**ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ЗАТВЕРДЖУЮ**
Декан факультету IT
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«__08__» _____ 2023 р.

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## *Основи інформаційної безпеки*

| | |
|---|---|
| ***Галузь знань*** | 12 – Інформаційні технології |
| ***Спеціальність*** | 125 – Кібербезпека та захист інформації |
| ***Рівень вищої освіти*** | Перший бакалаврський |
| ***Освітньо-професійна програма*** | Кібербезпека та захист інформації |
| ***Обсяг дисципліни*** | 5 кредитів ЄКТС |
| ***Шифр дисципліни*** | ОПП.01 |
| ***Мова навчання*** | Українська |
| ***Статус дисципліни*** | Обов'язкова, дисципліна професійної підготовки |
| ***Факультет*** | Інформаційних технологій |
| ***Кафедра*** | Кібербезпеки |

| Форма навчання | Курс | Семестр | Обсяг дисципліни | | Кількість годин | | | | | | Курсовий проєкт | Курсова робота | Форма семестрового контролю | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Аудиторні заняття | | | | | Самостійна робота, у т.ч. ІРС | | | | |
| | | | Кредити ЄКТС | Години | Разом | Лекції | Лабораторні роботи | Практичні заняття | Семінарські заняття | | | | Залік | Іспит |
| Очна (денна) | 1 | 1 | 5 | 150 | 51 | 17 | 34 | | | 99 | | | + | |

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доц. Юрій КЛЬОЦ

_____ Наталія ПЕТЛЯК
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

# ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

| | |
|---|---|
| **Тип дисципліни** | Обов'язкова |
| **Рівень вищої освіти** | Перший (бакалаврський) |
| **Мова викладання** | Українська |
| **Семестр** | Перший |
| **Кредити ЄКТС** | 5,0 |
| **Форми навчання, для яких викладається дисципліна** | Очна денна |

Студент, який успішно завершив вивчення дисципліни, повинен: *виявляти* загальні знання та розуміння предметної області та розуміння професії; *мати* базові знання та практичні навички з використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, в тому числі для забезпечення функціонування спеціального програмного забезпечення з захисту інформації від руйнуючих програмних впливів, а також для вирішення завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами і оцінки результативності якості прийнятих рішень; використовувати інформаційно-комунікаційних технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем*; вирішувати* базові задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

**Зміст навчальної дисципліни**. Загальні принципи безпеки інформаційних технологій. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації. Методи та засоби блокування технічних каналів витоку інформації. Основи безпеки даних в комп'ютерних системах. Ідентифікація і автентифікація користувачів. Основи захисту даних.

**Пререквізити:** вихідна

**Кореквізити:** Операційні системи та технології їх захисту, Нормативно-правове забезпечення кібербезпеки, Безпека вебресурсів

**Запланована навчальна діяльність:** лекції – 17 год., лабораторних робіт – 34 год., самостійної роботи 99 год., разом 150 год.

**Методи навчання**: пояснювально-ілюстративні, практичні, репродуктивні, ігрові, модульно-розвивальні, застосування інформаційно-комп'ютерних технологій (Virtual Box, R-Studio, інструменти та утиліти ОС Windows та Linux Ubuntu).

**Форми оцінювання результатів навчання**: усне опитування, тестування, захист лабораторних робіт.

**Вид семестрового контролю:** залік.

**Навчальні ресурси:**

1. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
2. Кушнерьов. О.С. Безпека інформації : конспект лекцій – Суми : Сумський державний університет, 2021. – 99 с.
3. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підр.. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
5. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

**Викладач:** Петляк Н.С.

## ВСТУП

Дисципліна „Основи інформаційної безпеки” - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації».

**Мета дисципліни.** Метою дисципліни "Основи інформаційної безпеки" є: формування термінологічного фундаменту, знань та розуміння предметної області; ознайомлення студентів із основними методами, принципами та алгоритмами захисту інформації в інформаційних системах.

**Предмет дисципліни.** Основи забезпечення інформаційної та кібербезпеки.

**Завдання дисципліни.** Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації”:

***компетентності:***

КЗ 01. Здатність застосовувати знання у практичних ситуаціях;

КФ 01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 02. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

КФ 04. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

КФ 05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

***результати навчання:***

РН 02. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 05. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень;

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах;

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

Студент, який успішно завершив вивчення дисципліни, повинен: *виявляти* загальні знання та розуміння предметної області та розуміння професії; *мати* базові знання та практичні навички з використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах, в тому числі для забезпечення функціонування спеціального програмного забезпечення з захисту інформації від руйнуючих програмних впливів, а також для вирішення завдання захисту програм та інформації, що

обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами і оцінки результативності якості прийнятих рішень; використовувати інформаційно-комунікаційних технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем*; вирішувати* базові задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

**СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ**

| Назва теми | Кількість годин, відведених на: | | |
|---|---|---|---|
| | **лекції** | **лабораторні роботи** | **самостійну роботу** |
| Тема 1. Основи інформаційної безпеки | 6 | 8 | 30 |
| Тема 2. Архітектура комп'ютерів | 6 | 12 | 30 |
| Тема 3. Безпека мереж | 2 | 4 | 16 |
| Тема 4. Особливості застосування інформаційної безпеки | 3 | 8 | 23 |
| **Разом:** | **17** | **34** | **99** |

## ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
### Зміст лекційного курсу

| Номер лекції | Перелік тем лекцій, їх анотації | Кількість годин |
|---|---|---|
| | **Тема 1. Основи інформаційної безпеки** | |
| **1** | **Загальні основи інформаційної безпеки**<br>Основні поняття та стандарти інформаційної безпеки. Класифікація загроз інформаційної безпеки. Основні характеристики інформації.<br>Літ.: [3] с.8-37; [7] с.8-27; [8] с.7-62. | 2 |
| **2** | **Основні принципи кібербезпеки**<br>Принципи кібербезпеки і приватності. Знання основних правил кібергігієни.<br>Літ.: [1] с.83-85, [4] с.35-102 | 2 |
| **3** | **Безпечне використання корпоративних систем обміну повідомленнями**<br>Корпоративні системи обміну повідомленнями (чати та інші) і відповідне програмне забезпечення. Вміння ними безпечно користуватися та адмініструвати їх.<br>Літ.: [9] с.500-547, [10] с.5-17, [11] с.1-9 | 2 |
| | **Тема 2. Архітектура комп'ютерів** | |
| **4** | **Архітектура комп'ютерів**<br>Архітектура комп'ютерів (друковані плати, мікросхеми, процесори, елементи пам'яті тощо). Типи комп'ютерних архітектур.<br>Літ.: [1] с.146-148 | 2 |
| **5** | **Компоненти системи та робота з операційною системою**<br>Призначення ОС, класифікація ОС, архітектури ОС, вразливості ОС.<br>Літ.: [12] с.8-35 | 2 |
| **6** | **Базові програми для забезпечення безпеки**<br>Типи ПЗ для забезпечення безпеки. Встановлення та налаштування базових програм (антивірусів, файерволів, програм резервування та архівування даних).<br>Літ.: [1] с.316-343, [13] с.128-145, с.240-254 | 2 |
| | **Тема 3. Безпека мереж** | |
| **7** | **Комп'ютерні мережі**<br>Принципи обміну інформацією в мережах. Мережа ETHERNET, типи мережевих пристроїв та їх призначення. Типи мереж. Мережева модель OSI. Основні протоколи стеку TCP/IP<br>Літ.: [1] с.126-138, [5] с.106-127 | 2 |
| | **Тема 4. Особливості застосування інформаційної безпеки** | |
| **8** | **Основи безпеки даних в комп'ютерних системах**<br>Основні поняття щодо захисту інформації в автоматизованих системах. Загрози безпеки даних та їх особливості. Канали проникнення та принципи побудови систем захисту. Основи фізичного захисту об'єктів.<br>Літ.:[6] с.76-102, [2] с.31-41 | 2 |
| **9** | **Забезпечення інформаційної безпеки у соціальних інтернет-сервісах**<br>Поняття соціальних інтернет-сервісів (СІС). Вплив СІС на психіку користувачів. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави. Протидія впливу СІС.<br>Літ.:[2] с.43-65, с.79-92, [14] с.1-11 | 1 |
| | **Разом:** | **17** |

**Перелік лабораторних робіт**

| № з/п | Теми лабораторних робіт | Кількість годин |
|---|---|---|
| 1 | Кодування та шифрування даних як основа інформаційної безпеки<br>Літ.: [15] | 4 |
| **2** | Безпечне використання корпоративних систем обміну повідомленнями<br>Літ.: [30-31] | 4 |
| **3** | Організація та підтримка контролю цілісності даних та парольного доступу<br>Літ.: [7] с.163-167, [8], [32] | 4 |
| **4** | Встановлення віртуальних машин та операційних систем, інтеграція та оптимізація компонентів системи<br>Літ.:[3] с.270-295, [26], [33] | 4 |
| **5** | Захист від шкідливих програм, відновлення та резервування даних<br>Літ.: [6] с.106-121, [35-37] | 4 |
| **6** | Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів<br>Літ.: [3] с.105-159, [26], [40-41] | 4 |
| **7** | Дослідження і налаштування інтегрованих засобів операційних систем для захисту даних<br>Літ.: [1] с.40-69, с.195-234; [42] | 4 |
| **8** | Безпечна робота із соціальними інтернет-сервісами та інструменти виявлення неправдивих повідомлень<br>Літ.: [43-46] | 4 |
| **9** | Підсумкове заняття. Тестування | 2 |
| | **Разом:** | 34 |

## НЕФОРМАЛЬНЕ НАВЧАННЯ

Проходження студентами альтернативних он-лайн курсів з дисципліни та пред'явлення ними відповідних сертифікатів дає змогу зарахувати лабораторні роботи, а саме:

1) сертифікат з курсу "Основи інформаційної безпеки" (https://courses.prometheus.org.ua/courses/KPI/IS101/2014_T1/about ) - лабораторні роботи №1,3;

2) сертифікат з курсу "Cybersecurity Essentials" (https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials) - лабораторні роботи №5,7;

3) сертифікат з курсу "IT Essentials: PC Hardware and Software" (https://www.netacad.com/courses/os-it/it-essentials) - лабораторну роботу №4,6.

**Зміст самостійної (індивідуальної) роботи**

На самостійне опрацювання студентів виноситься опрацювання лекційного матеріалу, підготовка до виконання і захисту лабораторних робіт та змістовних модулів. Керівництво самостійною роботою та виконанням завдань здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

| Номер тижня | Вид самостійної роботи | Кількість годин |
|---|---|---|
| 1 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №1. | 6 |
| 2 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №1. | 6 |
| 3 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №2. | 5 |
| 4 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №2. | 6 |
| 5 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №3. | 6 |
| 6 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №3. | 6 |
| 7 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №4. | 6 |
| 8 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №4. | 6 |
| 9 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №5. | 6 |
| 10 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №5. | 6 |
| 11 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №6. | 6 |
| 12 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №6. | 6 |
| 13 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №7. | 6 |
| 14 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №7. | 6 |
| 15 | Опрацювання теоретичного матеріалу. Підготовка до виконання лабораторної роботи №8. | 6 |
| 16 | Опрацювання теоретичного матеріалу. Підготовка до захисту лабораторної роботи №8. | 6 |
| 17 | Опрацювання лекційного матеріалу. Підготовка до підсумкового тестового контролю. | 4 |
| | **Разом:** | **99** |

## ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів, зокрема: лекції (з використанням пояснювально-ілюстративних та репродуктивних методів та засобів візуалізації); лабораторні роботи (з використанням практичних, ігрових, модульно-розвивальних методів, з застосування інформаційно-комп'ютерних технологій (Virtual Box, R-Studio, інструменти та утиліти ОС Windows та Linux Ubuntu).

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: виконання частини лабораторних робіт передбачає роботу у малих групах з призначенням тім-лідера, що сприяє розвитку лідерських якостей у студентів, здатності до спілкування і організації командної роботи над спільними задачами, а змінюваність складу робочих груп між лабораторними роботами сприяє розвитку навичок адаптованості, гнучкості, комунікативності і оперативного налагоджування міжособистісних відносин в різних колективах; 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 тестових 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 зарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.pdf .

## МЕТОДИ КОНТРОЛЮ

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:

- усне опитування;
- захист лабораторних робіт;
- тестування.

Семестровий контроль проводиться у формі заліку. Виведення підсумкової семестрової оцінки виконується за результатами поточного контролю

## ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

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 у семестрі за ваговими коефіцієнтами**

| | Аудиторна робота | Контрольні заходи | Семестровий контроль |
|---|---|---|---|
| Вид заняття | Лабораторні роботи №: | Тестовий контроль | Залік за рейтингом |
| Тема | 1-4 | Т 1-4 | |
| Ваговий коефіцієнт | 0,6 | 0,4 | |

**Оцінювання лабораторних занять.** Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і графічної частини; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Для виконання програми дисципліни студент повинен отримати 8 оцінок за лабораторні роботи.

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

Оцінку, отриману за лабораторну роботу, викладач оголошує студенту одразу після його відповіді і проставляє в електронний журнал дисципліни.

**Оцінювання тестових завдань.** Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20.

Оцінювання здійснюється за чотирибальною шкалою.

**Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту**

| Сума балів за тестове завдання | 0-11 | 12-14 | 15–18 | 19-20 |
|---|---|---|---|---|
| Оцінка за 4-ри бальною шкалою | 2 | 3 | 4 | 5 |

На тестування відводиться 20 хвилин. Тестування проводиться з використанням модульного середовища для навчання MOODLE. Правильні відповіді студент реєструє в он-лайн режимі в модульному середовищі MOODLE. Через 20 хвилин студенти завершують тестування та надсилають свої відповіді на сервер. Викладач оголошує результати тестування згідно журналу оцінок модульного середовища MOODLE.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

**Критерії оцінювання знань студентів**

| Оцінка за інституційною шкалою | Узагальнений критерій |
|---|---|
| Відмінно | Студент 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 державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки. |
| Добре | Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, 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 закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки. |
| Задовільно | Студент 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 студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, 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 | Студент 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 студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни. |

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

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно".

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

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

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** | | **Вітчизняна оцінка, критерії** | |
|---|---|---|---|---|
| A | 4,75–5,00 | | Зараховано | ***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків |
| B | 4,25–4,74 | | | ***Добре*** – повне знання навчального матеріалу з кількома незначними помилками |
| C | 3,75–4,24 | | | ***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками |
| D | 3,25–3,74 | | | ***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією |
| E | 3,00–3,24 | | | ***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання |
| FX | 2,00–2,99 | | Незараховано | ***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни |
| F | 0,00–1,99 | | | ***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни |

## ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Способи подання інформації.
2. Основні характеристики інформації.
3. Основні принципи кібербезпеки.
4. Правила кібергігієни.
5. Корпоративні системи обміну повідомленнями (чати та інші) і відповідне програмне забезпечення.
6. Адміністрування корпоративних систем обміну повідомленнями
7. Системи числення.
8. Архітектура комп’ютерів.
9. Типи комп’ютерних архітектур.
10. Призначення ОС
11. Класифікація ОС
12. Архітектури ОС
13. Вразливості ОС
14. Будова комп'ютерних систем.
15. Комп'ютерні мережі.
16. Мережева модель OSI
17. Основні протоколи стеку TCP/IP
18. Зміст і основні поняття комп'ютерної безпеки
19. Основні поняття та стандарти інформаційної безпеки.
20. Класифікація загроз інформаційної безпеки.
21. Основні характеристики інформації.
22. Інформація як об’єкт посягань і захисту
23. Основні поняття щодо захисту інформації в автоматизованих системах.
24. Загрози безпеки даних та їх особливості.
25. Захист даних від комп'ютерних вірусів.
26. Шкідливі програми на ЕОМ.
27. Засоби захисту від комп'ютерних вірусів та їх особливості.
28. Вбудовані засоби операційних систем для захисту даних
29. Відновлення та резервування даних
30. Поняття соціальних інтернет-сервісів (СІС).
31. Вплив СІС на психіку користувачів.
32. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави.
33. Протидія впливу СІС.

## МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни "Основи інформаційної безпеки" повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

## РЕКОМЕНДОВАНА ЛІТЕРАТУРА

### Основна


1. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький: ЦНТУ, 2022. – 967 с.
2. Кушнерьов. О.С. Безпека інформації : конспект лекцій – Суми : Сумський державний університет, 2021. – 99 с.
3. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020.– 236 с.
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.
5. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посібник - Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
6. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. - Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
7. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інфомаційна та кібербезпека – К.: ДУТ, 2015. – 288 с.
8. Грабар І. Г., Грищук Р. В., Молодецька К. В.; за заг. ред. Грищука Р. В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія – Житомир: ЖНАЕУ, 2019. – 280 с.
9. Бобало Ю. Я. та ін.; за заг. ред. д-ра техн. наук, проф. Бобала Ю. Я. та д-ра техн. наук, доц. Горбатого І. В. Інформаційна безпека: навч. посіб. - Львів: Видавництво Львівської політехніки, 2019. 580 с.
10. Бибка О.І. Конспект лекцій з дисципліни „Автоматизація адміністрування мережної інфраструктури" - Харків: ХНУРЕ, 2020. - 51с.
11. Архипова, Е., & Гудела, М. (2020). MODERN TRENDS IN THE FORMATION OF THE CORPORATE COMMUNICATION SYSTEM IN PUBLIC AUTHORITIES. SWorldJournal, 3(06-03), 75–83. https://doi.org/10.30888/2663-5712.2020-06-03-028
12. Федотова-Півень І. М., Миронець І. В., Півень О. Б., Сисоєнко С. В., Миронюк Т. В.; за ред. В. М. Рудницького. Операційні системи: навч.посіб. - Харків: ТОВ «ДІСА ПЛЮС»,2019. 216с.
13. Жаровський Р.О. Захист інформації у комп'ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
14. Sokolov, V. Y., & Kurbanmuradov, D. M. (2018). МЕТОДИКА ПРОТИДІЇ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(1), 6–16. https://doi.org/10.28925/2663-4023.2018.1.616
15. Олександр Мізюк. Системи числення. https://nrs.rozh2sch.org.ua/


### Додаткова


16. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 від 08.10.1997.
17. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.
18. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.
19. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200.
20. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах

від несанкціонованого доступу.
21. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
22. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної ради України. – 1994. – №31.
23. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT). Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. – Чинний від 2016-27-12. – Київ: ДП «УкрНДНЦ», 2018. – [50] с.
24. Барабаш О. В. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних інтернет-сервісів / О. В. Барабаш, Р. В. Грищук, К. В. Молодецька-Гринчук // Наукоємні технології. – 2018. – № 2 (38). – С. 232–239. – Режим доступу: http://jrnl.nau.edu.ua/index.php/SBT/article/view/12855
25. Молодецька К. В. Механізми синергетично керованої самоорганізації акторів у соціальних інтернет-сервісах / К. В. Молодецька // Управління розвитком. – 2018. – Т. 4, вип. 4. – С. 1–13. – Режим доступу: http://ir.znau.edu.ua/handle/123456789/9582
26. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
27. Peter Dordal. An Introduction to Computer Networks / Peter Dordal, Loyola. – Independent, 2020. – 886c.
28. Кібергігієна. Кібербезпека. Безпека держави: матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ: Київ. нац. торг.-екон. ун-т, 2020. –101 с.
29. Основні правила кібергігієни. Дата звернення 15.07.2023: https://cert.gov.ua/recommendation/31
30. Gursev Singh Kalra. "Threat analysis of an enterprise messaging system". [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1353485814701217#preview-section-abstract
31. Gerardus Blokdyk. (2019). Secure Messaging: A Complete Guide. Inc. ISBN: 0655820469. 480 p.
32. National Institute of Standards and Technology. (2017). An Introduction to Information Security. Special Publication 800-12r1. 101 p. Режим доступу : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
33. The Art of Service - Virtual Machines Publishing. (2021). Virtual Machines: A Complete Guide. Packt Publishing. ISBN: 186743556X. 500 p.
34. Захист від шкідливих програм і відновлення та резервування даних
35. Peter Dordal. An Introduction to Computer Networks / Peter Dordal, Loyola. – Independent, 2020. – 886c.
36. S. Gokulakrishnan and J. M. Gnanasekar, “Data integrity and recoverymanagement under peer-to-peer convoluted fault recognition cloud sys-tems,” Journal of Computational and Theoretical Nanoscience, vol. 17,no. 5, pp. 2147–2150, 2020.
37. FreeVacy. (2023). Resources. [Електронний ресурс]. – Режим доступу : https://www.freevacy.com/resources
38. Організація безпеки мереж на основі SOHO-маршрутизаторів та використання брандмауерів
39. Kim D. Fundamentals of information systems security / David Kim, Michael G. Solomon. – Third edition. – Burlington :Jones & Bartlett Learning, 2018. – 571 p.
40. LazyAdmin, (2020) Home Network Security, [Електронний ресурс]. – Режим доступу : https://lazyadmin.nl/home-network/home-network-security
41. National Security Agency. (2022). Network Infrastructure Security Guide. [Електронний ресурс]. – Режим доступу : https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615
42. Hamdani, Syed Wasif Abbas, et al. “Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons.” ACM Computing Surveys (CSUR) 54.3 (2021): 1-36.
43. Безпечна робота із соціальними інтернет сервісами та інструменти виявлення неправдивих повідомлень

44. Zhou, X., & Zafarani, R. (2020). A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. ACM Computing Surveys, 53(5), 1–40.
45. Social Engineering. [Електронний ресурс]. – Режим доступу : https://www.imperva.com/learn/application-security/social-engineering-attack/
46. Gardner, B. (2018). Social Engineering in Non-Linear Warfare. Journal of Applied Digital Evidence, 1(1). [Електронний ресурс]. – Режим доступу : http://mds.marshall.edu/jade/vol1/iss1/1

## ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/.
2. Електронна бібліотека університету. URL: http://library.khmnu.edu.ua/