛЬОЦ (Ім'я, ПРІЗВИЩЕ)

Робоча програма розглянута та схвалена Вченою радою факультету інформаційних технологій

Голова Вченої ради факультету _____ (Підпис) Олег САВЕНКО (Ім'я, ПРІЗВИЩЕ)

Хмельницький 2023

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Англійська, українська
Семестр	Сьомий
Обсяг кредитів ЄКТС	5
Форма здобуття освіти	Очна (денна)

Результати навчання. Студент, який успішно завершив вивчення дисципліни, має: аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. . Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем. *Застосовувати* інформаційні технології обробки, зберігання та передачі даних, а також методи та засоби забезпечення інформаційної безпеки ПЗ; *аналізувати*, *вибирати* і *застосовувати* сучасні досягнення науки і техніки для забезпечення інформаційної безпеки ПЗ; *використовувати* операційні системи, мережеві технології, засоби розробки інтерфейсу при конструюванні та захисті ПЗ.

Пререквізити – Архітектура та проєктування програмного забезпечення
Кореквізити – Професійна практика

Зміст навчальної дисципліни. Введення в безпеку програм та даних. Засоби захисту програм та даних. Криптографічний захист програм та даних. Перевірка цілісності програм і даних. Моделі розповсюдження програмного забезпечення. Пакувальники і їх відмінності від архіваторів. Основні поняття ОС, необхідні для захисту програмного забезпечення. Програмно-апаратні методи захисту ПЗ від несанкціонованого копіювання. Захист програм від несанкціонованого дослідження. Захист від дизасемблювання. Захист програм шляхом обфускації. Захист від несанкціонованого налагоджування. Сучасні технології дампінга і захисту від нього.
Запланована навчальна діяльність: лекції – 34 год., лабораторні заняття – 34 год., самостійна робота – 82 год.; разом – 150 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, письмова контрольна робота, підсумковий контрольний захід.

Вид семестрового контролю: іспит.
Навчальні ресурси:

1. Безпека програм та даних: навчальний посібник/ В. І. Горбенко, А.О. Лісняк. Запоріжжя: ЗНУ, 2022. 72 с.
2. Основи інформаційної безпеки : навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Основи криптології: навч. Посібник/ Н.О. Щур, О.А. Покотило. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
4. Вступ до технології блокчейн та криптовалют. Частина 1: навчальний посібник/ Л.В.Ковальчук, А.М.Кудін, Н.В. Кучинська/ Київ: КПІ ім. Ігоря Сікорського, 2022. 141 с.
5. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua.
6. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua

Викладач: кандидат технічних наук, доцент Віра ТІТОВА

3. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Безпека програм та даних» є однією із дисциплін професійної підготовки і займає провідне місце у підготовці фахівців освітнього рівня "бакалавр" за освітньо-професійною програмою "Інженерія програмного забезпечення".

Пререквізити – Архітектура та проєктування програмного забезпечення
Кореквізити – Професійна практика

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення захисту програм та даних; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань захисту ПЗ від несанкціонованого копіювання програмними та програмно-апаратними методами.

Предметом дисципліни є методи та засоби забезпечення захисту програмного забезпечення; методи і засоби підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності «Інженерія програмного забезпечення»:

Відповідно до ***Стандарту вищої освіти*** із та освітньої програми дисципліна сприяє забезпеченню:

компетентностей:

ФК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

ФК12. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

програмних результатів навчання:

ПРН1. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПРН4. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

ПРН18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Результати навчання. Студент, який успішно завершив вивчення дисципліни, має: аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки. . Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем. *Застосовувати* інформаційні технології обробки, зберігання та передачі даних, а також методи та засоби забезпечення інформаційної безпеки ПЗ; *аналізувати*, *вибирати* і *застосовувати* сучасні досягнення науки і техніки для забезпечення інформаційної безпеки ПЗ; *використовувати* операційні системи, мережеві технології, засоби розробки інтерфейсу при конструюванні та захисті ПЗ.

Політика дисципліни Організація освітнього процесу з дисципліни відповідає вимогам

положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні заняття, лабораторні роботи, тощо, згідно з розкладом, не запізнюватися на заняття, виконувати усі завдання та контрольні точки відповідно до графіка. Пропущені практичні заняття і лабораторні роботи студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До практичних занять і лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Технології захисту програм та даних	14	24	60
Тема 2. Методи захисту ПЗ від несанкціонованого копіювання	20	10	22
Разом:	**34**	**34**	**82**

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Технології захисту програм та даних		
1	**Введення в безпеку програм та даних** 1. Проблеми захисту інформації в програмних системах. Критерії оцінки захищеності інформації. 2. Види кіберзлочинів з точки зору безпеки програм та даних. 3. Поняття і класифікація комп'ютерних вірусів. 4. Засоби зламу програмного забезпечення. Їх класифікація. 5. Інструментарій виявлення вразливостей в програмному коді. Літ.: [2] с. 53-89	2
2	**Засоби захисту програм та даних** 1. Автентификация, авторизація та адміністрування дій користувачів 2. Засоби захисту вмісту файлів та папок. 3. Засоби захисту вмісту локальних дисків. 4. Антивіруси. 5. Міжмережні екрани (брандмауери). Літ.: [1], с. 13-21, 55-71; [2] с. 53-89, 106-115	2
3	**Криптографічний захист програм та даних (частина 1)** 1. Класичні методи шифрування. Шифр Цезаря. Квадрат Полібія. Шифр Вернама. Шифр гамування. 2. Потокові криптосистеми. Літ.: [3], с. 6-26	2
4	**Криптографічний захист програм та даних (частина 2)** 1. Блокова криптосистема DES. Режими шифрування. 2. Стандарт шифрування Rijndael. Літ.: [3], с. 33-66	2
5	**Криптографічний захист програм та даних (частина 3)** 1. Схема Діффі – Хелмана розповсюдження ключів по відкритим каналам. 2. Криптосистема з відкритим ключем RSA. Літ.: [3], с. 76-86	2
6	**Криптографічний захист програм та даних (частина 4)** 1. Хеш-функції. Основні алгоритми хешування. 2. Електронний цифровий підпис. Цифровий підпис RSA. Літ.: [3], с. 86-105	2
7	**Перевірка цілісності програм і даних** 1. Основні підходи. 2. Перевірка цілісності за допомогою CRC-кодів. Літ.: [4], с. 231-247	2
Тема 2. Методи захисту ПЗ від несанкціонованого копіювання (НСК)		
8	**Моделі розповсюдження програмного забезпечення** 1. Безкоштовне програмне забезпечення (Freeware). 2. Умовно безкоштовне програмне забезпечення (Demoware, Trialware, Nagware та ін.). 3. Комерційне програмне забезпечення. Літ.: [5], с. 20-30, 47-48	2

9	**Пакувальники і їх відмінності від архіваторів** 1. Огляд сучасних пакувальників. 2. Ідентифікація параметрів пакування виконуваного файлу. Літ.: [5], с. 7-20	2
10	**Основні поняття ОС, необхідні для захисту програмного забезпечення** 1. Склад та функції операційної системи. 2. BIOS - Базова система введення-виведення. 3. UEFI – інтерфейс розширюваної прошивки. 4. CMOS - Complementary Metal Oxide Semiconductor 5. Переривання, їх роль та процедура звернення в програмах Літ.: [5], с. 49-53	2
11	**Програмно-апаратні методи захисту ПЗ від НСК (частина 1)** 1. Робота з дисками на фізичному рівні. Функції BIOS для роботи з дисками. Захист від НСК методом прив'язки до диску. 2. Аналіз вмісту CMOS-пам'яті. 3. Реєстраційні коди. 4. Навісні захисти (протектори). Літ.: [5], с. 53-64, 78-93, 108-117	2
12	**Програмно-апаратні методи захисту ПЗ від НСК (частина 2)** 1. Апаратні ключі. Їх будова та класифікація. 2. Захист програм за допомогою ключа. 3. Огляд та характеристика відомих ключів захисту. 4. Система «SecretKey». 5. Двухфакторна автентифікація на основі технології RSA SecurID. Літ.: [5], с. 119-135	2
13	**Захист програм від несанкціонованого дослідження** 1. Основні методи та засоби дослідження програм. 2. Способи впровадження захисних механізмів в ПЗ. 3. Структура програм, захищених від дослідження. Літ.: [6], с. 6-12	2
14	**Захист від дизасембювання** 1. Необхідність і доцільність захисту від дизасемблювання. 2. Основні методи протидії дизасемблюванню програм. 3. Шифрування коду. 4. Маніпулювання з EXE-заголовком. Літ.: [6], с. 13-30	2
15	**Захист програм шляхом обфускації** 1. Поняття обфускації та її види. Лексична обфускація. Обфускація даних. Обфускація графа потоку управління. 2. Аналіз ефективності роботи обфускаторів. 3. Відомі обфускатори і їх можливості. Літ.: [6], с. 30-53	2
16	**Захист від несанкціонованого налагоджування** 1. Огляд і класифікація налагоджувачів. 2. Захист від налагоджувачів реального режиму. 3. Боротьба з налагоджувачами захищеного режиму. 4. Додаткові прийоми “витонченого” програмування. Літ.: [6], с. 65-74	2
17	**Сучасні технології дампінга і захисту від нього** 1. Порядок завантаження програми і виділення пам’яті процесу. 2. Доступ до пам’яті та списку процесів. 3. Отримання дампу пам’яті обраного процесу.	2

	4. Програми для визначення дампу і захист від них. 5. Методи захисту від дампінгу. Літ.: [6], с. 84-97	
	Разом за семестр:	**34**

5.2 Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Розмежування повноважень користувачів на основі парольної автентифікації Літ.: [2] с. 53-89	4
2	Логування дій користувачів у програмних системах Літ.: [2] с. 53-89	4
3	Захист програмного забезпечення за допомогою механізму CAPTCHA Літ.: [2] с. 53-89	4
4	Захист даних за допомогою цифрового підпису Літ.: [3] с. 94-95	4
5	Захист даних за допомогою технології Blockchain Літ.: [7], с. 8-48	4
6	Перевірка цілісності файлів на основі CRC-кодів Літ.: [4], с. 231-247	4
7	Розробка умовно безкоштовного програмного забезпечення Літ.: [5], с. 47-48	4
8	Захист програмного забезпечення за допомогою механізму обфускації Літ.: [6], с. 30-53	4
9	Підсумкове заняття. Контрольна робота	2
	Разом за семестр:	**34**

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Об’єм самостійної роботи з дисципліни становить 65 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	5
2	Підготовка до виконання лабораторної роботи №1	5
3	Опрацювання теоретичного матеріалу лекції №2.	5
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	5
5	Опрацювання теоретичного матеріалу лекції №3.	5
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	5
7	Опрацювання теоретичного матеріалу лекції №4.	5
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	5
9	Опрацювання теоретичного матеріалу лекції №5.	5
10	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	5
11	Опрацювання теоретичного матеріалу лекції №6.	5
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	5
13	Опрацювання теоретичного матеріалу лекції №7.	5
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	5
15	Опрацювання теоретичного матеріалу лекції №8.	4
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	4
17	Опрацювання теоретичного матеріалу лекції №9. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом.	4
	Разом за семестр:	82

***** При плануванні лекцій за чисельником/за знаменником (розрахунок здійснюється відповідно до розкладу занять)

6. МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться словесними та наочними методами з супроводом презентаційними матеріалами, лабораторні роботи проводяться з використанням практичних та частково-пошукових методів, сучасних інформаційно-комп'ютерних технологій і мають за мету – набуття студентами практичних навичок забезпечення захисту програм та даних; захисту ПЗ від несанкціонованого копіювання програмними та програмно-апаратними методами.

7. ФОРМИ І МЕТОДИ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: обговорення проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт і контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- захист лабораторних робіт;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота		Семестровий контроль
Вид заняття	Лабораторні роботи	Контрольна робота	іспит
Тема	1-2	1-2	1-2
Ваговий коефіцієнт	0,3	0,3	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу,

складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з двох теоретичних питань. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичні питання.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичні питання, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичні питання.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичні питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання

FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

8. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Проблеми захисту інформації в програмних системах.
2. Критерії оцінки захищеності інформації.
3. Види кіберзлочинів з точки зору безпеки програм та даних.
4. Поняття і класифікація комп'ютерних вірусів.
5. Засоби зламу програмного забезпечення. Їх класифікація.
6. Інструментарій виявлення вразливостей в програмному коді.
7. Автентификация, авторизація та адміністрування дій користувачів
8. Засоби захисту вмісту файлів та папок.
9. Засоби захисту вмісту локальних дисків.
10. Антивіруси.
11. Міжмережні екрани (брандмауери).
12. Шифр Цезаря.
13. Квадрат Полібія.
14. Шифр Вернама.
15. Шифр гамування.
16. Потокові криптосистеми.
17. Блокова криптосистема DES. Режими шифрування.
18. Стандарт шифрування Rijndael.
19. Схема Діффі – Хелмана розповсюдження ключів по відкритим каналам.
20. Криптосистема з відкритим ключем RSA.
21. Хеш-функції. Основні алгоритми хешування.
22. Електронний цифровий підпис. Цифровий підпис RSA.
23. Основні підходи до перевірки цілісності програм і даних.
24. Перевірка цілісності за допомогою CRC-кодів.
25. Моделі розповсюдження програмного забезпечення.
26. Безкоштовне програмне забезпечення (Freeware).
27. Умовно безкоштовне програмне забезпечення (Demoware, Trialware, Nagware та ін.).
28. Комерційне програмне забезпечення.
29. Пакувальники і їх відмінності від архіваторів
30. Огляд сучасних пакувальників.
31. Ідентифікація параметрів пакування виконуваного файлу.
32. Склад та функції операційної системи.
33. BIOS - Базова система введення-виведення.
34. UEFI – інтерфейс розширюваної прошивки.
35. CMOS - Complementary Metal Oxide Semiconductor
36. Переривання, їх роль та процедура звернення в програмах
37. Робота з дисками на фізичному рівні. Функції BIOS для роботи з дисками. Захист від НСК методом прив'язки до диску.
38. Аналіз вмісту CMOS-пам'яті для захисту від НСК.
39. Реєстраційні коди, як захист від НСК.
40. Навісні захисти (протектори).
41. Апаратні ключі. Їх будова та класифікація.
42. Захист програм за допомогою ключа.
43. Огляд та характеристика відомих ключів захисту.
44. Система «SecretKey».
45. Двухфакторна автентифікація на основі технології RSA SecurID.
46. Основні методи та засоби дослідження програм.
47. Способи впровадження захисних механізмів від несанкціонованого дослідження в ПЗ.
48. Структура програм, захищених від дослідження.
49. Необхідність і доцільність захисту від дизасемблювання.
50. Основні методи протидії дизасемблюванню програм.

51. Шифрування коду, як захист від дизасемблювання
52. Маніпулювання з EXE-заголовком, як захист від дизасемблювання.
53. Поняття обфускації та її види.
54. Лексична обфускація.
55. Обфускація даних.
56. Обфускація графа потоку управління.
57. Аналіз ефективності роботи обфускаторів.
58. Відомі обфускатори і їх можливості.
59. Огляд і класифікація налагоджувачів.
60. Захист від налагоджувачів реального режиму.
61. Боротьба з налагоджувачами захищеного режиму.
62. Додаткові прийоми “витонченого” програмування.
63. Порядок завантаження програми і виділення пам’яті процесу.
64. Доступ до пам’яті та списку процесів.
65. Отримання дампу пам’яті обраного процесу.
66. Програми для визначення дампу і захист від них.
67. Методи захисту від дампінгу.

9. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Освітній процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Безпека програм та даних: навчальний посібник/ В. І. Горбенко, А.О. Лісняк. Запоріжжя: ЗНУ, 2022. 72 с.
2. Основи інформаційної безпеки : навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Основи криптології: навч. Посібник/ Н.О. Щур, О.А. Покотило. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
4. Теорія інформації і кодування: курс лекцій: навч. посіб./ А.Є.Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.
5. Захист програмного забезпечення. Частина 1: навчальний посібник/В. А. Каплун, О. В. А.В. Дудатьєв, В. П. Семеренко В.П. Вінниця: ВНТУ, 2017. 140 с.
6. Захист програмного забезпечення. Частина 2: навчальний посібник/В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев. Вінниця: ВНТУ, 2017. 105 с.
7. Вступ до технології блокчейн та криптовалют. Частина 1: навчальний посібник/ Л.В.Ковальчук, А.М.Кудін, Н.В. Кучинська/ Київ: КПІ ім. Ігоря Сікорського, 2022. 141 с.

Додаткова

8. Четверіков І. О., Петренко А. І. Технологія Blockchain в системі захисту інформації/ Моделювання та інформ. системи в економіці: зб. наук. праць/ відп. ред. О. Є. Камінський. 2020. № 99.1. С. 162-170.

9. Корнага Я.І., Герасименко О.Ю., Базака Ю.А., Базалій М.Ю., Мухін О.В. Method of Protecting Software Code from Reengineering Using Virtual Machines. Sciences of Europe, 2020. № 58. С. 59-62.

10. Корнага Я.І., Базака Ю.А., Базалій М.Ю. Захист програмного забезпечення за допомогою заплутуючих перетворень. The scientific heritage, 2020. № 54. С. 72-75.

11. Семенов С.Г., Давидов В.В., Волошин Д.Г., Гребенюк Д.С. Метод захисту модуля програмного забезпечення на основі процедури обфускації/ Телекомунікаційні та інформаційні технології. 2019. № 4 (65). С.71-80.

12. Privacy and Data Protection in Software Services. (2021). Springer Nature Singapore, pp.220

13. Lenhard, T. H. (2022). Data Security: Technical and Organizational Protection Measures Against Data Loss and Computer Crime. Springer Fachmedien Wiesbaden, pp.113

14. Bhushan, M., Rathore, R. S., Jamshed, A. (2017). Fundamentals of Cyber Security. BPB Publications, pp.228

15. Preston, W. C. (2021). Modern Data Protection. (n.p.): O'Reilly Media, pp.386

11. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

KHMELNYTSKYI NATIONAL UNIVERSITY

APPROVED
Dean of the Faculty
_____ Savenko O.S.
"09" _____ 2023.

COURSE PROGRAM
Software and Data Security

Field of study: 12 - Information Technologies
Major: 121 – Software Engineering
Level of Higher Education: First Level (Bachelor)
Educational program: Software Engineering
Discipline status: Compulsory
Faculty: Information Technologies
Department: Cybersecurity

Study mode	Year	Semester	Total Credits	Number of hours						Course project	Coursework	Semester control form	
				Classwork hours				Seminar classes	Independent work, including individual			pass/ fail test	Exam
			ECTS credits	Total	Lectures	Laboratory works	Practical classes						
Full-time (Daytime)	4	7	5	150	34	34			82				+
Total			**5**	**150**	**34**	**34**			**82**				**1**

The course program is based on the Higher Education Standard, the 2023 Bachelor's degree educational program, and the curriculum.

Program's author _____ V. Titova

Approved at the staff meeting of the Cybersecurity Department

Minutes from 31.08.2023 No. 1

Head of the Cybersecurity Department _____ Yu. Klots

The course program is approved by the Academic Board of the Faculty of Information technologies

Head of the Academic Board _____ O.S. Savenko

Khmelnytskyi 2023

SOFTWARE AND DATA SECURITY

Type of Discipline	Compulsory
Level of Higher Education	First (Bachelor's)
Language of Instruction	English
Semester	7
ECTS Credits	5
Course study mode	Full-time (Daytime)

Learning outcomes. A student who has successfully completed the study of the discipline must: *apply* information technologies for data processing, storage and transmission, as well as methods and means of ensuring software information security; *analyze* , *select* and *apply* modern achievements of science and technology to ensure software information security; *use* operating systems, network technologies, interface development tools when designing and protecting software.

Content of the academic discipline. Introduction to program and data security. Program and data protection tools. Cryptographic protection of programs and data. Checking the integrity of programs and data. Software distribution models. Packers and their differences from archivers. Basic OS concepts needed to protect software. Software and hardware methods of software protection against unauthorized copying. Protection of programs from unauthorized research. Protection against disassembly. Protection of programs by obfuscation. Protection against unauthorized debugging. Modern technologies of dumping and protection against it.

Prerequisites – software architecture and design

The prerequisites Professional Practice

Planned educational activity : lectures - 34 hours, laboratory classes - 34 hours, independent work – 82 hours; together - 150 hours

Teaching methods : verbal and visual (lectures); practical and partially research (laboratory works); explanatory and illustrative and research (independent work).

Forms of evaluation of learning results : defense of laboratory work, written control work, final control measure.

Type of semester control: exam.

Educational resources:

1. Preston, W. C. (2021). Modern Data Protection. (n.p.): O'Reilly Media.386 p.
2. Lenhard, T. H. (2022). Data Security: Technical and Organizational Protection Measures Against Data Loss and Computer Crime. Springer Fachmedien Wiesbaden.. 113 p.
3. Fundamentals of cryptology: teaching. Manual/ N.O. Shchur, O.A. It rolled. Zhytomyr: Zhytomyr Polytechnic State University, 2021. 120 p.
4. Introduction to blockchain technology and cryptocurrencies. Part 1: study guide/ L.V. Kovalchuk, A.M. Kudin, N.V. Kuchynska/ Kyiv: KPI named after Igor Sikorskyi, 2022. 141 p.
5. MOODLE Learning Platform. Access to the resource https://msn.khmnu.edu.ua.
6. University Electronic Library. Access to the resource: http://library.khmnu.edu.ua.

Lecturer : Ph.D., associate professor Titova V.Yu.

3. EXPLANATORY NOTE

The discipline "Software and data security" is a component of the professional training of bachelors in the specialty "Software engineering".

The purpose of teaching the academic discipline is to form future specialists' skills and competencies to ensure the protection of programs and data; development of students' professional thinking style; provision of deep and solid knowledge on software protection from unauthorized copying by software and software-hardware methods.

The subject of the discipline is methods and means of software protection; methods and means of maintaining the integrity, general functionality and reliability of the software.

The task of the discipline is to ensure the acquisition of competencies and the achievement of program learning outcomes in accordance with the educational and professional training program for bachelors in the specialty "Software Engineering":

According to the Standard of higher education and the educational program, the discipline must ensure:

Integral competence

Ability to solve complex, specialised tasks or practical problems in software engineering, characterised by complexity and uncertainty of conditions, using information technology theories and methods

***competences* :**

PC6. Ability to analyse, select, and apply methods and tools for ensuring information security (including cybersecurity).

PC12. Ability to execute the system integration process and apply standards and change management procedures to maintain the integrity, overall functionality, and reliability of the software.

learning outcomes:

PLO1 To analyse, purposefully search for, and select the necessary information, reference resources, and knowledge for solving professional tasks, considering modern scientific and technical achievements.

PLO4 To know and apply professional standards and other regulatory documents in the field of software engineering.

PLO18 To know and be able to apply information technologies for data processing, storage, and transmission.

PLO21 To understand, analyse, select, and competently use tools to ensure information security (including cybersecurity) and data integrity relative to applied tasks and created software systems.

A student who has successfully completed the study of the discipline must: *apply* information technologies for data processing, storage and transmission, as well as methods and means of ensuring software information security; *analyze* , *select* and *apply* modern achievements of science and technology to ensure software information security; *use* operating systems, network technologies, interface development tools when designing and protecting software.

Discipline Policy. The organization of the educational process for the discipline complies with the requirements of the provisions on organizational and instructional-methodological support of the educational process, the educational program, and the curriculum. Students are required to attend lectures, practical classes, laboratory work, etc., according to the schedule, not to be late for classes, and to complete all tasks and checkpoints according to the schedule. Missed practical classes and laboratory work must be independently completed by the student in full and reported to the instructor no later than one week before the next assessment. For practical classes and laboratory work, students must prepare on the relevant topic and demonstrate active participation. Knowledge acquired by an individual in the discipline or its specific sections through informal education is credited according to the Regulation on the procedure for transferring learning outcomes and determining academic differences at KhNU.

4. COURSE CREDIT STRUCTURE

Topic name	The number of hours allocated to:		
	lectures	**laboratory work**	**independent work**
Topic 1. Program and data protection technologies	14	24	60
Topic 2. Methods of software protection against unauthorized copying	20	10	22
Together:	**34**	**34**	**82**

5 . COURSE PROGRAM

5.1 Content of the lecture course

Lecture number	List of lecture topics, their abstract	hours
	Topic 1. Program and data protection technologies	
1	**Introduction to program and data security** 1. Problems of information protection in software systems. Information security assessment criteria. 2. Types of cybercrimes from the point of view of program and data security. 3. Concept and classification of computer viruses. 4. Software hacking tools. Their classification. 5. Toolkit for detecting vulnerabilities in software code. Lit.: [2] c. 53-89	2
2	**Program and data protection tools** 1. Authentication, authorization and administration of user actions 2. Means of protecting the contents of files and folders. 3. Means of protecting the contents of local disks. 4. Antiviruses. 5. Inter-network screens (firewalls). Lit.: [1], c . 13-21, 55-71; [2] 53-89, 106-115	2
3	**Cryptographic protection of programs and data (part 1)** 1. Classic encryption methods. Caesar's Cipher. Square of Polybius. Vernam cipher. Jamming cipher. 2. Stream cryptosystems. Lit.: [3], c . 6-26	2
4	**Cryptographic protection of programs and data (part 2)** 1. DES block cryptosystem. Encryption modes. 2. Rijndael encryption standard. Lit.: [3], c . 33-66	2
5	**Cryptographic protection of programs and data (part 3)** 1. Diffie-Hellman key distribution scheme over open channels. 2. RSA public key cryptosystem. Lit.: [3], c . 76-86	2
6	**Cryptographic protection of programs and data (part 4)** 1. Hash functions. Basic hashing algorithms. 2. Electronic digital signature. RSA digital signature.	2

	Lit.: [3], c . 86-105	
7	**Checking the integrity of programs and data** 1. Basic approaches. 2. Integrity check using CRC codes. Lit.: [4], c . 231 - 247	2
Topic 2. Software protection methods against unauthorized copying (NSC)		
8	**Software distribution models** 1. Free software (Freeware) . 2. Conditionally free software (Demoware, Trialware , Nagware , etc.) . 3. Commercial software. Lit.: [5], c . 2 0-30, 47-48	2
9	**Packers and their differences from archivers** 1. Overview of modern packers. 2. Identification of the packaging parameters of the executable file. Lit.: [5], c . 7-20	2
10	**Basic OS concepts needed to protect software** 1. Composition and functions of the operating system. 2. BIOS - Basic input-output system. 3. UEFI is an extensible firmware interface. 4. CMOS - Complementary Metal Oxide Semiconductor 5. Interrupts, their role and application procedure in programs Lit.: [5], c . 49-53	2
11	**Software and hardware methods of software protection from NSC (part 1)** 1. Working with disks at the physical level. BIOS functions for working with disks. Protection against NSC by the method of binding to the disk. 2. Analysis of CMOS memory content. 3. Registration codes. 4. Hinged protections (protectors). Lit.: [5], c . 53-64, 78-93, 108-117	2
12	**Software and hardware methods of software protection from NSC (part 2)** 1. Hardware keys. Their structure and classification. 2. Protection of programs using a key. 3. Overview and characteristics of known protection keys. 4. "SecretKey" system. 5. Two-factor authentication based on RSA SecurID technology. Lit.: [5], c . 119-135	2
13	**Protection of programs from unauthorized research** 1. Basic methods and means of program research. 2. Methods of implementing protective mechanisms in software. 3. Structure of programs protected from research. Lit.: [6], c . 6-12	2
14	**Protection against disassembly** 1. Necessity and expediency of protection against disassembly. 2. Basic methods of counteracting program disassembly. 3. Code encryption. 4. Manipulation with the EXE header. Lit.: [6], c . 13-30	2
15	**Protection of programs by obfuscation** 1. Concept of obfuscation and its types. Lexical obfuscation. Data obfuscation. Control flow graph obfuscation.	2

	2. Analysis of obfuscation efficiency. 3. Known obfuscators and their capabilities. Lit.: [6], c . 30-53	
16	**Protection against unauthorized debugging** 1. Overview and classification of debuggers. 2. Protection against real mode debuggers. 3. Combating protected mode debuggers. 4. Additional techniques of "sophisticated" programming. Lit.: [6], c . 65-74	2
17	**Modern technologies of dumping and protection against it** 1. The procedure for loading the program and allocating process memory. 2. Access to memory and process list. 3. Obtaining a memory dump of the selected process. 4. Programs for determining the dump and protection against them. 5. Methods of protection against dumping. Lit.: [6], c . 84-97	2
	Total per semester:	**34**

5.2 Contents of laboratory works

No n/p	**Topics of laboratory work**	**Number of hours**
1	User authorization based on password authentication Lit.: [2] c. 53-89	4
2	Logging of user actions in software systems Lit.: [2] c. 53-89	4
3	Software protection using the CAPTCHA mechanism Lit.: [2] c. 53-89	4
4	Data protection using a digital signature Lit.: [3] c . 94-95	4
5	Data protection using Blockchain technology Lit.: [7], c . 8-48	4
6	File integrity check based on CRC codes Lit.: [4], c . 231 - 247	4
7	Development of conditionally free software Lit.: [5], c . 47-48	4
8	Software protection using an obfuscation mechanism Lit.: [6], c . 30-53	4
9	Final lesson. Control work	2
	Total per semester:	**34**

5.3 Content of independent (including individual) work

The volume of independent work on the discipline is 65 hours. It includes processing of lecture material and literature sources, preparation for control work, preparation for performance and protection of laboratory work. Management of independent work is carried out by the teacher according to the schedule of consultations outside of class time.

No week	Topics of independent work	Number of hours
1	Elaboration of the theoretical material of lecture #1.	5
2	Preparation for laboratory work No. 1	5
3	Elaboration of the theoretical material of lecture #2.	5
4	Preparation for the defense of laboratory work #1. Preparation for laboratory work No. 2.	5
5	Elaboration of the theoretical material of lecture #3.	5
6	Preparation for the defense of laboratory work #2. Preparation for laboratory work No. 3.	5
7	Elaboration of the theoretical material of lecture #4.	5
8	Preparation for the defense of laboratory work #3. Preparation for laboratory work No. 4.	5
9	Elaboration of the theoretical material of lecture No. 5.	5
10	Preparation for the defense of laboratory work #4. Preparation for laboratory work No. 5.	5
11	Elaboration of the theoretical material of lecture #6.	5
12	Preparation for the defense of laboratory work No. 5. Preparation for laboratory work No. 6.	5
13	Elaboration of the theoretical material of lecture #7.	5
14	Preparation for the defense of laboratory work #6. Preparation for laboratory work No. 7.	5
15	Elaboration of the theoretical material of lecture #8.	4
16	Preparation for the defense of laboratory work #7. Preparation for laboratory work No. 8.	4
17	Elaboration of the theoretical material of lecture #9. Preparation for the defense of laboratory work #8. Preparation for the test based on the material covered.	4
	Total per semester:	82

6 . TEACHING METHODS

The process of learning in the discipline is based on the use of traditional and modern methods. In particular, the lectures are conducted by verbal and visual methods accompanied by presentation materials, laboratory work is conducted using practical and partially research methods, modern information and computer technologies and have the goal of students acquiring practical skills to ensure the protection of programs and data; protection of software against unauthorized copying by software and software-hardware methods.

The teaching methods used in the teaching of the discipline contribute to the development of soft skills in students: discussion of problematic issues during lectures, public defenses of laboratory works with the justification of decisions made regarding the choice of methods for solving tasks in dialogue with the teacher and the group contribute to the formation and improvement of public speaking skills, empathic listening , advocacy of one's own point of view, introspection and self-

criticism; adaptability, the ability to use Internet resources and other sources of information, synthesize and critically interpret information from various sources provided by the specifics of the discipline; limited time for performing laboratory work and control tasks, clearly defined and provided in the syllabus deadlines for passing control points and working off debts contribute to the development of punctuality, the ability to self-organize and manage time (time management).

When studying a discipline, learning results obtained in non-formal education can be credited. The recognition of learning results obtained in non-formal education is implemented in accordance with the current legislation and is regulated by the Regulation on the procedure for recognition and re-enrollment of learning results of students of higher education at KhNU.

7. ASSESSMENT FORMS AND METHODS

Current control is carried out during laboratory classes, as well as on the days of control activities established by the work plan of the discipline.

At the same time, the following methods of current control are used:

- protection of laboratory works;
- written control work.

Semester control is conducted in the form of an exam. When deriving the final semester grade, the results of both the current control and the final control event are taken into account.

Assessment of the student's academic achievements is carried out in accordance with the "Regulations on control and evaluation of the results of studies of students of higher education at KhNU". Each type of work in the discipline is evaluated on an institutional four-point scale. The semester final grade is defined as a weighted average of all types of academic work completed and passed positively, taking into account the weighting factor. The weighting factors change depending on the structure of the discipline and the importance of certain types of its work.

The structuring of the discipline by types of work and the assessment of student learning outcomes by weighting factors

	Auditory work		Semester control
Type of occupation	Laboratory work	Control work	exam
Topic	1-2	1-2	1-2
Weight factor	0.3	0.3	0.4

Evaluation of laboratory works . The grade given for laboratory work consists of the following elements: knowledge of theoretical material on the topic; the quality of the report design; the student's fluency in special terminology and the ability to professionally justify the adopted constructive decisions; timely protection of laboratory work.

The deadline for the defense of the laboratory work report is considered timely if the student defended it on the day of completion or at the next class after the completion of the work. The student must complete the missed class in the department's laboratories by the deadline set by the teacher, with registration in the department's journal, but no later than two weeks before the end of theoretical classes in the semester.

The teacher announces the grade for the laboratory work immediately after the defense of the report and puts it in the electronic journal of the discipline.

Evaluation of control works. The test consists of two theoretical questions. Evaluation is carried out on a four-point scale.

The grade "excellent" is awarded to a student who gave a complete written answer to the theoretical questions.

A grade of "good" is given to a student who gave the correct answer to the theoretical questions, but there are two or three insignificant errors in the answer.

A "satisfactory" grade is given to a student who gave a partial answer to the theoretical questions.

An "unsatisfactory" grade is given to a student who did not answer the theoretical questions.

The teacher puts the grade for the control work in the electronic journal of the discipline no later than ten days after the control event.

Semester control (exam). The final control measure in the discipline is conducted in the form of an exam. The examination ticket consists of two theoretical questions and a problem. During the exam, based on the provided answers and solutions (solutions), the student's level of assimilation of the subject material is evaluated.

The grade for the final control measure is entered by the teacher in the electronic journal of the discipline on the day of the exam and is taken into account in the automated mode when determining the final semester grade of the student in the discipline according to the institutional scale and the ECTS scale. The student's assimilation of the subject material is assessed according to the criteria listed in the table.

If a student received a negative grade for a certain type of work, then he must resubmit it in the established order, but necessarily before the next inspection deadline.

A student who scored a positive weighted average score for the current work and did not pass the final control measure (exam) is considered to have failed.

The final semester grade according to the institutional scale and the ECTS scale is set in an automated mode after the teacher enters all the grades into the electronic journal.

Correlation of the domestic evaluation scale and the ECTS evaluation scale

Evaluation of ECTS	**Institutional interval scale of points**	**Institutional assessment, assessment criteria**	
A	4.75–5.00	5	***Excellent*** - deep and complete mastery of the basic material and identification of relevant skills and abilities
B	4.25–4.74	4	***Good*** - complete knowledge of the educational material with a few minor errors
C	3.75–4.24	4	***Good*** - a generally correct answer with two or three significant errors
D	3.25–3.74	3	***Satisfactory*** - incomplete mastery of the software material, but sufficient for practical activity in the profession
E	3.00–3.24	3	***Satisfactory*** - incomplete mastery of the program material that meets the minimum evaluation criteria
FX	2.00–2.99	2	***Unsatisfactory*** – the unsystematic nature of the acquired knowledge and the impossibility of continuing education without additional knowledge of the discipline
F	0.00–1.99	2	***Unsatisfactory*** - serious further work and re-study of the discipline is necessary

8. QUESTIONS FOR STUDENTS' SELF-CONTROL

1. Problems of information protection in software systems.
2. Information security assessment criteria.
3. Types of cybercrimes from the point of view of software and data security.
4. Concept and classification of computer viruses.
5. Software hacking tools. Their classification.
6. Toolkit for detecting vulnerabilities in software code.
7. Authentication, authorization and administration of user actions
8. File and folder content protection tools.
9. Means for protecting the contents of local drives.

10. Antiviruses.
11. Inter-network screens (firewalls).
12. Caesar's Cipher.
13. Square of Polybius.
14. Vernam cipher.
15. Jamming cipher.
16. Stream cryptosystems.
17. DES block cryptosystem. Encryption modes.
18. Rijndael encryption standard.
19. Diffie-Hellman key distribution scheme over open channels.
20. RSA public key cryptosystem.
21. Hash functions. Basic hashing algorithms.
22. Electronic digital signature. RSA digital signature.
23. Basic approaches to checking the integrity of programs and data.
24. Integrity check using CRC codes.
25. Software distribution models.
26. Free software (Freeware).
27. Conditionally free software (Demoware, Trialware, Nagware, etc.).
28. Commercial software.
29. Packers and their differences from archivers
30. Overview of modern packers.
31. Identification of the packaging parameters of the executable file.
32. Composition and functions of the operating system.
33. BIOS - Basic Input-Output System.
34. UEFI is an extensible firmware interface.
35. CMOS - Complementary Metal Oxide Semiconductor
36. Interrupts, their role and application procedure in programs
37. Working with disks at the physical level. BIOS functions for working with disks. Protection against NSC by the method of binding to the disk.
38. Analysis of the contents of CMOS memory for protection against NSC.
39. Registration codes as protection against NSC.
40. Hinged protections (protectors).
41. Hardware keys. Their structure and classification.
42. Protecting programs with a key.
43. Overview and characteristics of known protection keys.
44. "SecretKey" system.
45. Two-factor authentication based on RSA SecurID technology.
46. Basic methods and means of program research.
47. Methods of implementing protective mechanisms against unauthorized research in software.
48. Structure of programs protected from research.
49. Necessity and expediency of protection against disassembly.
50. Basic methods of combating program disassembly.
51. Code encryption as protection against disassembly
52. Manipulation of the EXE header as protection against disassembly.
53. Concept of obfuscation and its types.
54. Lexical obfuscation.
55. Data obfuscation.
56. Control flow graph obfuscation.
57. Analysis of obfuscation efficiency.
58. Known obfuscators and their capabilities.
59. Overview and classification of debuggers.
60. Protection against real-mode debuggers.
61. Fighting protected mode debuggers.

62. Additional techniques of "sophisticated" programming.
63. The order of program loading and process memory allocation.
64. Access memory and process list.
65. Obtaining a memory dump of the selected process.
66. Programs for dump detection and protection against them.
67. Methods of protection against dumping.

9. TEACHING AND LEARNING MATERIALS

The educational process of the discipline is fully and in sufficient quantity provided with the necessary educational and methodical literature, which is placed in the MOODLE modular environment.

10. RECOMMENDED BOOKS

Main

1. Безпека програм та даних: навчальний посібник/ В. І. Горбенко, А.О. Лісняк. Запоріжжя: ЗНУ, 2022. 72 с.
2. Основи інформаційної безпеки : навч. посібник/ В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Основи криптології: навч. Посібник/ Н.О. Щур, О.А. Покотило. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
4. Теорія інформації і кодування: курс лекцій: навч. посіб./ А.Є.Коваленко. Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.
5. Захист програмного забезпечення. Частина 1: навчальний посібник/В. А. Каплун, О. В. А.В. Дудатьєв, В. П. Семеренко В.П. Вінниця: ВНТУ, 2017. 140 с.
6. Захист програмного забезпечення. Частина 2: навчальний посібник/В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев. Вінниця: ВНТУ, 2017. 105 с.
7. Вступ до технології блокчейн та криптовалют. Частина 1: навчальний посібник/ Л.В.Ковальчук, А.М.Кудін, Н.В. Кучинська/ Київ: КПІ ім. Ігоря Сікорського, 2022. 141 с.

Additional

8. Четверіков І. О., Петренко А. І. Технологія Blockchain в системі захисту інформації/ Моделювання та інформ. системи в економіці: зб. наук. праць/ відп. ред. О. Є. Камінський. 2020. № 99.1. С. 162-170.
9. Корнага Я.І., Герасименко О.Ю., Базака Ю.А., Базалій М.Ю., Мухін О.В. Method of Protecting Software Code from Reengineering Using Virtual Machines. Sciences of Europe, 2020. № 58. С. 59-62.
10. Корнага Я.І., Базака Ю.А., Базалій М.Ю. Захист програмного забезпечення за допомогою заплутуючих перетворень. The scientific heritage, 2020. № 54. С. 72-75.
11. Семенов С.Г., Давидов В.В., Волошин Д.Г., Гребенюк Д.С. Метод захисту модуля програмного забезпечення на основі процедури обфускації/ Телекомунікаційні та інформаційні технології. 2019. № 4 (65). С.71-80.
12. Privacy and Data Protection in Software Services. (2021). Springer Nature Singapore, pp.220
13. Lenhard, T. H. (2022). Data Security: Technical and Organizational Protection Measures Against Data Loss and Computer Crime. Springer Fachmedien Wiesbaden, pp.113
14. Bhushan, M., Rathore, R. S., Jamshed, A. (2017). Fundamentals of Cyber Security. BPB Publications, pp.228
15. Preston, W. C. (2021). Modern Data Protection. (n.p.): O'Reilly Media, pp.386

11 . INFORMATION RESOURCES

1. MOODLE Learning Platform. Access to the resource https://msn.khmnu.edu.ua.
2. University Electronic Library. Access to the resource: http://library.khmnu.edu.ua.
3. University Repository. Access to the resource https://elar.khmnu.edu.ua/home.