Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ О. О. Ілляшенко
(підпис) (ініціали та прізвище)

«31» серпня 2021 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації: проектування, впровадження, супровід (КП)
(назва навчальної дисципліни)

Галузь знань: 12 Інформаційні технології
(шифр і найменування галузі знань)

Спеціальність: 125 Кібербезпека
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних та комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

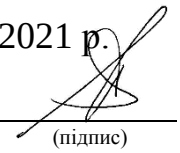
Рівень вищої освіти: перший (бакалаврський)

Харків 2021рік

Розробник: Пєвнєв В.Я., доцент, к.т.н. , доцент 
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2021 р.

Завідувач кафедри д.т.н., професор  В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 2</td><td rowspan="12">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітня програма
Безпека інформаційних та комунікаційних систем
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 1</td><td>2021/ 2022</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання немає</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 12 / 60</td><td>8-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 1
самостійної роботи студента – 4</td><td>0 годин</td></tr>
<tr><td>Практичні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні *</td></tr>
<tr><td>12 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>48 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Диференційований залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до загальної кількості годин становить: 12/48.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до комплексних систем захисту інформації.

Завдання: систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсове проектування, а також:

- придбання знань про засобі й основні принципи побудови мереж відеоспостереження;
- придбання знань про фізичну й логічну структури мереж відеоспостереження;
- придбання знань про принципи функціонування обладнання мереж відеоспостереження.

Компетентності, які набуваються:

–здатність застосовувати знання у практичних ситуаціях.
–знання та розуміння предметної області та розуміння професії.
–здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
–вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
–здатність до пошуку, оброблення та аналізу інформації.
–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.
–здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
–здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

–застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
–організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
–використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
–аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які

характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
- вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
- застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

Пререквізити – дисципліна базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності. «Технології захисту інформації», «Організація баз даних», «Системи технічного захисту інформації», «Мікропроцесорні системи», «Web-технології», «(КП) Технології захисту інформації», «Мікропроцесорні системи захисту інформації», «Управління інформаційною безпекою», «Захист інформації в інформаційно-комунікаційних системах»,

«Технології захисту інформації», «Мікропроцесорні системи захисту інформації (КП)», «Технології програмування (КП)».

Кореквізити –«Дипломний робота (проект) бакалавра».

3. Програма навчальної дисципліни

Модуль 1.
Змістовний модуль 1. Розробка захищеної мережі відеоспостереження
Тема 1. Видача завдання. Постановка задачі.
Тема 2. Проектування логічної моделі мережі відеоспостереження.
Тема 3. Проектування фізичної моделі мережі відеоспостереження.
Тема 4. Вибір камер спостереження та пристроїв зберігання інформації.
Тема 5. Формулювання вимог до програми резервного доступу до камер спостереження.
Тема 6. Розроблення технічного завдання.
Тема 7. Проектування програми. Розроблення програми.
Тема 8. Розроблення пояснювальної записки презентації та публічний захист.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин *Денна форма*				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Розробка захищеної мережі відеоспостереження					
1. Видача завдання. Постановка задачі	7			2	5
2. Проектування логічної моделі мережі відеоспостереження	5				5
3. Проектування фізичної моделі мережі відеоспостереження	5				5
4. Вибір камер спостереження та пристроїв зберігання інформації	12			2	10
5. Формулювання вимог до програми резервного доступу до камер спостереження	7			2	5
6. Розроблення технічного завдання	7			2	5
7. Проектування програми. Розроблення програми	7			2	5
8. Розроблення пояснювальної записки. Розроблення презентації та публічний захист	10			2	8
Разом за змістовним модулем 1	**60**			**12**	**48**
Усього годин	**60**			**12**	**48**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Видача завдання. Постановка задачі	2
2	Вибір камер спостереження та пристроїв зберігання інформації	2
3	Формулювання вимог до програми резервного доступу до камер спостереження	2
4	Розроблення технічного завдання	2
5	Проектування програми. Розроблення програми	2
6	Розроблення пояснювальної записки.	2
	Разом	12

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Видача завдання. Постановка задачі	5
2	Проектування логічної моделі мережі відеоспостереження	5
3	Проектування фізичної моделі мережі відеоспостереження	5
4	Вибір камер спостереження та пристроїв зберігання інформації	10
5	Формулювання вимог до програми резервного доступу до камер спостереження	5

6	Розроблення технічного завдання	5
7	Проектування програми. Розроблення програми	5
8	Розроблення пояснювальної записки. Розроблення презентації та публічний захист	8
	Разом	**48**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення практичних занять, консультацій, а також самостійна робота студентів із використання відповідних матеріалів (п.14, п. 15).

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді публічного захисту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Лабораторні заняття	0…4	6	0…24
Підсумковий котнроль	0...76	1	0...76
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:
<u>виконання і захист лабораторних робіт:</u>
при виконанні всіх вимог завдань методик на роботи - 4 бали;
- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1балл;
- якщо робота не виконана і не захищена - 0 балів.

<u>На підсумковий контроль</u> (всього 76 балів) виносяться всі пройдені за контрольований період теми.

Необхідний обсяг знань для одержання позитивної оцінки.

Студент повинен знати:

- загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види руйнівних програм та атаки на інформаційні та комунікаційні системи, вимоги до їх захищеності);
- встановлену політику інформаційної та/або кібербезпеки;
- методи забезпечування захисту інформації, в системах відеоспостереження;

− характеристику методів реалізації основних функцій системи відеоспостереження.

Необхідний обсяг вмінь для одержання позитивної оцінки.

Студент повинен вміти:

− забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації в мережах відеоспостереження;

− вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в мережах відеоспостереження;

− забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в мережах відеоспостереження;

− вирішувати завдання захисту програм та інформації, що обробляється в мережах відеоспостереження програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень

Розподіл балів, які отримують студенти за виконання курсової роботи (проекту)

Пояснювальна записка	Ілюстративна частина	Захист роботи	Сума
до _70__	до _10__	до _20__	100

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо захисту інтелектуальної власності.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення наукових робіт. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти виконувати інформаційне забезпечення наукових досліджень.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Тексти лекцій
2. Презентації лекцій
3. Керівництво до лабораторних робіт
4. Робоча програма навчальної дисципліни

14. Рекомендована література

Базова

1. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.
2. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс] : учеб. пособие для вузов. М. : Горячая линия – Телеком, 2014. 193 с.

Допоміжна

1. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.
2. Скляров Д. Искусство защиты и взлома информации. Спб.: БХВ-Петербург, 2004. 288 с.
3. Ачилов Р. Построение защищенных корпоративных сетей. М.: ДМК Пресс, 2013. 250 с.
4. Есин В.И., Кузнецов А.А., Сорока Л.С. Безопасность информационных систем и технологий. Х.: ООО «ЭДЭНА», 2010. : 656 с.
5. Разрушающие программные воздействия: Учебно-методическое пособие . под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. 328 с.

15. Інформаційні ресурси

1. Архитектура комп’ютера [Электрон. ресурс]. - Режим доступа: http://inf1.info/book/export/html/44
2. Вікіпедія — вільна енциклопедія [Электрон. ресурс]. - Режим доступа: http://www. ru.wikipedia.org/
3. Википедия — свободная энциклопедия [Электрон. ресурс]. - Режим доступа: http://www. ru.wikipedia.org/
4. Microsoft Virtual Academy [Электрон. ресурс]. - Режим доступа: http://www.microsoftvirtualacademy.com/
5. Microsoft IT Academy Program [Электрон. ресурс]. - Режим доступа: https://itacademy.microsoftelearning.com/
6. Cisco Networking Academy [Электрон. ресурс]. - Режим доступа:
7. https://www.netacad.com/, http://www.cisco.com/web/learning/netacad/