**МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ**

**Комп'ютерної інженерії та інноваційних технологій**

**«ПРИЙНЯТО»**
Вченою радою
Міжнародного гуманітарного
університету
Протокол № ____
від «____»_____ 20___

**Введено в дію наказом ректора**
Міжнародного гуманітарного
університету від 30.08.24 № ___

Ректор _____ К.В. Громовенко

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# КОМПЛЕКСНІ СИСТЕМИ БЕЗПЕКИ

| | |
|---|---|
| Галузь знань | 12 Інформаційні технології |
| Спеціальність | 125 Кібербезпека та захист інформації |
| Назва освітньої програми | Кібербезпека |
| Рівень вищої освіти | другий (магістерський) рівень |

Одеса – 2024

Робоча програма затверджена на засіданні кафедри Комп'ютерної інженерії та інноваційних технологій протокол №1 від 29.08.24 2024 року.

| Розробники і викладачі | Контактний тел. | E-mail |
|---|---|---|
| доцент кафедри Комп'ютерної інженерії та інноваційних технологій **Онацький Олексій Віталійович** | 0503761048 | onatsky@meta.ua |

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій, доцент _____ Лариса ЙОНА

Гарант освітньої програми _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лариса РАЙЧЕВА

## 1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 3<br><br>Загальна кількість годин – 90</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="5">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">1-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="9">Мова навчання – українська</td><td rowspan="9">Рівень вищої освіти – другий (магістерський) рівень</td><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>62 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Дисципліна **Комплексні системи безпеки** є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов’язковим компонентом освітньої програми для здобуття освітнього рівня «магістр» та забезпечує студентів базовими знаннями з проблем захисту інформаційних ресурсів у системах телекомунікації та мережах від порушення її конфіденційності, цілісності та доступності; етапів створення комплексної системи захисту інформації (КСЗІ), формування вимог до КСЗІ, вимогам щодо захисту інформації від несанкціонованого доступу, проектування КСЗІ в інформаційно-комунікаційних системах (ІКС), введення КСЗІ в ІКС в дію та її супровід

**Метою** викладання навчальної дисципліни Комплексні системи безпеки ознайомлення студентів з принципами побудови системи захисту та етапи створення комплексних систем захисту інформації з застосуванням існуючої нормативної бази в Україні; розвиток у студентів практичних навичок у послідовності розробки КСЗІ; підготовка висококваліфікованих фахівців, здатних ставити завдання на виконання етапів створення КСЗІ

**Передумови для вивчення дисципліни.** Знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки. Передбачає підвищення професійної компетентності фахівців з кібербезпеки та сприяє ефективній самореалізації їх.

## 2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Комплексні системи безпеки» формуються наступні компетентності із передбачених освітньою програмою:

**Інтегральна компетентність**

ІК1. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

**Загальні компетентності**

КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні.

КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

**Спеціальні (фахові, предметні) компетентності**

КФ1. 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.

КФ2. 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.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захистуінформації 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.

**Програмні результати навчання**

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. 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.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН23. 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.

**Заплановані результати навчання за навчальною дисципліною**

***Знання***

Основні положень законодавчої та нормативно-правової бази України в галузі захисту інформації; основи, напрямки, етапи побудови систем захисту інформації; основні принципи побудови системи захисту; технологію проектування системи захисту інформації; моделі загроз безпеці інформації та потенційні ризики; оцінку ефективності систем захисту інформації; програмно-технічні методи й засоби захисту інформації; порядок проведення робіт щодо створення комплексної системи захисту інформації на об'єкті інформаційної діяльності.

***Уміння***

Виконати оцінку якості систем захисту інформації на основі матриці знань; виконати оцінку якості систем захисту інформації на основі аналізу профілю безпеки; визначення політики інформаційної безпеки, організаційно-технічних заходів на об'єкті інформаційної діяльності; виконати модель загроз безпеці інформації; виконати оцінку ефективності систем захисту інформації; визначати структури та складу, завдань і функцій, обов'язків і відповідальності служби захисту інформації при побудови систем захисту інформації; виконати розроблення та впровадження заходів із захисту інформації; розробляти технічне завдання на створення комплексної системи захисту інформації; розробляти моделі порушника безпеки інформації; розробляти моделі загроз для інформації в інформаційно-комунікаційних системах; оцінювати рівень гарантій та функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

***Навички***

Ефективного спілкування в кіберпросторі, провадження професійної діяльності за допомогою сучасних інформаційно-комунікаційних технологій; провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації; оцінювати захищеність систем, комплексів та засобів; обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти в галузі інформаційної безпеки та/або кібербезпеки; обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки; аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

## 3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Тема 1. Системний підхід до вирішення проблеми захисту інформації**

Основні положення інформаційної безпеки. Поняття інформаційної безпеки, основні задачі. Основні положення системи захисту інформації. Об'єктно-орієнтований підхід до інформаційної безпеки. Компоненти моделі безпеки інформації. Поняття інформації. Види інформації. Властивості інформації. Важливість інформації в сучасному світі. **З**агрози безпеці інформації. Основні поняття і класифікація загроз**. З**агрози доступності, цілісності, конфіденційності. Порушники інформаційної безпеки.

**Тема 2. Основні етапи створення систем захисту інформації**

Основи, напрями захисту інформації, етапів побудови СЗІ. Законодавча, нормативно-правова, методична бази забезпечення захисту інформації. Структура й завдання органів (підрозділів), що забезпечують безпеку інформаційних технологій. Організаційно-технічні та режимні заходи і методи захисту інформації. Цикл етапів (кроків) побудови систем захисту

інформації (СЗІ). Матриця інформаційної безпеки (ІБ) блоків "основи", "напрями" і "етапи". Процес формування СЗІ з використанням матриці ІБ. Елементи матриці ІБ.

**Тема 3. Функціональні вимоги безпеки стандарту ISO/IEC 15408**

Стандарти і специфікації в галузі безпеки інформаційних систем. Класи безпеки інформаційних систем. Технічна специфікація X.800. Стандарт ISO/IEC 15408. Профіль захисту. Завдання з безпеки. Функціональний пакет. Базовий профіль захисту Функціональні вимоги. Функціональні класи, сімейства, компоненти. Форма представлення вимог довіри. Порядок виконання зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004. Відомості щодо відповідності функціональних компонентів безпеки згідно з ISO/IEC 15408 вимогам критеріїв конфіденційності, цілісності, доступності, спостережності з вимогами НД ТЗІ 2.5-004.

**Тема 4. Питання оцінки ефективності й проектування систем захисту**

Загальний похід до оцінки ефективності систем додаткового захисту. Захищеність системи з погляду ризику. Основний критерій захищеності. Способи завдання вихідних параметрів для оцінки захищеності. Метод статистичної оцінки. Оптимістично-песимістичний похід. Метод експертної оцінки. Способи завдання відповідності між параметрами погроз. Етапи оцінки захищеності й вибору оптимального варіанта системи захисту. Метод послідовного вибору поступок. Метод динамічного аналізу. Принципи організації й контролю систем захисту. Адміністративна група керування захистом. Моделі керування доступом. Функції контролю й керування систем захисту інформації.

**Тема 5. Апаратні засоби захисту інформації**

Апаратні засоби захисту. Програмні засоби захисту. Криптографічні засоби захисту. Інженерно-технічний рівень інформаційної безпеки. Поняття інженерно-технічного захисту. Фізичні засоби захисту. Види фізичних засобів. Охоронні системи. Охоронне телебачення. Охоронне освітлення та засоби охоронної сигналізації . Захист елементів будинків і приміщень. Огляд переліку стандартів та технічних специфікацій дозволених Адміністрацією державної служби спеціального зв’язку та захисту інформації. Стандарти, що визначають вимоги до блокових шифрів, потокових шифрів, асиметричних криптографічних алгоритмів та методів, кодів автентифікації повідомлень, геш-функцій, автентифікації, управління ключами, випадкової генерації біт, методів встановлення чутливих параметрів безпеки, форматів криптографічних повідомлень.

**Тема 6. Обґрунтування необхідності створення КСЗІ**

Головні принципи та етапи захисту від загроз. Нормативно-правове забезпечення захисту інформації. Нормативно-правові акти України на створення КСЗІ. Етапи створення КСЗІ. Положення про службу захисту інформації в ІКС. Складання моделі порушника та моделі загроз безпеки інформації в ІКС. Розробка політики безпеки інформації в ІКС. Складання Плану захисту інформації в ІКС.

**Тема 7. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС. Дослідна експлуатація КСЗІ**

Підготовка КСЗІ до введення в дію. Проведення попередніх випробувань КСЗІ. Проведення дослідної експлуатації КСЗІ. Проведення державної експертизи КСЗІ. Забезпечення супроводу КСЗІ. Державний контроль за станом ТЗІ. Відповідальність за невиконання вимог захисту інформації. Комплекси технічного захисту інформації.

## 4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| Назви змістових модулів і тем | Кількість годин | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | Заочна форма | | | |
| | усього | у тому числі | | | усього | у тому числі | | |
| | | лекц. | прак. | сам. роб. | | лекц. | прак. | сам. роб. |
| Тема 1. Системний підхід до вирішення проблеми захисту інформації | 8 | 2 | 2 | 4 | 8 | 2 | | 6 |
| Тема 2. Принципи побудови системи захисту | 7 | | 2 | 5 | 7 | | | 7 |
| Тема 3. Основні етапи створення систем захисту інформації. | 6 | 2 | | 4 | 6 | | | 6 |
| Тема 4. Матриця інформаційної безпеки. Подання елементів матриці | 8 | | 2 | 6 | 8 | | 2 | 6 |
| Тема 5. Функціональні вимоги безпеки стандарту ISO/IEC 15408 | 6 | 2 | | 4 | 6 | | | 6 |
| Тема 6. Система управління інформаційною безпекою | 7 | | 2 | 5 | 7 | | | 7 |
| Тема 7. Питання оцінки ефективності й проектування систем захисту | 6 | 2 | | 4 | 6 | | | 6 |
| Тема 8. Програмно-технічні методи й засоби захисту інформації | 7 | | 2 | 5 | 7 | 2 | | 5 |
| Тема 9. Апаратні засоби захисту інформації | 6 | 2 | | 4 | 6 | | | 6 |
| Тема 10. Порядок проведення робіт із створення КСЗІ в ІКС | 9 | | 2 | 7 | 9 | | | 9 |
| Тема 11. Обгрунтування необхідності створення КСЗІ | 6 | 2 | | 4 | 6 | | | 6 |
| Тема 12. Загальні проблеми експертних процедур при прийнятті рішень | 8 | | 2 | 6 | 8 | | 2 | 6 |
| Тема 13. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС. Дослідна експлуатація КСЗІ | 6 | 2 | | 4 | 6 | | | 6 |
| ***Усього годин*** | **90** | **14** | **14** | **62** | **90** | **4** | **4** | **82** |
| **ПІДСУМКОВИЙ КОНТРОЛЬ – ЗАЛІК** | | | | | | | | |

## 5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

| № з/п | Назва теми | Кількість годин | |
|---|---|---|---|
| | | денна форма | заочна форма |
| 1 | **Тема 1. Системний підхід до вирішення проблеми захисту інформації**<br>***Питання до підготовки:***<br>1. Основні положення інформаційної безпеки<br>2. Основними задачами інформаційної безпеки<br>3. Поняття комплексної системи захисту інформації<br>4. Основні вимоги до комплексної системи захисту інформації | | |
| 2 | **Тема 2. Принципи побудови системи захисту**<br>***Питання до підготовки:***<br>1. Цикл етапів (кроків) побудови систем захисту інформації<br>2. Напрями захисту інформації<br>3. Взаємозв'язок елементів основи, напрями, етапи<br>4. Динаміка побудови СЗІ та супровідні процеси | 2 | - |
| 3 | **Тема 3. Матриця інформаційної безпеки. Подання елементів матриці**<br>***Питання до підготовки:***<br>1. Процес формування системи захисту інформації з використанням матриці інформаційної безпеки<br>2. Елементи матриці інформаційної безпеки<br>3. Матриця інформаційної безпеки для стандарту ISO/IEC 15408 | 2 | 2 |
| 4 | **Тема 4. Система управління інформаційною безпекою**<br>***Питання до підготовки:***<br>1. Стандарти сімейства ISO/IEC 27000<br>2. Етапи створення систем управління інформаційною безпекою<br>3. Впровадження системи управління інформаційною безпекою<br>4. Управління інцидентами інформаційної безпеки | 2 | - |
| 5 | **Тема 5. Програмно-технічні методи й засоби захисту інформації**<br>***Питання до підготовки:***<br>1. Служби та механізми захисту<br>2. Огляд засобів захисту інформації<br>3. Технічні засоби захисту інформації<br>4. Комплекси засобів захисту | 2 | - |
| 6 | **Тема 6. Порядок проведення робіт із створення КСЗІ в ІКС**<br>***Питання до підготовки:***<br>1. Формування вимог до КСЗІ в ІКС<br>2. Розробка політики безпеки інформації в ІКС<br>3. Розробка технічного завдання на створення КСЗІ та проектування<br>4. Оцінка захищеності інформації в ІКС | 2 | - |
| 7 | **Тема 7. Загальні проблеми експертних процедур при прийнятті рішень**<br>***Питання до підготовки:***<br>1. Математичні моделі систем та процесів захисту<br>2. Методи попарних порівнянь<br>3. Методи крапкових оцінок<br>4. Модель комплексної оцінки | 2 | 2 |
| | **Всього** | **14** | **4** |

## 6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Комплексні системи безпеки» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання теоретичного матеріалу, здобутого під час семестру.
3. Виконання практичних та індивідуальних завдань, сформованих викладачем.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю знань.

**Тематика та питання до самостійної підготовки та індивідуальних завдань**

| № з/п | Назва теми | Кількість годин | |
|---|---|---|---|
| | | денна форма | заочна форма |
| 1 | **Тема 1. Системний підхід до вирішення проблеми захисту інформації**<br>***Питання до підготовки:***<br>1. Для захисту від яких видів загроз створюється КСЗІ?<br>2. Як технічно вирішується перший етап захисту від загроз?<br>3. Як технічно вирішується другий етап захисту від загроз?<br>4. Як технічно вирішується третій етап захисту від загроз?<br>5. Яка інформація підлягає захисту?<br>6. Які властивості щодо ТЗІ має інформація?<br>7. Які є види захисту інформації? | 4 | 6 |
| 2 | **Тема 2. Принципи побудови системи захисту**<br>Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації.<br>***Питання до підготовки:***<br>1. Які є головні принципи та етапи захисту від загроз?<br>2. Які були перші нормативні акти України з питань захисту інформації?<br>3. Які нормативні акти України визначають види інформації за порядком доступу?<br>4. Які нормативні акти України передбачають створення КСЗІ?<br>5. Для захисту від яких видів загроз створюється КСЗІ?<br>6. Яку інформацію від яких видів загроз треба захищати?<br>7. Які засоби захисту використовуються у складі КСЗІ?<br>8. Хто може бути виконавцем робіт із захисту інформації?<br>9. Хто є відповідальним за захист інформації в установі? | 5 | 7 |
| 3 | **Тема 3. Основні етапи створення систем захисту інформації**<br>***Питання до підготовки:***<br>1. Який документ визначає етапи створення КСЗІ?<br>2. Яку послідовність та назву мають етапи створення КСЗІ?<br>3. Які документи визначають порядок проведення першого етапу створення КСЗІ?<br>4. З якого обсягу робіт складається перший етап створення КСЗІ?<br>5. З якого обсягу робіт складається передостанній етап створення КСЗІ?<br>***Виконання розрахунку на тему:***<br>Розрахунок оцінки захищеності (згідно з варіантом). | 4 | 6 |

| | | | |
|---|---|---|---|
| 4 | **Тема 4. Матриця інформаційної безпеки. Подання елементів матриці**<br>***Питання до підготовки:***<br>1. Які основи побудови систем захисту інформації?<br>2. Які напрями захисту інформації?<br>3. Які етапи побудови систем захисту інформації?<br>4. Який взаємозв'язок елементів основи, напрями, етапи?<br>5. Який процес формування системи захисту інформації з використанням матриці інформаційної безпеки?<br>6. Яким чином виконуються позначення елементів матриці?<br>***Виконання розрахунку на тему:***<br>Розрахунок узагальнених кількісних оцінок профілю безпеки (згідно з варіантом). | 6 | 6 |
| 5 | **Тема 5. Функціональні вимоги безпеки стандарту ISO/IEC 15408**<br>***Питання до підготовки:***<br>1. Які функціональні вимоги щодо безпеки інформаційних технологій, описані в "Загальних критеріях" (ISO/IEC 15408)?<br>2. Які механізми довіри безпеці описані в "Загальними критеріями"?<br>3. Пояснить поняття клас – сімейство – компонент – елемент.<br>4. Які у стандарті ISO/IEC 15408 виділено класи функції (функціональні вимоги)?<br>5. Яка структура стандарту ISO/IEC 15408?<br>6. Які у стандарті ISO/IEC 15408 визначені вимоги довіри?<br>***Оформлення (розроблення) документів:***<br>1. Структура профілю захисту і завдання з безпеки. Порядок виконання зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. | 4 | 6 |
| 6 | **Тема 6. Система управління інформаційною безпекою**<br>***Питання до підготовки:***<br>1. Які основні категорій безпеки визначені у стандарті ДСТУ 27002?<br>2. Пояснить складники категорій безпеки організація інформаційної безпеки у стандарті ДСТУ 27002?<br>3. Пояснить складники категорій безпеки управління активами у стандарті ДСТУ 27002?<br>4. Пояснить складники категорій безпеки фізична безпека та безпека інфраструктури у стандарті ДСТУ 27002?<br>***Оформлення документів:***<br>1. Визначить структуру категорії безпеки контролю доступу та управління інцидентом інформаційної безпеки згідно стандарту ДСТУ 27002. | 5 | 7 |
| 7 | **Тема 7. Питання оцінки ефективності й проектування систем захисту**<br>***Питання до підготовки:***<br>1. Які критерії проектування оптимальної системи захисту?<br>2. Пояснить метод експертної оцінки?<br>3. Пояснить динамічного аналізу?<br>4. Які є способи завдання відповідності між параметрами погроз?<br>***Виконання розрахунку на тему:***<br>1. Розрахунок ефективної системи інформаційної безпеки Розрахунок варіантів системи для забезпечення цілісності та автентичност документів (згідно з варіантом). | 4 | 6 |
| 8 | **Тема 8. Програмно-технічні методи й засоби захисту інформації**<br>***Питання до підготовки:***<br>1. Які послуги безпеки забезпечує комплекс засобів захисту ЛОЗА-1? | 5 | 5 |

| | | | |
|---|---|---|---|
| | 2. Які програмні засоби роботи розроблені для адміністрування системи ЛОЗА-1?<br>3. Яка структура головного меню програми Аудитор ЛОЗА-1?<br>4. Які функції виконує програма Монітор захисту системи ЛОЗА-1?<br>***Виконання практичної роботи:***<br>1. Інсталяція комплексу засобів захисту ЛОЗА-1 (Virtual Machine) Налаштування користувачів. Конфігурація параметрів системи захисту Перегляд журналу захисту. | | |
| | **Тема 9. Апаратні засоби захисту інформації**<br>***Питання до підготовки:***<br>1. Які є типи засобів криптографічного захисту інформації?<br>2. Які є види засобів криптографічного захисту інформації?<br>3. Яка є класи засобів криптографічного захисту інформації?<br>4. Які функції виконує електронний ключ “Кристал-1”?<br>5. Які алгоритми та протоколи реалізовані в ключі “Кристал-1”?<br>4. Які функції виконує криптомодуль “Гряда-61”?<br>5. Які алгоритми, протоколи реалізовані в криптомодулі “Гряда-61”?<br>***Виконання практичної роботи:***<br>1. Тестування та конфігурування криптомодуля “Гряда-61” для ОС Microsoft Windows та електронного ключа “Кристал-1”. | 4 | 6 |
| | **Тема 10. Порядок проведення робіт із створення КСЗІ в ІКС**<br>***Питання до підготовки:***<br>1. Яку назву має НД ТЗІ, що визначає етапи створення КСЗІ?<br>2. Коли в ІКС здійснюється створення комплексів ТЗІ від витоку технічними каналами?<br>3. Хто приймає рішення щодо захисту ІКС від спеціальних впливів на інформацію?<br>4. Після чого створюється служба захисту інформації в ІКС?<br>5. Скільки є етапів створення КСЗІ згідно НД ТЗІ?<br>6. Яку назву має перший етап створення КСЗІ?<br>7. Яку назву має другий етап створення КСЗІ?<br>8. Яку назву має третій етап створення КСЗІ?<br>9. Яку назву має четвертий етап створення КСЗІ?<br>10. Яку назву має п’ятий етап створення КСЗІ?<br>11. Яку назву має шостий етап створення КСЗІ?<br>***Оформлення (розроблення) документів:***<br>1. Наказ про створення СЗІ.<br>2. Наказ про порядок проведення робіт зі створення КСЗІ.<br>3. Наказ про призначення комісії з обстеження.<br>4. Формуляр ІКС. | 7 | 9 |
| | **Тема 11. Обґрунтування необхідності створення КСЗІ**<br>***Питання до підготовки:***<br>1. Який закон України розподіляє інформацію за порядком доступу?<br>2. Як поділяється інформація за порядком доступу?<br>3. Яка інформація є інформацією з обмеженим доступом?<br>4. Якою інформацією за режимом доступу є персональні дані?<br>5. Яка інформація підлягає захисту?<br>6. Що таке конфіденційність інформації?<br>7. Що таке доступність інформації?<br>8. Що таке цілісність інформації?<br>9. Який закон України розподіляє інформацію за порядком доступу? | 4 | 6 |

| | | | |
|---|---|---|---|
| | ***Оформлення (розроблення) документів:***<br>1. Положення про службу захисту інформації (НД ТЗІ 1.4-001).<br>2. Наказ про призначення комісії з категоріювання.<br>3. Акт категоріювання (НД ТЗІ 1.6-005-2013). | | |
| | **Тема 12. Введення КСЗІ в дію та оцінка захищеності інформації в ІКС**<br>***Питання до підготовки:***<br>1. Що є метою попередніх випробувань КСЗІ в ІКС?<br>2. Згідно якого документу проводяться попередні випробування КСЗІ?<br>3. Які відомості містить програма випробувань КСЗІ в ІКС?<br>4. Які документи завершують випробування КСЗІ в ІКС?<br>5. Хто повинен підписати документи з випробувань КСЗІ?<br>6. З яких 6 перевірок складається випробування КСЗІ в ІКС?<br>7. Який документ визначає вимоги ТЗІ для будівництва?<br>8. Який висновок повинен бути у документах з випробувань КСЗІ?<br>9. Для чого, як правило, виконуються будівельно-монтажні роботи?<br>10. З яких розділів складається технологічна інструкція?<br>11. Які акти складаються під час пусконалагоджувальних робіт?<br>***Комплектування КСЗІ. Оформлення (розроблення) документів:***<br>1. Протокол попередніх випробувань КСЗІ в ІКС.<br>2. Акт приймання робіт з технічного захисту інформації.<br>3. Акт атестації комплексу технічного захисту інформації.<br>4. Акт інсталяції та налагодження АВПЗ і КЗЗ від НСД. | 6 | 6 |
| | **Тема 13. Дослідна експлуатація КСЗІ**<br>***Питання до підготовки:***<br>1. Які заходи здійснюються під час дослідної експлуатації КСЗІ?<br>2. Які настанови розробляються під час дослідної експлуатації КСЗІ?<br>3. Який документ складається після завершення дослідної експлуатації?<br>4. Який висновок повинен бути в акті завершення дослідної експлуатації?<br>5. Хто повинен підписати акт завершення дослідної експлуатації КСЗІ?<br>6. З яких розділів складається акт завершення дослідної експлуатації КСЗІ?<br>7. Який документ складається після завершення створення КСЗІ?<br>***Оформлення (розроблення) документів:***<br>1. Акт завершення дослідної експлуатації КСЗІ в ІКС.<br>2. Акт завершення робіт зі створення КСЗІ в ІКС. | 4 | 6 |
| | **Всього** | **62** | **82** |

## 7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

| **Види контролю** | **Складові оцінювання** |
|---|---|
| **Поточний контроль**, який здійснюється у ході: проведення практичних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань | **50%** |
| **Підсумковий контроль**, який здійснюється у ході проведення іспиту | **50%** |

| | |
|---|---|
| **Методи діагностики знань (контролю)** | фронтальне опитування; наукова доповідь, усне повідомлення, індивідуальне опитування; робота у групах; розв`язання ситуаційних завдань, кейсів, практичних завдань, іспит |

**Питання до заліку**

На якому етапі КСЗІ оформляється План захисту інформації?

На якому етапі КСЗІ відпрацьовується розмежування доступу користувачів до ресурсів ІКС?

На якому етапі КСЗІ проводиться дослідна експлуатація КСЗІ?

Які накази створюються на етапі формування вимог до КСЗІ?

При формування завдання на створення КСЗІ визначаються/здійснюється?

Після завершення будівельних робіт на створення КСЗІ в ІКС створюється комісія?

Який документ розробляється на етапі розробки політики безпеки інформації?

Опис профілю захищеності включає?

Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації здійснюється згідно?

В акті категоріювання наведені такі відомості?

Загрози, що стосуються порушення можливості використання комп'ютерних систем або інформації, що обробляється ними, становлять загрози?

При обстеженні середовищ функціонування ІКС аналізу підлягає?

На якому етапі КСЗІ проводиться дослідна експлуатація КСЗІ?

При обстеженні інформаційного середовища мають бути наведені?

Вкажіть правильну послідовність етапів створення КСЗІ.

Доступність це властивість інформації, яка характеризує?

Об'єктам, на яких обробляється інформація з обмеженим доступом, що не становить державної таємниці, встановлюється категорія

Комплекс засобів захисту це сукупність

Під політикою безпеки інформації слід розуміти

До якого класу АС відноситься локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу?

На якому етапі КСЗІ створюється акт обстеження середовищ функціонування ІТС?

Якій функціональній критерії містить такі послуги: реєстрація, ідентифікація і автентифікація, цілісність комплексу засобів захисту, самотестування, автентифікація відправника та одержувача?

Обстеження якого елемента ІКС передбачає аналіз і опис класу і структури ІТС, виду каналів зв'язку та апаратно-програмних засобів?

Розробка Плану захисту здійснюється згідно

За результатами роботи комісії з прийняття робіт складається акт

Захист інформації, яка становить державну таємницю, забезпечується варіантом

Об'єктами категоріювання є

Як називається категоріювання ІКС, що здійснюється у разі її створення?

Розроблення та оформлення технічного завдання на КСЗІ має відповідати

Положення про службу захисту інформації затверджується

До якого класу АС відноситься одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу?

На якому етапі КСЗІ проводиться державна експертиза КСЗІ?

За результатами обстеження середовищ функціонування ІТС затверджується

Порядок проведення обстеження обчислювальної системи ІТС повинен відповідати

До якого класу АС відноситься розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу?

На якому етапі КСЗІ створюється акт категоріювання?

Відповідальність за забезпечення захисту інформації в системі покладається на

Для захисту від яких видів загроз створюється КСЗІ?

При обстеженні середовища користувачів здійснюється аналіз

При обстеженні обчислювальної системи ІКС повинні бути проаналізовані й описані

При обстеженні інформаційного середовища аналізу підлягає

При обстеженні фізичного середовища здійснюється аналіз

На якому етапі створення КСЗІ проводиться навчання користувачів?

Який документ визначає повноваження та відповідальність працівників СЗІ

Які основні функції реалізують програмні засоби захисту?

Ідентифікація та контроль за діями користувачів, керування комп'ютерною системою становлять предмет послуг

Загрози несанкціонованої модифікації інформації становлять загрози

Загрози, пов'язані з несанкціонованим ознайомленням з інформацією, становлять загрози

Загрози, що стосуються порушення можливості використання комп'ютерних систем або інформації, що обробляється ними, становлять загрози

Загрози порушення цілісності це

Загрози порушення доступності це

Загроза порушення конфіденційності це

Доступність це властивість інформації, яка характеризує

Цілісність це властивість інформації, яка характеризує

Конфіденційність це властивість інформації, яка характеризує

Опис політики безпеки інформації в ІКС має бути затверджений

Опис моделі загроз для інформації, оброблюваної в ІКС, має містити

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від

Опис моделі порушника безпеки інформації в ІКС мають бути визначені

Згідно з Положенням про державну експертизу у сфері технічного захисту інформації, об'єктами експертизи є

Метою пусконалагоджувальних робіт є

Які можливі варіанти захисту інформації?

Типове положення про службу захисту інформації має відповідати

Порядок проведення робіт із створення комплексної системи захисту має відповідати

Категоріювання може бути?

Стандартний функціональний профіль захищеності це

Який документ створюється за результатами категоріювання ІКС?

## 8. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ
**(для заліку)**

Рівень знань оцінюється:

- ***«відмінно» / «зараховано» А - від 90 до 100 балів.*** Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- ***«добре» / «зараховано» В - від 82 до 89 балів.*** Здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- ***«добре» / «зараховано» С - від 74 до 81 балів.*** Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до

самостійної роботи, реферату та активність у науково-дослідній роботі;

- ***«задовільно» / «зараховано» D - від 64 до 73 балів.*** Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);

- ***«задовільно» / «зараховано» E - від 60 до 63 балів.*** Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.

- ***«незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів***. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

- ***«незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів.*** Здобувач не володіє навчальним матеріалом.

**Таблиця відповідності результатів контролю знань за різними шкалами**

| 100-бальною шкалою | Шкала за ECTS | За національною шкалою | |
|---|---|---|---|
| | | екзамен | залік |
| 90-100 (10-12) | A | Відмінно | зараховано |
| 82-89 (8-9) | B | Добре | |
| 74-81(6-7) | C | | |
| 64-73 (5) | D | Задовільно | |
| 60-63 (4) | E | | |
| 35-59 (3) | FX | незадовільно | не зараховано |
| 1-34 (2) | F | | |

## 9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

### Основна


1. НД ТЗІ 3.7-003-23. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. (Серія видань "Нормативний документ").
2. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах. (Серія видань "Нормативний документ").
3. НД ТЗІ 3.6-005-21. Порядок категоріювання безпеки інформаційної системи та інформації. (Серія видань "Нормативний документ").
4. НД ТЗІ 3.6-006-21. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. (Серія видань "Нормативний документ").
5. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. (Серія видань "Нормативний документ").
6. НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. (Серія видань "Нормативний документ").
7. НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем. (Серія видань "Нормативний документ").
8. НД ТЗІ 2.3-025-21. Том 1, 2, 3. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. (Серія видань "Нормативний документ").
9. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого

доступу. (Серія видань “Нормативний документ”).

10. Про внесення змін до Закону України “Про інформацію” № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32,ст. 313. – (Серія видань “Законодавство України”)

11. Закон України “Про захист персональних даних” № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481. – (Серія видань “Законодавство України”).

12. Закон України “Про критичну інфраструктуру” № 2684-IX від 18.10.2022. – (Серія видань “Законодавство України”).

13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань “Нормативний документ”).

14. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999. – (Серія видань “Нормативний документ”).

15. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань “Нормативний документ”).

16. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).

17. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.:ООО "Д.В.К.", 2004. – 508 с.

18. Комплексні системи захисту інформації : навчальний посібник / К63 [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

**Допоміжна**

1. ДСТУ ISO/IEC 27002 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. (Серія видань “Законодавство України ”).

2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. (Серія видань “Законодавство України”).

3. НД ТЗІ 1.6-005-2013. Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, дециркулює інформація з обмеженим доступом, що не становить державної таємниці. (Серія видань “Нормативний документ”).

4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. (Серія видань “Нормативний документ”).

5. Про внесення змін до Закону України “Про захист інформації в автоматизованих системах ” № 2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, № 26, ст. 347. – (Серія видань “Законодавство України”).

6. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник. – К.: Вид-во Європ. Ун-ту, 2006. – 102 с.

**Інформаційні ресурси**

1. Сайт Державної служби спеціального зв’язку та захисту інформації. URL: https://cip.gov.ua/ua .

2. Сайт Технічний захист інформації. URL:https://tzi.ua/ua/index.html .

3. Комплексні системи захисту інформації. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/

4. Комплексні системи захисту інформації. Проектування, впровадження, супровід. URL: https://books.google.com.ua/books?id=GcBlDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

5. Сайт Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua .
6. Сайт Законодавство України. URL: https://zakon.rada.gov.ua/laws.