ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

"___" _____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптологія
Назва дисципліни

Призначення Робочої програми	Для освітніх програм різних спеціальностей
Рівень вищої освіти	Перший (бакалаврський)
Мова навчання	Українська
Обсяг дисципліни, кредитів ЄКТС	8
Статус дисципліни	Вибіркова
Факультет	Інформаційних технологій
Кафедра	Комп'ютерної інженерії та інформаційних систем

Форма здобуття освіти	Обсяг дисципліни		Кількість годин						Форма семестрового контролю
			Аудиторні заняття					Самостійна робота (в т.ч. ІРС)	
	Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття		Залік
Д	8	240	96	32	32	32		144	+

Робоча програма складена на основі освітніх програм підготовки бакалавра та стандарту вищої освіти спеціальності.

Робоча програма складена _____ к.т.н., доцент Марія Капустян
Підпис Науковий ступінь, вчене звання, Ім'я, Прізвище

Схвалена на засіданні кафедри комп'ютерної інженерії та інформаційних систем
Назва

Протокол від 18.08.2025 №1.

Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Назва Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

3. Пояснювальна записка

Мета дисципліни. Дисципліна "Стандарти та засоби інформаційної безпеки" є однією з вибіркових дисциплін загальної підготовки у підготовці бакалаврів комп'ютерної інженерії.

Метою дисципліни "Стандарти та засоби інформаційної безпеки" є: 1) формування теоретичних знань щодо можливих небезпек і ступеня ризику втрат інформації; 2) формування компетентностей та практичних навичок щодо забезпечення захисту програмної продукції; 3) розвиток у студентів фахового стилю мислення; 4) формування у майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, організації та держави, необхідних для подальшої роботи; 5) вивчення застосування методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Предмет дисципліни. Сучасні стандарти інформаційної безпеки, інформаційні технології у галузі інформаційної безпеки, методи захисту інформації; розробка та впровадження технологій комп'ютерного захисту інформації, забезпечення цілісності даних, конфіденційності; контроль передачі інформації, ідентифікація, автентифікація, криптографія, політика безпеки.

Завдання дисципліни. Надати студентам знання і практичні навички із забезпечення інформаційної безпеки в комп'ютерних системах та мережах.

Після вивчення дисципліни "Стандарти та засоби інформаційної безпеки" студент має досягти таких результатів навчання (сукупність знань, умінь, навичок, компетентностей):

Результати навчання. Після вивчення дисципліни студент повинен: *знати* об'єкт, предмет, задачі, проблематику дисципліни та її основні розділи, наукові і математичні положення, що лежать в основі забезпечення інформаційної безпеки мереж; базові поняття й визначення, використовувані у галузі комп'ютерної інженерії, інновації у галузі технічного та програмного захисту інформації; *вміти:* застосовувати отримані знання для вирішення задач налаштування та обслуговування технічних та програмних засобів захисту інформації відповідно до сучасних стандартів у галузі інформаційної безпеки; застосовувати знання технічних характеристик, призначення засобів захисту інформації в ІС; здійснювати пошук інформації про технічні характеристики, інструкції з експлуатації, особливості налаштування обладнання із захисту інформаційної безпеки; вміти ідентифікувати, класифікувати та описувати можливі канали витоку інформації; поєднувати теорію і практику інформаційної безпеки і організації, а також приймати оптимальні рішення при обслуговуванні та налаштуванні технічних та програмних засобів захисту; *оцінювати* отримані результати та обґрунтовувати прийняті рішення при обслуговуванні та налаштуванні персональних комп'ютерів та периферійного обладнання; вести діалог із замовником та роботодавцем щодо вимог до рівня захищеності інформаційної системи; *вирішувати* складні задачі і проблеми в галузі інформаційної безпеки, що передбачає проведення досліджень та/або здійснення інновацій; *демонструвати* вміння абстрактно мислити, аналізувати стан комплексної системи захисту; *проявляти* здатність вибрати необхідну стратегію при побудові моделі порушника та створенні політики інформаційної безпеки; адмініструвати наявні рішення та методи інформаційної безпеки, змінювати їхні налаштування у відповідності до зміни вимог та/або стандартів у галузі; діяти у складних і непередбачуваних умовах, що потребує застосування нових підходів, креативності, самостійного пошуку помилок, критичного оцінювання своєї поведінки та отриманих результатів; проводити дослідницьку та/або інноваційну діяльність в галузі інформаційної безпеки.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:			
	лекції	**практичні заняття**	**лабора-торні роботи**	**самостійну роботу**
Непарний семестр				
1.Загальні поняття захисту інформації. Закони України про захист інформації. Аналіз даних захисту.	2	2	2	8
2. Політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки.	2	2	2	12
3. Міжнародні стандарти у галузі інформаційної безпеки. Правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем. Метод шифрування. Ключ шифрування.	4	4	4	16
4. Симетричні методи шифрування. Несиметричні методи шифрування. Проблеми та перспективи криптографічних систем. Симетричне шифрування. Асиметричне шифрування та його використання. Управління ключами шифрування.	2	2	2	10
5. Електронний цифровий підпис (ЕЦП). Правовий статус електронного цифрового підпису. Призначення електронного підпису. Необхідність сертифікації засобів ЕЦП і відкритих ключів. Особливості рукописного підпису. Особливості ЕЦП.	4	4	4	16
6. Поняття токенів. Еліптичне шифрування інформації.	2	2	2	8
7. Загальна характеристика систем захисту в інформаційних мережах. Фізична безпека. Аутентифікація та безпека мережі. Паролі. Захист інформації в бездротових локальних мережах.	2	2	2	8
8. Криптостійкість засобів ЕЦП. Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні.	4	4	4	16
9. Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем. Безпека протоколів TCP/IP. Програмні засоби захисту інформації.	4	4	4	16
10. Інформаційні технології та право. Комп'ютерні злочини. Правила роботи з WWW. Обов'язки користувача.	2	2	2	10
11. Правила використання електронної пошти. Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією.	2	2	2	10
12. Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.	2	2	2	14
Разом за непарний семестр:	**32**	**32**	**32**	**144**

Примітка. * по чисельнику – 16 годин, по знаменнику – 16 годин (розрахунок здійснюється відповідно до розкладу занять)

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації *Сьомий семестр*	Кількість годин
1	**Вступ до інформаційної безпеки** Поняття інформації та даних. Загальні поняття захисту інформації. Канал передачі інформації. Канали витоку інформації. Закони України про захист інформації. Аналіз даних захисту.	2
2	**Політика інформаційної безпеки.** Управління безпекою. Розробка правил безпеки.	2
3	**Міжнародні стандарти у галузі інформаційної безпеки.** Правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем. Метод шифрування. Ключ шифрування.	4
4	**Методи шифрування.** Симетричні методи шифрування. Несиметричні методи шифрування. Проблеми та перспективи криптографічних систем. Симетричне шифрування. Асиметричне шифрування та його використання. Управління ключами шифрування.	2
5	**Електронний цифровий підпис (ЕЦП).** Призначення ЕЦП. Необхідність сертифікації засобів ЕЦП і відкритих ключів. Особливості рукописного підпису. Особливості ЕЦП.	4
6	**Еліптичне шифрування інформації.** Поняття токенів. Еліптичне шифрування інформації.	2
7	**Системи захисту в інформаційних мережах.** Загальна характеристика. Фізична безпека. Аутентифікація та безпека мережі. Паролі. Захист інформації в бездротових локальних мережах..	2
8	**Криптостійкість засобів ЕЦП.** Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні.	4
9	**Телекомунікації та віддалений доступ. Резервне копіювання**. Адміністрування інформаційних систем. Безпека протоколів TCP/IP. Програмні засоби захисту інформації.	2
10	**Інформаційні технології та право.** Комп'ютерні злочини. Правила роботи з WWW. Обов'язки користувача.	2
11	**Правила використання електронної пошти.** Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією.	2
12	**Комп'ютерні віруси.** Класифікація і властивості вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.	2
Разом за перший семестр:		**32**

5.2 Зміст практичних занять

№ п/п	Теми практичних занять	К-ть годин
1	***Практичне заняття №1.*** Політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки.	4
2	***Практичне заняття №2.*** Міжнародні стандарти інформаційної безпеки ISO 2700x	4
3	***Практичне заняття №3.*** Симетричні методи шифрування.	4
4	***Практичне заняття №4.*** Несиметричні методи шифрування.	4
5	***Практичне заняття №5.*** Електронний цифровий підпис (ЕЦП**).**	4
6	***Практичне заняття №6.*** Системи захисту в інформаційних мережах.	4
7	***Практичне заняття №7.*** Регламент GDPR. Основні положення.	4
8	***Практичне заняття №8.*** Регламент GDPR. Особливості для роботи з резидентами ЄС.	4
Всього		**32**

5.3 Зміст лабораторних занять

№ п/п	Теми лабораторних робіт	К-ть годин
1	***Лабораторна робота №1.*** Політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки.	4
2	***Лабораторна робота №2.*** Криптографічні методи захисту інформації. Шифр Цезара.	4
3	***Лабораторна робота №3.*** Симетричні методи шифрування.	4
4	***Лабораторна робота №4.*** Несиметричні методи шифрування.	4
5	***Лабораторна робота №5.*** Електронний цифровий підпис (ЕЦП**).**	6
6	***Лабораторна робота №6.*** Системи захисту в інформаційних мережах.	4
7	***Лабораторна робота №7.*** Електронний сертифікат. Адміністрування електронної пошти.	4
8	***Лабораторна робота №8.*** Програми виявлення вірусів та заходи по захисту та профілактиці.	4
Всього		**2**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до практичних занять, лабораторних робіт. До послуг студентів сторінка кафедри у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні матеріали з її навчально-методичного забезпечення та контролю результатів навчання.

Номер тижня	Вид самостійної роботи	Кількість годин
1-2	Опрацювання лекційного матеріалу. Підготовка до ЛР1 та ПЗ1. Підготовка до захисту ЛР1.	18
3-4	Опрацювання лекційного матеріалу. Підготовка до ЛР2 та ПЗ2. Підготовка до захисту ЛР2.	18
5-6	Опрацювання лекційного матеріалу. Підготовка до ЛР3 та ПЗ3. Підготовка до захисту ЛР3	18
7-8	Опрацювання лекційного матеріалу. Підготовка до ЛР4 та ПЗ4. Підготовка до захисту ЛР4.	18
9-10	Опрацювання лекційного матеріалу. Підготовка до ЛР5 та ПЗ5. Підготовка до захисту ЛР5	18
11-12	Опрацювання лекційного матеріалу. Підготовка до ЛР6 та ПЗ6. Підготовка до захисту ЛР6.	18
13-14	Опрацювання лекційного матеріалу. Підготовка до ЛР7 та ПЗ7. Підготовка до захисту ЛР7.	18
15-16	Опрацювання лекційного матеріалу. Підготовка до ЛР8 та ПЗ8. Підготовка до захисту ЛР8	18
	Разом 1-й семестр:	**144**

***Примітки*:** ЛР – лабораторна робота, ПЗ– практичне заняття.

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних технологій); практичні заняття (з використанням інструктування, демонстрування, вирішення типових і прикладних задач, аналізу кейсів, ситуаційних завдань, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних практичних та 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 роботи на практичних заняттях (опитування теоретичного матеріалу, участь у обговоренні ситуацій);

– оцінювання результатів захисту лабораторних робіт.

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, 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 практичних та лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття (наведені у Методичних рекомендаціях до лабораторних занять)), активно працювати на занятті, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами лабораторних робіт тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних занять та під час захисту лабораторних робіт.

Здобувач вищої освіти, виконуючи самостійну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності 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, 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 студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». 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.

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 студентів *денної* форми здобуття освіти у семестрі

Аудиторна робота										**Семестровий контроль**
Лабораторні заняття №:								Практичні заняття (мінімум 3 контрольні точки)		Залік
1*	2	3	4	5	6	7	8	1	2	
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)										
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	3-5	3-5	За рейтингом
48-80								**6-20**		**60-100****

Примітки: *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 на практичних заняттях

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; вільне володіння студентом термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач; результати самостійних робіт.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

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; повнота відповіді та знання.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

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.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий залік виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень 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

10. Питання для самоконтролю результатів навчання

1. Загальні поняття захисту інформації.
2. Закони України про захист інформації.
3. Аналіз даних захисту.
4. Право інтелектуальної власності та політика інформаційної безпеки.
5. Управління безпекою.
6. Розробка правил безпеки.
7. Міжнародні правила застосування шифру.
8. Управління криптографією.
9. Вимоги до криптографічних систем.
10. Метод шифрування.
11. Ключ шифрування.
12. Симетричні методи шифрування.
13. Несиметричні методи шифрування.
14. Проблеми та перспективи криптографічних систем.
15. Симетричне шифрування.
16. Асиметричне шифрування та його використання.
17. Управління ключами шифрування.
18. Правовий статус електронного цифрового підпису
19. Призначення електронного підпису.
20. Необхідність сертифікації засобів ЕЦП і відкритих ключів.
21. Особливості рукописного підпису.
22. Особливості ЕЦП.
23. Поняття токенів.
24. Еліптичне шифрування інформації.
25. Загальна характеристика систем захисту в інформаційних мережах.

26. Фізична безпека.
27. Автентифікація та безпека мережі.
28. Паролі.
29. Захист інформації в бездротових локальних мережах.
30. Криптостійкість засобів ЕЦП.
31. Поняття електронного сертифікату.
32. Моделі систем сертифікації.
33. Проблеми та перспективи впровадження ЕЦП в Україні.
34. Користувацький інтерфейс.
35. Телекомунікації та віддалений доступ.
36. Резервне копіювання.
37. Адміністрування інформаційних систем.
38. Безпека протоколів TCP/IP.
39. Програмні засоби захисту інформації.
40. Інформаційні технології та право.
41. Комп'ютерні злочини.
42. Правила роботи з WWW.
43. Обов'язки користувача.
44. Правила використання електронної пошти.
45. Адміністрування електронної пошти.
46. Використання електронної пошти для конфіденційного обміну інформацією.
47. Комп'ютерні віруси та їх властивості.
48. Класифікація вірусів.
49. Основні види комп'ютерних вірусів та схеми їх функціонування.
50. Структура комп'ютерних вірусів.
51. Програми виявлення вірусів та заходи по захисту та профілактиці.
52. ISO 27001.
53. Регламент GDPR.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Стандарти та засоби інформаційної безпеки» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою.

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

Вивчення навчальної дисципліни не потребує використання спеціального програмного прикладного забезпечення, крім загальновживаних програм і операційних систем.

13. Рекомендована література:

1. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є. Забезпечення інформаційної безпеки держави: підручник/ МОН України, НАУ. – Київ: НАУ, 2016. – 256 с.
2. Зибін С.В., В.В. Кузавков, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. Стандартизація та правове забезпечення інформаційної безпеки: навчальний посібник/ МОН України, НАУ. –Е.: ЦП «Компринт», 2020. – 140 с.
3. Захист інформації в комп'ютерних системах: підручник / В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. –Ніжин: ФОП Лукяненко В.В., ТПК «Орхідея», 2020. -236 с.
4. Бабак В.П. Теоретичні основи захисту інформації: підручник/ НАУ; МОН. – Київ, 2008. – 751 с.
5. Захист систем електронних комунікацій : навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ : Київ. нац. торг.-екон. ун-т, 2019. -164 с.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/course/view.php?id=7741
2. Електронна бібліотека університету. URL: http://library.khmnu.edu.ua/
3. Репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

МОБІЛЬНО-ОРІЄНТОВАНА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (*бакалаврський*)
Мова викладання	Українська
Семестр	–
Кількість призначених кредитів ЄКТС	8,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *знати* об'єкт, предмет, задачі, проблематику дисципліни та її основні розділи, наукові і математичні положення, що лежать в основі забезпечення інформаційної безпеки мереж; базові поняття й визначення, використовувані у галузі комп'ютерної інженерії, інновації у галузі технічного та програмного захисту інформації; *вміти:* застосовувати отримані знання для вирішення задач налаштування та обслуговування технічних та програмних засобів захисту інформації відповідно до сучасних стандартів у галузі інформаційної безпеки; застосовувати знання технічних характеристик, призначення засобів захисту інформації в ІС; здійснювати пошук інформації про технічні характеристики, інструкції з експлуатації, особливості налаштування обладнання із захисту інформаційної безпеки; вміти ідентифікувати, класифікувати та описувати можливі канали витоку інформації; поєднувати теорію і практику інформаційної безпеки і організації, а також приймати оптимальні рішення при обслуговуванні та налаштуванні технічних та програмних засобів захисту; *оцінювати* отримані результати та обґрунтовувати прийняті рішення при обслуговуванні та налаштуванні персональних комп'ютерів та периферійного обладнання; вести діалог із замовником та роботодавцем щодо вимог до рівня захищеності інформаційної системи; *вирішувати* складні задачі і проблеми в галузі інформаційної безпеки, що передбачає проведення досліджень та/або здійснення інновацій; *демонструвати* вміння абстрактно мислити, аналізувати стан комплексної системи захисту; *проявляти* здатність вибрати необхідну стратегію при побудові моделі порушника та створенні політики інформаційної безпеки; адмініструвати наявні рішення та методи інформаційної безпеки, змінювати їхні налаштування у відповідності до зміни вимог та/або стандартів у галузі; діяти у складних і непередбачуваних умовах, що потребує застосування нових підходів, креативності, самостійного пошуку помилок, критичного оцінювання своєї поведінки та отриманих результатів; проводити дослідницьку та/або інноваційну діяльність в галузі інформаційної безпеки.

Зміст навчальної дисципліни. Загальні поняття захисту інформації. Закони України про захист інформації. Аналіз даних захисту. Право інтелектуальної власності та політика інформаційної безпеки. Управління безпекою. Розробка правил безпеки. Міжнародні правила застосування шифру. Управління криптографією. Вимоги до криптографічних систем. Метод шифрування.Ключ шифрування. Симетричні методи шифрування.Несиметричні методи шифрування. Проблеми та перспективи криптографічних систем. Симетричне шифрування. Асиметричне шифрування та його використання. Управління ключами шифрування. Правовий статус електронного цифрового підпису. Призначення електронного підпису. Необхідність сертифікації засобів ЕЦП і відкритих ключів. Особливості рукописного підпису. Особливості ЕЦП. Поняття токенів. Еліптичне шифрування інформації. Загальна характеристика систем захисту в інформаційних мережах. Фізична безпека.Аутентифікація та безпека мережі. Паролі. Захист інформації в бездротових локальних мережах. Криптостійкість засобів ЕЦП. Поняття електронного сертифікату. Моделі систем сертифікації. Проблеми та перспективи впровадження ЕЦП в Україні. Користувацький інтерфейс. Телекомунікації та віддалений доступ. Резервне копіювання. Адміністрування інформаційних систем. Безпека протоколів TCP/IP; Програмні засоби захисту інформації. Інформаційні технології та право. Комп'ютерні злочини. Правила роботи з WWW. Обов'язки користувача. Правила використання електронної пошти. Адміністрування електронної пошти. Використання електронної пошти для конфіденційного обміну інформацією. Комп'ютерні віруси та їх властивості. Класифікація вірусів. Основні види комп'ютерних вірусів та схеми їх функціонування. Структура комп'ютерних вірусів. Програми виявлення вірусів та заходи по захисту та профілактиці. Антивірусні пакети.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів, інформаційно-комунікаційних

технологій); практичні заняття (з використанням інструктування, демонстрування, вирішення типових і прикладних задач, аналізу кейсів, ситуаційних завдань, елементів дискусії тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання практичних робіт, поточного та підсумкового контролю, виконання індивідуальних та домашніх завдань), з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання практичних та лабораторних робіт.

Вид семестрового контролю: залік.

Навчальні ресурси:

1. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є. Забезпечення інформаційної безпеки держави: підручник/ МОН України, НАУ. – Київ: НАУ, 2016. – 256 с.
2. Зибін С.В., В.В. Кузавков, І.В. Пискун, В.О. Хорошко, Ю.Є. Хохлачова. Стандартизація та правове забезпечення інформаційної безпеки: навчальний посібник/ МОН України, НАУ. –Е.: ЦП «Компринт», 2020. – 140 с.
3. Захист інформації в комп'ютерних системах: підручник / В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. –Ніжин: ФОП Лукяненко В.В., ТПК «Орхідея», 2020. -236 с.
4. Бабак В.П. Теоретичні основи захисту інформації: підручник/ НАУ; МОН. – Київ, 2008. – 751 с.
5. Захист систем електронних комунікацій : навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ : Київ. нац. торг.-екон. ун-т, 2019. -164 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=7741
7. Електронна бібліотека університету. Доступ до ресурсу: http://library.khmnu.edu.ua/

Викладач: к.т.н., доцент Капустян М.В.