

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра інформаційних технологій та кібербезпеки, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід»

обов'язкових компонент

освітньої програми першого (бакалаврського) рівня вищої освіти

125 «Кібербезпека»

Харків 2020

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол № 10 від 22.10.2020

СХВАЛЕНО

Вченою радою факультету № 4
Протокол № 6 від 21.10.2020

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС
Протокол № 6 від 22.10.2020

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 20.10.2020 № 19)

Розробники:

1. Доцент кафедри, к. т. н., доцент Соляник Т. М.

Рецензенти:

1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

**1. Розподіл часу навчальної дисципліни за темами
(денна форма навчання)**

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські за-	Практичні за-	Лабораторні за-	Самостійна робота	
Семестр № 7							
Тема № 1. Загальні питання організації та функціонування систем технічного захисту інформації.	10	4		2		4	
Тема № 2. Нормативно-правова база України у сфері технічного захисту інформації.	16	2		2		12	
Тема № 3. Комп'ютерні системи захисту інформації як об'єкт дослідження.	18	4		2		12	
Тема № 4. Побудова комплексних систем захисту інформації.	18	4		2	4	8	
Тема № 5. Процес створення комплексних систем захисту інформації.	20	4		4	4	8	
Тема № 6. Розробка проекту комплексних систем захисту інформації.	18	4		2	4	8	
Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.	16	2		2	4	8	
Тема № 8. Експертиза комплексних систем захисту інформації.	18	4		2	4	8	
Тема № 9. Впровадження та супровід КСЗІ.	16	2		2	4	8	
Всього по дисципліні	150	30		20	24	76	Залік

2. Методичні вказівки до практичних занять

Тема № 1. Загальні питання організації та функціонування систем технічного захисту інформації.

Практичне заняття № 1. Розробка генерального та ситуаційного планів об'єкту технічного захисту.

Навчальна мета заняття: засвоїти основне призначення генерального та ситуаційного планів то основні принципи їх побудови.

Кількість годин: 2.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Аналіз зразка генерального плану.
4. Аналіз зразка ситуаційного плану.
5. Побудова генерального та ситуаційного планів обраного об'єкта захисту.
6. Висновки.

Література:

1. Матеріали лекції за темою 1.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Intertnet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити загальні питання організації та функціонування систем технічного захисту інформації.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації. для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 2. Нормативно-правова база України у сфері технічного захисту інформації.

Практичне заняття № 2. Аналіз засобів і систем забезпечення інформаційної діяльності.

Навчальна мета заняття: набуття практичних навичок щодо побудови схем розташування технічних засобів, систем та інженерних комунікацій для забезпечення інформаційної діяльності на об'єкті захисту.

Кількість годин: 2.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Аналіз основних засобів та систем забезпечення інформаційної діяльності.
4. Побудова схеми розташування технічних засобів та систем забезпечення інформаційної діяльності.
5. Побудова схеми розташування інженерних комунікацій, які виходять за межі контрольованої території.
6. Висновки.

Література:

1. Матеріали лекції за темою 2.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити загальні питання організації та функціонування систем технічного захисту інформації.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації. для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 3. Комп'ютерні системи захисту інформації як об'єкт дослідження.

Практичне заняття № 3-4. Виявлення та дослідження видів загроз інформаційній безпеці.

Навчальна мета заняття: набуття практичних навичок щодо ідентифікації та подання видів загроз інформаційній безпеці, наявних на об'єкті дослідження, а також оцінювання ризиків від їх виникнення.

Кількість годин: 4 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Аналіз можливих каналів витоку інформації.
4. Аналіз каналів спеціального впливу на інформацію.
5. Аналіз шляхів несанкційованого доступу до інформації.
6. Побудова схеми та механізмів впливу загроз на об'єкт дослідження.
7. Висновки.

Література:

1. Матеріали лекції за темою 3.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити види загроз та механізми їх реалізації.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 4. Побудова комплексних систем захисту інформації.

Практичне заняття № 5. Побудова окремої моделі загроз.

Навчальна мета заняття: набуття практичних навичок щодо компоновки окремої моделі загроз на базі проведеного аналізу об'єкту інформаційного захисту для подальшого розроблення технічного завдання на створення системи захисту інформації.

Кількість годин: 2 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Аналіз зразка окремої моделі загроз.
4. Побудова окремої моделі загроз для обраного об'єкту інформаційного захисту.
5. Висновки.

Література:

1. Матеріали лекції за темою 3 та темою 4.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити особливості окремої моделі загроз та основні принципи її побудови. Мати в наявності результати виконання аналізу об'єкту дослідження з попередніх практичних занять.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації. для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 5. Процес створення комплексних систем захисту інформації.

Практичне заняття № 6-7. Розробка технічного завдання на систему захисту інформації для обраного об'єкта дослідження.

Навчальна мета заняття: набуття практичних навичок щодо загальних принципів побудови технічного завдання на систему захисту інформації.

Кількість годин: 4 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.

2. Письмове опитування студентів.
3. Вивчення основних принципів побудови технічного завдання.
4. Аналіз зразка технічного завдання на систему захисту інформації об'єкта дослідження.
5. Побудова календарного плану виконання технічного завдання.
6. Висновки.

Література:

1. Матеріали лекції за темами 4 та 5.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити загальні принципи побудови технічного завдання. Мати у наявності окрему модель загроз, побудовану на попередньому практичному занятті.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації. для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 6. Розробка проекту комплексних систем захисту інформації.

Практичне заняття № 8. Розробка проекту комплексних систем захисту інформації.

Навчальна мета заняття: набуття практичних навичок щодо загальних принципів побудови проекту системи захисту інформації обраного об'єкта дослідження згідно розробленого технічного завдання на систему захисту інформації.

Кількість годин: 2 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Вивчення основних елементів та складових проекту системи захисту інформації.
4. Аналіз зразка проекту системи захисту інформації.
5. Побудова проекту системи захисту інформації обраного об'єкта дослідження згідно розробленого технічного завдання на систему захисту інформації.
6. Висновки.

Література:

1. Матеріали лекції за темами 5 та 6.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити основні елементи проекту системи захисту інформації.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації, для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.

Практичне заняття № 9. Оцінювання захищеності інформації після введення систем захисту інформації в дію.

Навчальна мета заняття: набуття практичних навичок щодо оцінювання ступеня захищеності інформації після введення системи захисту інформації в дію.

Кількість годин: 2 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Вивчення методів оцінювання захищеності інформації.
4. Оцінка захищеності інформації в обраному об'єкті дослідження.
5. Висновки.

Література:

1. Матеріали лекції за темою 7.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локальної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити загальні питання оцінювання ступеня захищеності інформації в системі.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації, для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема № 8. Експертиза комплексних систем захисту інформації.

Практичне заняття № 10. Експертне оцінювання системи захисту інформації.

Навчальна мета заняття: набуття практичних навичок щодо експертного оцінювання комплексних систем захисту інформації.

Кількість годин: 2 години.

Місце проведення: комп'ютерний клас.

Навчальні питання:

1. Вступ.
2. Письмове опитування студентів.
3. Вивчення основних принципів проведення експертиз комплексних систем захисту інформації.
4. Експертне оцінювання системи захисту інформації запропонованого об'єкта захисту.
5. Висновки.

Література:

1. Матеріали лекції за темами 8 та 9.
2. Методичні вказівки до практичного завдання.
3. Нормативні документи [1-10].

Матеріально-технічне забезпечення занять: комп'ютерна мережа із підключенням до Internet.

Заняття проводиться в комп'ютерному класі. Кожний студент (курсант) забезпечується окремим робочим місцем (комп'ютером, підключеним до локаль-

ної мережі та із підключенням до Internet). Методичне забезпечення, індивідуальні завдання надаються в електронному вигляді через локальну комп'ютерну мережу університету.

Підготовка до заняття

Вивчити загальні принципи проведення експертизи комплексних систем захисту інформації.

План проведення заняття:

Порядок проведення вступу до заняття.

I. Оголошення теми заняття та його мети. Надати посилання на відповідні презентації. для проведення заняття. Письмове опитування курсантів з відповідного теоретичного матеріалу.

II. Порядок проведення основної частини заняття.

Виконання завдань практичного заняття за методичними вказівками. Здобувачі вищої освіти згідно керівництва до практичних занять за темою виконують задачі навчальних питань.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернет

Основна

1. Інформаційна безпека / Ю. Я. Бобал [та ін.]; за ред. Ю. Я. Бобала, І. В. Горбатого . – Львівська політехніка, 2019. – 580 с.
2. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition // Bruce Schneier. – 2017. – 784 p.
3. Matt Walker. CEH Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
4. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. / ITU-T Recommendation X.805, 10/2003. URL: <https://www.itu.int/rec/T-REC-X.805-200310-I/en> (дата звернення: 20.09.2016).
5. Конспект лекцій.

Допоміжна

1. Гришук, Р. Основи кібербезпеки / Р. Гришук, Ю. Даник. – Житомир : ЖНАЕУ, 2016. – 636 с.
2. Основи захисту інформації: навч. посіб. / Ю. Даник, С. Вдовенко, В. Шестаков, О. Писарчук, Р. Гришук, М. Куликівський, В. Ходаківський. – Житомир: ЖВІ ДУТ, 2015. – 220 с.
3. Бурячок, В. Політика інформаційної безпеки. / В. Бурячок, Р. Гришук, В. Хорошко. – ПВП «Задруга», 2014. – 222 с.
4. Корченко, А. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / А. Корченко, О. Архипов, Ю. Дрейс. – К: наук.-вид. центр НА СБУ України, 2014. – 332 с.
5. Остапов, С.Е. Технології захисту інформації / С.Е. Остапов, С.П. Євсєєв, О. Г. Король. – Родовід, 2014. – 428 с.
6. Забезпечення інформаційної безпеки держави / І. Іванченко [та ін.]; за ред. проф. В. Хорошка. – К: ПВП «Задруга», 2013. – 170 с.
7. Юдін, О. Інформаційна безпека. Нормативно-правове забезпечення / О. Юдін. – К.: НАУ, 2011. – 640 с.
8. Голубєв, В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк; за заг. ред. Р. А. Калюжного. – Запоріжжя: Просвіта, 2001. – 252 с.

Інформаційні ресурси в Інтернеті

1. Про інформацію: Закон України від 25 квітня 2019 року N 2704-VIII. URL: <http://www.ukrstat.gov.ua/Zakon/ukr/lawinform.html> (дата звернення: 01.09.2020)
2. Про державну таємницю: Закон України від 15.08.2020 № 3855-XII URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (дата звернення: 01.09.2020)
3. Про доступ до публічної інформації: Закон України від 15.08.2020, № 3856-XII URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення: 01.09.2020)
4. Про захист персональних даних: Закон України від 20.03.2020, № 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 01.09.2020)
5. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 03.07.2020, № 3475-IV URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text> (дата звернення: 01.09.2020)
6. Про основні засади забезпечення кібербезпеки України: Закон України від 03.07.2020, № 2163-VIII URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 01.09.2020)

7. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. –Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.

8. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. –Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.

9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Терміни та визначення. –Чинний з 1998-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.