ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 28 «УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ»

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

Схвалено на засіданні
кафедри комп'ютерної інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
_____ Андрій ЄФІМЕНКО
Гарант освітньо-
професійної програми
_____ Андрій ЄФІМЕНКО

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Покотило Олександра Андріївна

Житомир
2026-2027 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів 3	Галузь знань 12 «Інформаційні технології»	нормативна (нормативна, за вибором)
Модулів – 1	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки:
Змістових модулів – 2		4-й
		Семестр
Загальна кількість годин - 90		8-й
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи – 2,63	Освітній ступінь «бакалавр»	Лекції
		24 год.
		Практичні
		–
		Лабораторні
		12 год.
		Самостійна робота
		54 год.
		Вид контролю: залік

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

для денної форми навчання – 40 % аудиторних занять, 60 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Управління кібербезпекою» є формування комплексу знань щодо основ управління кібербезпекою, набуття студентом теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

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

– знання та уміння складати та впроваджувати політики інформаційної безпеки;

– знання та вміння організовувати інформаційну безпеку, її внутрішню організацію, політику щодо мобільного обладнання та віддаленої роботи;

– знання та вміння забезпечувати безпеку людських ресурсів перед наймом, протягом найму та за припинення чи зміні умов найму;

– знати та застосовувати заходи управління ресурсами СУІБ: відповідальності за ресурси СУІБ, класифікації інформації та поводження з носіями;

– знати та застосовувати заходи контролю доступу, зокрема, бізнес-вимоги до контролю доступу, управління доступом користувача, відповідальності користувача та контроль доступу до систем і прикладних програм;

– знання та вміння застосовувати криптографічні засоби захисту, розробляти політику використання криптографічних засобів;

– знання та вміння забезпечувати заходи фізичної безпеки та безпеки інфраструктури: зони безпеки, обладнання;

– знання та вміння застосовувати засоби забезпечення безпеки експлуатації, зокрема безпечні процедури експлуатації та відповідальності, захисту від зловмисного коду, резервне копіювання, ведення журналів аудиту та моніторинг, управління технічною вразливістю, розгляд аудиту інформаційних систем;

– знання та вміння застосовувати засоби забезпечення безпеки комунікацій: управління безпекою мережі та обміну інформацією;

– знання та вміння застосовувати засоби забезпечення безпеки для інформаційних систем: вимоги щодо безпеки для інформаційних систем, безпека в процесах розроблення та підтримки, дані для тестування системи;

– знання та вміння застосовувати засоби забезпечення вимог щодо відносин з постачальниками: інформаційна безпека у взаємовідносинах з постачальниками, управління наданням послуг постачальником.

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

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

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

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно 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 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

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

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

РН 44. 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.

3. Програма навчальної дисципліни

Змістовий модуль 1. Теорія управління кібербезпекою

Тема 1. Основні поняття та стандарти інформаційної безпеки

1. Поняття інформаційної безпеки та кібербезпеки.
2. Основні складові та загрози інформаційної безпеки.
3. Управління кібербезпекою. Система управління інформаційною безпекою.
5. Міжнародні організації, що мають вплив на управління ІБ.
6. Міжнародна стандартизація. Стандарт ISO / IEC 27001: ціль і призначення.

Тема 2. Нормативна документація СУІБ. Організація інформаційної безпеки

1. Підготовка документів для впровадження СУІБ.
2. Внутрішні документи. Політика ІБ.
3. Внутрішня організація ІБ.
4. Організація ІБ. Зовнішнє середовище.
5. Мобільне обладнання та віддалена робота.

Тема 3. Управління ресурсами СУІБ. Безпека людський ресурсів

1. Відповідальність за ресурси СУІБ.
2. Класифікація, маркування і правила обробки інформації.
3. Поводження з носіями.
4. Питання забезпечення безпеки людських ресурсів на підприємстві.
5. Аналіз загроз безпеки людських ресурсів.
6. Технології захисту людських ресурсів.

Тема 4. Контроль доступу. Криптографічний захист

1. Вимоги до контролю доступу.
2. Управління правами доступу користувачів.
3. Відповідальність користувача.
4. Контроль доступу до систем та прикладних програм.
5. Криптографічні засоби захисту.
6. Політика щодо використання криптографічних методів.

7. Управління криптографічними ключами.

Змістовий модуль 2. Створення і забезпечення безпеки СУІБ

Тема 5. Фізична безпека та безпека експлуатації

1. Безпека приміщень, зони безпеки.
2. Безпека обладнання. Процедури експлуатації та відповідальності.
3. Захист від зловмисного коду. Резервне копіювання. Ведення журналів аудиту та моніторинг.
4. Контроль програмного забезпечення, що перебуває в експлуатації. Управління технічною вразливістю.
5. Розгляд аудиту інформаційних систем.

Тема 6. Безпека комунікацій. Придбання, розробка та підтримка інформаційних систем

1. Управління безпекою мережі.
2. Обмін інформацією.
3. Вимоги щодо безпеки для інформаційних систем.
4. Безпека в процесах розробки та підтримки.
5. Дані для тестування систем.

Тема 7. Управління інцидентами ІБ

1. Основна задача та цілі управління інцидентами ІБ.
2. Аналіз інцидентів інформаційної безпеки.
3. Особливості менеджменту інцидентів.

Тема 8. Взаємовідносини з постачальниками. Аспекти інформаційної безпеки управління безперервністю бізнесу

1. Інформаційна безпека у взаємовідносинах з постачальниками.
2. Управління наданням послуг постачальником.
3. Безперервність інформаційної безпеки.
4. Резервне обладнання.

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
Змістовий модуль 1. Теорія управління кібербезпекою								
Тема 1. Основні поняття та стандарти інформаційної безпеки	11	2	1	8	-	-	-	-
Тема 2. Нормативна документація СУІБ. Організація інформаційної безпеки	11	4	1	6	-	-	-	-
Тема 3. Управління ресурсами СУІБ. Безпека людський ресурсів	11	2	2	7	-	-	-	-
Тема 4. Контроль доступу. Криптографічний захист	12	4	2	6	-	-	-	-
Разом за змістовий модуль 1	45	12	8	27	-	-	-	-
Змістовий модуль 2. Створення і забезпечення безпеки СУІБ								
Тема 5. Фізична безпека та безпека експлуатації	12	2	2	8	-	-	-	-
Тема 6. Безпека комунікацій. Придбання, розробка та підтримка інформаційних систем	11	4	1	6	-	-	-	-
Тема 7. Управління інцидентами ІБ	11	2	2	7	-	-	-	-
Тема 8. Взаємовідносини з постачальниками. Аспекти інформаційної безпеки управління безперервністю бізнесу	11	4	1	6	-	-	-	-
Разом за змістовий модуль 2	45	12	8	27	-	-	-	-
ВСЬОГО	90	24	12	54	-	-	-	-

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Створення політики інформаційної безпеки	1	-
2	Віддалений робочий стіл і помічник у Windows	1	-
3	Налаштування локальної політики безпеки Windows	2	-
4	Використання стандартних інструментів шифрування Bitlocker та Bitlocker To Go	2	-
5	Відновлення системи та резервне копіювання жорсткого диска	2	-
6	Створення облікових записів користувачів	1	-
7	Налаштування брандмауера Windows	2	-
8	Дослідження порушень PII, PHI, PCI	1	-
РАЗОМ		12	-

6. Завдання для самостійної роботи

Тема 1. Концепція національної безпеки України.

1. Концепція національної безпеки України.
2. Загрози національній безпеці України в інформаційній сфері. Термінологія в галузі кібербезпеки.
3. Принципи забезпечення національної безпеки.
4. Термінологія в галузі управління інформаційної безпеки.

Тема 2. Загрози безпеці державних інформаційних ресурсів.

1. Загрози безпеці державних інформаційних ресурсів.
2. Типові уразливості інформаційних та комунікаційних систем, причини їх появи.
3. Класифікація атак на державні ресурси.
4. Політика кібербезпеки інформації та модель порушника.

Тема 3. Поняття та категоризація державних інформаційних ресурсів.

1. Загрози інформації та вибір функціонального класу послуг захисту.
2. Особливості реалізації комплексних систем захисту інформації.
3. Структура та функції державної системи забезпечення інформаційно-психологічної безпеки.
4. Ліцензування в галузі забезпечення інформаційно-психологічної безпеки.

5. Сертифікація засобів і методів неусвідомлюваного інформаційного впливу.

6. Експертиза з метою забезпечення інформаційно-психологічної безпеки (психоекологічна експертиза). Контроль за забезпеченням інформаційно психологічної безпеки.

Тема 4. Стандарти серії 27xxx. Основні принципи, положення та завдання.

1. Стандарти серії 27xxx. Основні принципи та завдання управління інформаційної безпеки.
2. Стандарти, рекомендації та найкращі світові практики щодо управління інцидентами інформаційної безпеки.
3. Основні положення та структура стандарту ISO/IEC 27001:2005.
4. Додаток А стандарту ISO/IEC 27001.
5. Реалізація вимог стандарту.

Тема 5. Основні методи оцінки та аналізу інформаційних ризиків. Ризик-менеджмент стандарт NIST 800-30 та ISO 27002.

1. Класифікація ризиків інформаційної безпеки.
2. Методика оцінки ризиків інформаційної безпеки.
3. Удосконалення системи інформаційної безпеки підприємства за допомогою страхування ризиків.

Тема 6. Соціотехнічна безпека.

1. Методи соціального інжинірингу.
2. Основні алгоритми соціотехнічних атак на державні інформаційні ресурси, етапи проведення.
3. Рекомендації щодо захисту від соціотехнічних атак.
4. Управління персоналом у сфері інформаційної безпеки.

Тема 7. Поняття та класифікація інцидентів інформаційної безпеки відповідно до міжнародних стандартів та рекомендацій (ISO 18044:2004, ISO/IEC 27002:2005, MOD, ITU-T E.409 тощо).

1. Функціональна схема системи обробки інцидентів інформаційної безпеки в лінійно-кабельних системах.
2. Реалізація автоматизованої системи обробки інцидентів безпеки первинної мережі.
3. Система обробки інцидентів безпеки телекомунікацій.
4. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035.

7. Індивідуальні завдання

Індивідуальні завдання з дисципліни «Управління кібербезпекою» полягають у виконанні лабораторних робіт згідно варіанту по списку в журналі, оволодіння навиками аналізу процедур управління послугами та механізмами захисту в об’єктах інформаційної діяльності типу телекомунікаційних мереж та відпрацюванні матеріалу навчальних курсів мережевої академії Cisco NetAcad, а саме: Introduction to Cybersecurity та Cybersecurity Essentials (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	Т8	100
12	12	13	13	12	12	13	13	

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. Богуш, В.М. Інформаційна безпека держави : навч. посібник [Електронний ресурс] / В.М. Богуш, О.К. Юдін. К.: «МК-Прес», 2005. 432 с. – Режим доступу: https://studfiles.net/preview/5376129/; https://studfiles.net/preview/5376129/.

2. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки: навч. посібник. / Кононович В.Г., Гладиш С.В. / Затверджено Міністерством транспорту та зв'язку України / за ред. В.Г. Кононовича. – Одеса: ОНАЗ, – 2009. – 208 с. – Режим доступу: https://old.onat.edu.ua/?pg=biblio_kaf_ib_pd.

3. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [КорченкоО.Г., Гнатюк С.О., КазмірчукС.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр.видань НАСБ України, 2014. – 190 с. – Режим доступу: http://193.178.34.24/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf .

4. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ,

2015. – 288 с. – Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf .

5. 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.

6. Daniel Pérez-González. Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation / Daniel Pérez-González, Pedro Solana-González, Sara Preciado., 2019. – 21 с - Режим доступу: https://doi.org/10.1108/ITP-06-2018-0261

7. Humphreys E. Implementing the ISO/IEC 27001 ISMS Standart. Second edition / Edward Humphreys., 2016. – 213 с. - Режим доступу: http://surl.li/anpvf

Допоміжна література

1. Стратегія національної безпеки України. Затверджено Указом Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015 .

2. Тардаскіна Т.М., Кононович В.Г. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. Затверджено Міністерством освіти та науки України як навчальний посібник для студентів вищих навчальних закладів [Лист № 1/11-7791 від 13 серпня 2010 року] / – Одеса: ОНАЗ, – 2010. – 268 с.

3. Про національну безпеку України: Закон України [Електронний ресурс] / Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. Затверджено Указом Президента України від 21 червня 2018 року № 2469-VIII – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19.

4. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.

5. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.

6. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.

7. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки.

8. Brotherston L. Defensive Security Handbook: Best Practices for Securing Infrastructure 1st Edition / Lee Brotherston., 2017. – 274 с.

12. Інформаційні ресурси в Інтернеті

1. 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.
2. Інформаційна безпека: науковий журнал: журнал: http://www.nbuv.gov.ua/portal/natural/Ibez/index.html
3. Казарин О. В. Безпека програмного забезпечення комп'ютерних систем. Електронний ресурс: http://citforum.ru/security/articles/kazarin
4. Наталія Жовницька. Основні засади забезпечення кібербезпеки України. Електронний ресурс: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya-kiberbezopasnosti-ukrainy
5. Президент України. Електронний ресурс: http://www.president.gov.ua
6. Верховна Рада України. Електронний ресурс: http://www.rada.gov.ua
7. Кабінет Міністрів України. Електронний ресурс: http://www.kmu.gov.ua
8. Сайт Держспецзв'язку. Електронний ресурс: https://cip.gov.ua/ua
9. Стандарти інформаційної безпеки. Електронний ресурс: http://www.is-standard.com
10. 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.
11. Федотов Н. Н. Защита информации (Учебный курс). Електронний ресурс: http://www.college.ru/UDP/texts/index.html
12. Центр інформаційної безпеки. Електронний ресурс: http://www.bezpeka.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).