ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-комп'ютерних технологій
30 серпня 2021 р., протокол № 7

Голова Вченої ради
Надія ЛОБАНЧИКОВА

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 25 «ТЕОРІЯ КІБЕРБЕЗПЕКИ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
125 «Кібербезпека»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
27 серпня 2021 р., протокол № 10

Завідувач кафедри
Андрій Єфіменко

Розробник: старший викладач Єлизавета БАЙЛЮК

Житомир
2023 - 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 3</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність код спеціальності «Кібербезпека»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>3-й</td><td>-</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 90</td><td>5-й</td><td>-</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи – 1,63</td><td rowspan="10">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>-</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>26 год.</td><td>-</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 71,1 % аудиторних занять, 28,9 % самостійної та індивідуальної роботи;

для заочної форми навчання − 0 % аудиторних занять, 0 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Теорія кібербезпеки» є формування розуміння студентами теоретичних основ методів захисту інформації, розвиток навичок з їх аналізу та застосування, набуття практичних навичок з розрахунку міцності захисту, побудови моделі загроз та моделі порушника інформаційної безпеки в ІКС, використання програмного забезпечення для моделювання загроз, реалізації моделей контролю доступу до інформації з обмеженим доступом, здійснення процедур управління інцидентами інформаційної безпеки.

Завданнями вивчення навчальної дисципліни «Теорія кібербезпеки» є набуття знань, умінь та навичок (компетентностей), спрямованих на:

– розуміння теоретичних засад кібербезпеки;

– розуміння різноманітності методів забезпечення кібернетичної безпеки та принципів, що лежать в їх основі;

– розуміння основних принципів та етапів роботи сучасних систем захисту інформації;

– здійснення аналізу інформації з відкритих джерел, відносно існуючих методів та систем кібернетичного захисту;

– вміння розслідувати та оцінювати інциденти інформаційної безпеки в інформаційно-комунікаційних системах;

– вміння формулювати критерії вибору та здійснювати за ними вибір методів захисту та систем на їх основі, для досягнення максимальної ефективності для вирішення кожної конкретної задач.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 спеціальності «Кібербезпека»:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека»:

РН 4. 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.

РН 12. Розробляти моделі загроз та порушника.

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

РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

3. Програма навчальної дисципліни

Змістовий модуль 1. Теоретичні основи інформаційної безпеки в ІКС.

Тема 1. Кіберпростір та кібербезпека: поняття і визначення.

1. Кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.
2. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози.

Тема 2. Загрози ІБ в ІКС, кібератаки та кібертероризм: поняття і визначення.

1. Загрози та вразливості інформаціної безпеки(ІБ) інформаційно-комунікаційних систем(ІКС): поняття, визначення та класифікація.
2. Кібератаки: поняття, визначення та класифікація. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу.
3. Кібертероризм: поняття та визначення. Наслідки кібертероризму.

Тема 3. Теоретичні основи захисту інформації.

1. Загальні поняття теорії захисту інформації.
2. Позначення, аксіоми та визначення.
3. Основні типи політик безпеки.
4. Математичні моделі безпеки.

Тема 4. Управління інцидентами інформаційної безпеки в ІКС.

1. Цілі та задачі управління інцидентами інформаційної безпеки.
2. Документи, що регламентують управління інцидентами інформаційної безпеки.
3. Можливі інциденти інформаційної безпеки.
4. Основні процеси системи управління інцидентами інформаційної безпеки в ІКС.
5. Склад документації системи управління інцидентами інформаційної безпеки в ІКС.

Змістовий модуль 2. Інформаційна та кібербезпека: соціотехнічний аспект.

Тема 5. Соціотехнічна безпека: проблемні аспекти.

1. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу.
2. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки.
3. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж – цілі та способи реалізації.
4. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем.

Тема 6. Методи і засоби соціального інжинірингу.

1. Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем: основні аспекти, поняття та визначення.
2. Методи соціального інжинірингу.
3. Алгоритм соціотехнічної атаки: етапи проведення, супутні уразливості та основні ризики.
4. Загрози соціального інжинірингу

Тема 7. Захист інформації від соціотехнічних атак.

1. Канали несанкціонованого доступу до інформації.
2. Методи та засоби протидії соціотехнічним атакам і захисту від них: переваги та недоліки.
3. Формалізована модель оцінювання загроз безпеці ІзОД.
4. Доопрацювання засобів захисту інформації.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	лабораторні	самостійна робота
Модуль 1								
Змістовий модуль 1. Теоретичні основи інформаційної безпеки в ІКС								
Тема 1. Кіберпростір та кібербезпека: поняття і визначення	11	4	4	3	-	-	-	-
Тема 2. Загрози ІБ в ІКС, кібератаки та кібертероризм: поняття і визначення	11	4	4	3	-	-	-	-
Тема 3. Теоретичні основи захисту інформації	11	4	4	3	-	-	-	-
Тема 4. Управління інцидентами інформаційної безпеки в ІКС.	12	4	4	4				
Разом за змістовий модуль 1	45	16	16	13	-	-	-	-
Змістовий модуль 2. Інформаційна та кібербезпека: соціотехнічний аспект								
Тема 5. Соціотехнічна безпека: проблемні аспекти	12	4	4	4	-	-	-	-
Тема 6. Методи і засоби соціального інжинірингу	14	6	4	4	-	-	-	-
Тема 7. Захист інформації від соціотехнічних атак	19	6	8	5	-	-	-	-
Разом за змістовий модуль 2	45	16	16	13	-	-	-	-
ВСЬОГО	90	32	32	26	-	-	-	-

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Дослідження процесів розрахунку міцності захисту інформації	4	-
2	Побудова узагальненої моделі загроз та моделі порушника інформаційної безпеки в ІКС	4	-
3	Розслідування та проведення оцінки інцидентів інформаційної безпеки в ІКС	4	-
4	Проведення підсумкової модульної контрольної роботи №1	4	-
5	Побудова моделі загроз ІБ в ІКС з використанням програми OWASP-Threat-dragon	4	-
6	Побудова моделі загроз ІБ в ІКС з використанням утиліти Microsoft Threat Modeling Tool	4	-
7	Дослідження дискреційних та мандатних моделей контролю доступу до інформації	4	-
8	Проведення підсумкової модульної контрольної роботи №2	4	-
РАЗОМ		32	-

6. Завдання для самостійної роботи

Тема 1. Засоби захисту в операційній системі UNIX

1. Архітектура системи UNIX.
2. Безпека UNIX.
3. Адміністрування засобів безпеки UNIX.

Тема 2. Засоби захисту в операційній системі Windows.

1. Основні відомості про систему.
2. Архітектура системи.
3. Розмежування доступу.

Тема 3. Системи оброблення конфіденційної інформації.

1. Обґрунтування застосування захищених ОС.
2. Система Trusted Solaris.
3. Операційна система Фенікс.

Тема 4. Безпека мережних протоколів та прикладних служб Інтернету.

1. Протоколи прикладного рівня та транспортні протоколи.
2. Протокол IP.

3. Протокол маршрутизації BGP.
4. Протоколи керування мережею.
5. Система електронної пошти.
6. Веб-служба.

Тема 5. Засоби захисту в розподілених інформаційно-комунікаційних системах.

1. Архітектура захищених мереж.
2. Міжмережні екрани.
3. Системи виявлення атак.
4. Додаткові інструментальні засоби.

Тема 6. Передавання інформації через захищені мережі.

1. Захист інформації, що передається відкритими каналами зв'язку.
2. Віртуальні захищені мережі.
3. Рівні реалізації віртуальних захищених мереж.
4. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні.

7. Індивідуальні завдання

Індивідуальні завдання з дисципліни «Теорія кібербезпеки» полягають у виконанні лабораторних робіт згідно варіанту по списку в журналі та відпрацюванні матеріалу навчальних курсів мережевої академії Cisco NetAcad, а саме: Cybersecurity Essentials, CCNA Security, CCNA Cybersecurity Operations (проходження онлайн навчання, виконання тестових контрольних робіт, виконання тестових проміжних оцінювань).

8. Методи навчання

В ході вивчення дисципліни використовуються наступні методи навчання: мультимедійні презентації, аналіз інформації з відкритих джерел, комп'ютерне моделювання, статистичний аналіз.

Основними видами занять, які проводяться під керівництвом викладача, є лекції, лабораторні роботи та самостійна робота.

На лекціях розглядаються загальні теоретичні положення дисципліни. Під час проведення лекцій використовуються мультимедійні засоби для інтерактивної демонстрації прикладів та графічного матеріали. До кожної лекції студентам додається презентація основних положень.

При виконанні лабораторних робіт зміцнюються знання, отримані на лекціях, набуваються первинні навички з проведення розрахунків міцності

захисту, створення моделі загроз та моделі порушника, комп'ютерного моделювання загроз за допомогою різного програмного забезпечення, реалізації моделей контролю доступу до інформації з обмеженим доступом.

При самостійній роботі студенти набувають навички самостійного освоєння матеріалу, який не використаний в навчальному процесі.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль. Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль. Оцінюється вхідний, проміжний, кінцевий рівень знань студента. Підсумковий контроль проводиться у вигляді комп'ютерних тестів та/або виконання практичних завдань.

10. Розподіл балів

Поточне тестування та самостійна робота							Сума
Змістовий модуль 1				Змістовий модуль 2			
Т1	Т2	Т3	Т4	Т5	Т6	Т7	100
10	10	15	15	15	15	20	

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015. — 288 с.

2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. 449 с.

3. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. — К.:Видавнича група BHV, 2009. — 608 с.:іл.

4. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. — М.: Горячая линия-Телеком, 2011. — 320 с.: ил.

5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

6. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

7. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

8. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

9. Закон України «Про інформацію» № 2657-ХИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650.

10. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).

11. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 р.

12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 80/94-ВР (Зі змінами, внесеними згідно із Законом № 1703-IV від 11.05.2004, в редакції Закону № 2594-IV від 31.05.2005, ВВР, 2005, № 26, ст. 347).

13. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).

14. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М ., Гладких, В.М. Домрачев, Н.М. Сивкова. – К.:ЦП «Компринт» О.В., 2021. – 444 с.

15. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

16. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

17. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.

18. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

19. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

20. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

21. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

22. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

23. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

Допоміжна література

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах управління / Антонюк А.О. – Київ: Видавничий дім "КМ академія", 2003. – 242 с.

2. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. – 172 с.

3. Коваленко М.М. Комп’ютерні віруси і захист інформації / М.М. Коваленко – К.: Наукова думка, 1999. – 267 с.

4. Henry K. Risk management and analysis / Kevin Henry // Information

Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. Part 1, Section 1.4, Ch. 28. P. 321-329.

5. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

6. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

7. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

8. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach 29 Publications, 2016. 504 p

12. Інформаційні ресурси в Інтернеті

1. Архипов О.Є., Бровко В.Д. Кібербезпека – виникнення, формування, розуміння. / Теоретико-методологічні засади забезпечення інформаційної безпеки людини, суспільства, держави. / Режим доступу до статті: http://nbuv.gov.ua/j-pdf/iblsd_2017_2_3.pdf

2. Державна служба спеціального зв'язку та захисту інформації України. Електронний ресурс: www.dsszzi.gov.ua

3. Закон України «Про основні засади забезпечення кібербезпеки України». Із змінами, внесеними згідно із Законами № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241 № 720-IX від 17.06.2020 – ВВР, 2017, № 45, ст. 403.

4. Інформаційна безпека: науковий журнал: журнал: http://www.nbuv.gov.ua/portal/natural/Ibez/index.html

5. Наталія Жовницька. Основні засади забезпечення кібербезпеки Україні. Електронний ресурс: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy

6. Сайт Держспецзв’язку. Електронний ресурс: https://cip.gov.ua/ua

7. Стандарти інформаційної безпеки. Електронний ресурс: http://www.is-standard.com

8. Шуклін Г.В., Барабаш О.В. Теоретичні засади державного регулювання кібербезпеки на фондовому ринку: механізми, методи, інструменти. / Сучасний захист інформації. №3(35), 2018 / Режим доступу до статті: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2029.

9. Центр інформаційної безпеки. Електронний ресурс: http://www.bezpeka.com

10. Cisco Talos Intelligence Group. URL: https://talosintelligence.com/

_____

*Індекс структурного підрозділу відповідно до наказу ректора «Про затвердження організаційної структури Державного університету «Житомирська політехніка» (наприклад, 22.06).

** Індекс освітньої програми відповідно до наказу ректора «Про індексацію освітніх програм Державного університету «Житомирська політехніка» (наприклад, 122.00.1/Б).

*** Шифр освітньої компоненти в освітній програмі (наприклад, ОК1).