ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

«29» 08 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія криптосистем та управління криптографічними ключами

Галузь знань	F – Інформаційні технології
Спеціальність	F5 – Кібербезпека та захист інформації
Рівень вищої освіти	Другий (магістерський)
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	6 кредитів ЄКТС
Мова навчання	Українська
Код дисципліни	ОФП.03
Статус дисципліни	Обов'язкова (фахової підготовки)
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРЗ				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	1	2	6	180	50	16	34			130				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю F5 «Кібербезпека та захист інформації»

Робоча програма складена _____ д-р. техн. наук, проф. Михайло КАСЯНЧУК
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки
Протокол від «29» 08.2025 р. №1

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

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ім'я, ПРІЗВИЩЕ
Зав. кафедри	кібербезпеки		Юрій КЛЬОЦ
Гарант ОП	кібербезпеки		Віра ТІТОВА

3. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Теорія криптосистем та управління криптографічними ключами» є однією із дисциплін фахової підготовки здобувачів другого (магістерського) рівня вищої освіти, очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

Пререквізити – методологія та організація наукових досліджень.

Постреквізити – переддипломна практика, кваліфікаційна робота.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

компетентностей

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. ЗК01. Здатність застосовувати знання у практичних ситуаціях. ЗК04. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК05. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). ФК01. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК02. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК03. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК08. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

програмних результатів навчання

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної

інфраструктури. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Мета дисципліни. Формування у студентів системних знань і практичних навичок з впровадження методів та засобів криптографічного захисту на об'єктах інформаційної діяльності

Предмет дисципліни. Технології, методи та засоби криптографічного захисту інформації, криптографічне програмне та програмно-апаратне забезпечення кіберзахисту.

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для розробки і супроводу методів та засобів криптографічного захисту інформації.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вільно *володіти* державною мовою для представлення результатів діяльності та обговорення питань у сфері криптографічного захисту інформації; чітко *формулювати* висновки й *обґрунтовувати* їх для персоналу, партнерів та інших осіб; *планувати* навчання та контролювати роботу персоналу у сфері управління криптографічними ключами; *здійснювати* дослідницьку діяльність, обираючи та розробляючи відповідні методи захисту; *застосовувати* комп'ютерне моделювання для аналізу процесів; *впроваджувати* та *вдосконалювати* математичні моделі; *аналізувати* та *впроваджувати* кращі світові практики; *розробляти* й *супроводжувати* системи захисту на об'єктах критичної інфраструктури, оцінюючи їх ефективність; *приймати* обґрунтовані організаційно-технічні рішення, зокрема щодо вибору програмного та апаратного забезпечення та його обмежень.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:

	лекції	лабораторні роботи	СРС
Тема 1. Теорія криптографічних систем	10	34	75
Тема 2. Управління криптографічними ключами	6	-	55
Разом:	**16**	**34**	**130**

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1 Зміст лекційного курсу

Перелік лекцій

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Теорія криптографічних систем		**10**
1	**Підходи до реалізації сучасних криптографічних систем та протоколів** Проєктування криптосистем за принципом Керкгоффса. Підхід до формування протоколів цифрового підпису різного призначення (сліпий підпис, колективний підпис тощо). Аналіз алгоритмів заперечного шифрування та їх модифікація. Проєктування криптосистем RSA та Ель-Гамаля на основі векторномодульного-методу модулярного множення та експоненціювання. Літ.: [1]; [2] с. 56-75; [3]; [13]; [14]; [17]	2
2	**Квантова криптографія** Дослідження переваг використання квантової криптографії. Розробка паралельних моделей протоколів квантової криптографії під технологію GPGPU. Порівняльний аналіз протоколів квантового розподілення ключів. Моделювання протоколів квантової криптографії на платформі CUDA. Літ.: [1]	2
3	**Теоретичні основи системи залишкових класів** Теоретичні основи системи залишкових класів. Методи відновлення десяткового числа за його залишками. Китайська теорема про залишки. Методи проєктування досконалої та модифікованої досконалої форм системи залишкових класів. Літ.: [5] с. 51-73	2
4	**Методи проєктування криптосистем на основі залишкових класів** Методи проєктування симетричних криптосистем на основі залишкових класів. Методи проєктування асиметричних криптосистем на основі залишкових класів. Використання модифікованої досконалої форми системи залишкових класів для проєктування криптосистем. Літ.: [5] с. 51-73; [11]; [12]; [15]; [16]; [18]	2
5	**Застосування методів криптоаналізу** Класифікація криптоаналітичних атак. Клептографічні атаки на криптосистеми та захист від них. Нові технології у криптоаналізі (нейронні мережі, генетичні алгоритми, квантові комп'ютери). Літ.: [1]; [2] с. 6-55	2
Тема 2. Управління криптографічними ключами		**6**
6	**Управління ключами** Аналіз цілей управління ключами. Протоколи розподілу криптографічних ключів. Особливості політики безпеки управління ключами (термін дії	2

	ключів, життєвий цикл ключів, послуги, що надаються довіреною третьою стороною). Процеси впровадження систем умовного депонування ключів підприємства для підтримки шифрування даних у стані спокою. Літ.: [1]; [2] с. 56-75; [3]; [9]; [13]; [14]; [17]	
7	**Інфраструктура відкритих ключів** Проєктування, впровадження та супровід захищених систем доменних імен DNS. Проєктування, впровадження та супровід систем захищеної електронної пошти PGP. Проєктування, впровадження та супровід систем захищених електронних транзакцій SET. Інфраструктура відкритих ключів Oauth, OpenID, SAML, SPML. Літ.: [9]	2
8	**Створення центру сертифікації ключів (ЦСК)** Категоріювання та обстеження ЦСК. Підготовка організаційно-розпорядчої документації. Проєктування, створення та впровадження ЦСК. Структура та склад центру. Особливості проектування ЦСК на базі криптомодулів. Розробка програми та супровід внутрішніх випробувань. Дослідна експлуатація. Планування навчання обслуговуючого персоналу. Експертизи та акредитація ЦСК. Літ.: [10]	2
	Разом за семестр:	**16**

5.2 Зміст лабораторних робіт

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Теорія криптографічних систем		**34**
1	Проєктування та дослідження криптосистем сучасними програмними та апаратними засобами Літ.: [1]; [2] с. 56-75; [3]	4
2	Проєктування та дослідження криптосистем на основі електронного цифрового підпису Літ.: [1]; [2] с. 56-75; [3]	4
3	Проєктування та дослідження криптосистем для аутентифікації повідомлень Літ.: [1]; [2] с. 56-75; [3]	4
4	Проєктування та модифікація криптосистем на основі заперечуваного шифрування Літ.: [1]; [2] с. 56-75; [3]	4
5	Проєктування та дослідження криптосистем на основі векторно-модульного методу модулярного множення та експоненціювання Літ.: [4] с. 92-130; [5] с. 33-51	4
6	Проєктування та дослідження криптосистем на основі системи залишкових класів Літ.: [5] с. 51-73; [11]; [12]; [15]; [16]; [18]	4
7	Аналіз стійкості криптосистем за допомогою нейронних мереж Літ.: [6]; [7]	4
8	Аналіз стійкості криптосистем за допомогою генетичних алгоритмів Літ.: [8]	4
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

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

Самостійна робота студентів полягає у опрацюванні теоретичного матеріалу з відповідних джерел інформації, підготовці до виконання та захисту лабораторних робіт, до тестування тощо. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	7
2	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	8
3	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2.	7
4	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	8
5	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3.	7
6	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	8
7	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4.	7
8	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	8
9	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5.	7
10	Опрацювання теоретичного матеріалу лекції №10. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	8
11	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6.	7
12	Опрацювання теоретичного матеріалу лекції №12. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	8
13	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7.	7
14	Опрацювання теоретичного матеріалу лекції №14. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	8
15	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8.	7
16	Опрацювання теоретичного матеріалу лекції №16. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	8
17	Підготовка до тестування за пройденим матеріалом.	10
	Разом за семестр:	130

6. ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп’ютерних технологій; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування), з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп’ютерних технологій та технологій дистанційного навчання.

7. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять. а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи та тестування, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів

навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при

	вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів

Аудиторна робота								**Контрольні заходи**	**Семестровий контроль**	
Лабораторні роботи №:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 1-2		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100***
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів навчання з теоретичного матеріалу

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60-65		66-72	73-82		83-89	90-100		
Кількість балів	-	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (40 балів для підсумкового контролю)

Види завдань	Для кожного окремого виду завдань		
	Мінімальний (достатній) бал (задовільно)	Потенційні позитивні бали* (середній бал) (добре)	Максимальний (високий) бал (відмінно)
Питання № 1	12	16	20
Питання № 2	12	16	20
Разом:	**24**		**40**

Примітка. **Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.*

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни	
		Залік	Іспит/диференційований залік
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній вище таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній здобувачем сумі балів відповідно до таблиці Співвідношення.

10. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Основні визначення криптографічних послуг безпеки.
2. Математичні методи сучасної інформаційної безпеки.
3. Принцип Керкгоффса.
4. Види криптографічних протоколів.
5. Властивості, що визначають безпеку криптографічних протоколів.
6. Аналіз і моделювання криптографічних протоколів.
7. Центр сертифікації ключів.
8. Кореневий центр сертифікації.
9. Кроссертифікація.
10. Сертифікат X.509 v3.
11. Список відкликаних сертифікатів. Причини відкликання сертифікату.
12. Протокол OCSP (Online Certificate Status Protocol).
13. Криптоаналітичні атаки та класи стійкості шифрів.
14. Атаки на схеми шифрування.
15. Атака вичерпного пошуку та словникова атака.
16. Атака на основі застосування таблиць передобчислень.
17. Атака розширення довжини на конструкцію Меркля-Дамгарда.
18. Атака «зустріч посередині» на шифр з відкритим ключем.
19. Застосування слабкого протоколу управління ключами.
20. Ідеальний шифр, принципи проєктування та властивості.
21. Безумовно стійкі та практично (обчислювально) стійкі шифри.
22. Метод грубої сили.
23. Парадокс днів народження.
24. Диференційний аналіз.
25. Лінійний аналіз.
26. Метод відпалу.
27. Методи визначення простоти чисел.
28. Методи факторизації великих чисел.
29. Методи цілочислового логарифмування.
30. Алгорим Полларда.
31. Алгоритм Ленстра.
32. Алгоритм факторизації на основі рішення нерівності.
33. Алгоритм дискретного логарифмування.
34. Алгоритм решета числового поля.
35. Криптоаналіз систем на еліптичних кривих.
36. Програмні шифратори, переваги та недоліки.
37. Апаратні шифратори, структура та проблеми застосування.
38. Шифратори для захисту мереж.
39. Криптографічні модулі, їх застосування в задачах криптографічної безпеки.
40. Особливості застосування шифраторів та криптомодулів на об’єктах критичної інфраструктури.
41. Встановлення захищеного каналу. Встановлення доступу до інформації.
42. Сегментування віртуальних машин.
43. Аутентифікація даних і електронний цифровий підпис.
44. Інтелектуальні засоби для криптоаналізу шифрів.
45. Апаратний криптографічний захист. Криптосистема на основі IP-шифраторів.
46. Апаратний криптографічний захист. Криптосистема на основі криптомодулів.
47. Теоретичні основи векторно-модульного-методу модулярного множення та експоненціювання.

48. Проєктування криптосистеми RSA на основі векторно-модульного-методу медулярного множення та експоненціювання.

49. Проєктування криптосистеми Ель-Гамаля на основі векторно-модульного-методу модулярного множення та експоненціювання.

50. Теоретичні основи системи залишкових класів.

51. Методи відновлення десяткового числа за його залишками. Китайська теорема про остачі.

52. Методи проєктування досконалої та модифікованої досконалої форм системи залишкових класів.

53. Методи проєктування симетричних криптосистем на основі залишкових класів.

54. Методи проєктування асиметричних криптосистем на основі залишкових класів.

55. Використання модифікованої досконалої форми системи залишкових класів для проєктування криптосистем.

11. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі для навчання: https://msn.khmnu.edu.ua/course/view.php?id=7850.

12. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: MS Visual Studio 19 або вище, Matlab 2019 або вище тощо.

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Кібербезпека: основи кодування та криптографії: навчальний посібник/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. Харків: Вид. "Новий Світ-2000", 2024. 658 с.
2. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
3. Криптографічний захист інформації: навч. посіб./ О. В. Онацький, Л. Г. Йона, Ю. В. Белова. Одеса: «Астропринт», 2023. 249 с.
4. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
5. Досконала форма системи залишкових класів: методи проєктування та застосування: монографія/ М. М. Касянчук. Тернопіль: ТНЕУ, 2019. 223 с.
6. Штучні нейронні мережі: базові положення. Навчальний посібник/ І.А. Терейковський, Д.А. Бушуєв, Л.О. Терейковська. Київ: КПІ ім. Ігоря Сікорського, 2022. 123 с.
7. С.В.Ткаліченко. Штучні нейронні мережі: Навчальний посібник. Кривий Ріг: Державний університет економіки і технологій, 2023. 150 с.
8. Генетичні алгоритми. Навчальний посібник/ Гордієнко Ю.Г., Кочура Ю.П. Київ: КПІ ім. Ігоря Сікорського, 2022. 329 с.

Додаткова

9. Теорія та практика інфраструктури відкритих ключів/ С.В. Кондакова. Київ: КНУБА, 2022. 32 с.

10. Створення центрів сертифікації ключів [Електронний ресурс]. Режим доступу: https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=2&type=1&id=70

11. Асиметричні алгоритми шифрування у системі залишкових класів/ Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.

12. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.

13. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.

14. Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. 2020. № 6. С. 33-39.

15. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems./ M Kasianchuk, I Yakymenko, V Yatskiv, MP Karpinski, S Yatskiv// IntelITSIS, 2022, P. 365-377

16. The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem/ Kasianchuk M., Yakymenko, I., Yatskiv, S., Gomotiuk, O., Bilovus, L.// CEUR Workshop Proceedings, 2023, 3373, P. 425–436

17. Residue Number System Asymmetric Cryptoalgorithms/ Nykolaychuk, Y.M., Yakymenko, I.Z., Vozna, N.Y., Kasianchuk, M.M.// Cybernetics and Systems Analysis, 2022, 58(4), P. 611–618

18. Methods of crypto-stable symmetric encryption in the residual number system/ Zawislak, S., Kasianchuk, M., Iakymenko, I., Jancarczyk, D.// Procedia Computer Science, 2022, 207, P. 128–137

14. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=7850
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

ТЕОРІЯ КРИПТОСИСТЕМ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	6
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вільно *володіти* державною мовою для представлення результатів діяльності та обговорення питань у сфері криптографічного захисту інформації; чітко *формулювати* висновки й *обґрунтовувати* їх для персоналу, партнерів та інших осіб; *планувати* навчання та контролювати роботу персоналу у сфері управління криптографічними ключами; *здійснювати* дослідницьку діяльність, обираючи та розробляючи відповідні методи захисту; *застосовувати* комп'ютерне моделювання для аналізу процесів; *впроваджувати* та *вдосконалювати* математичні моделі; *аналізувати* та *впроваджувати* кращі світові практики; *розробляти* й *супроводжувати* системи захисту на об'єктах критичної інфраструктури, оцінюючи їх ефективність; *приймати* обґрунтовані організаційно-технічні рішення, зокрема щодо вибору програмного та апаратного забезпечення та його обмежень.

Зміст навчальної дисципліни. Підходи до реалізації сучасних криптографічних систем та протоколів. Квантова криптографія. Проєктування криптосистем RSA та Ель-Гамаля на основі векторно-модульного методу модулярного множення та експоненціювання. Теоретичні основи системи залишкових класів. Методи проєктування криптосистем на основі залишкових класів. Застосування методів криптоаналізу. Управління ключами. Інфраструктура відкритих ключів. Створення центру сертифікації ключів.

Пререквізити – методологія та організація наукових досліджень.

Постреквізити – переддипломна практика, кваліфікаційна робота.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); лабораторні роботи (з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль теоретичного матеріалу.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Кібербезпека: основи кодування та криптографії: навчальний посібник/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. Харків: Вид. "Новий Світ-2000", 2024. 658 с.
2. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
3. Криптографічний захист інформації: навч. посіб./ О. В. Онацький, Л. Г. Йона, Ю. В. Белова. Одеса: «Астропринт», 2023. 249 с.

4. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
5. Штучні нейронні мережі: базові положення. Навчальний посібник/ І.А. Терейковський, Д.А. Бушуєв, Л.О. Терейковська. Київ: КПІ ім. Ігоря Сікорського, 2022. 123 с.
6. С.В.Ткаліченко. Штучні нейронні мережі: Навчальний посібник. Кривий Ріг: Державний університет економіки і технологій, 2023. 150 с.
7. Генетичні алгоритми. Навчальний посібник/ Гордієнко Ю.Г., Кочура Ю.П. Київ: КПІ ім. Ігоря Сікорського, 2022. 329 с.
8. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=7850
9. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: д-р. техн.наук, проф. Касянчук М.М.