ЗАТВЕРДЖЕНО
Вченою радою
факультету інформаційно-
комп'ютерних технологій
28 серпня 2024 р., протокол № 8

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЦІЛІСНІСТЬ ДАНИХ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 121 «Інженерія програмного забезпечення»
освітньо-професійна програма «Інженерія програмного забезпечення»
факультет інформаційно-комп'ютерних технологій
кафедра інженерії програмного забезпечення

Схвалено на засіданні кафедри
інженерії програмного забезпечення
28 серпня 2024 р.,
протокол № 7

Завідувач кафедри
_____ Тетяна ВАКАЛЮК

Гарант освітньо-професійної
програми
_____ Андрій МОРОЗОВ

Розробник: доцент кафедри інженерії програмного забезпечення
Надія ЛОБАНЧИКОВА

Житомир
2024 – 2025 н.р.

Робоча програма навчальної дисципліни «Інформаційна безпека та цілісність даних» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійна програма «Інженерія програмного забезпечення» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, 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">обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність 121 «Інженерія програмного забезпечення»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 4</td><td>3</td><td>3</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td>2</td><td>2</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3,0
самостійної роботи – 2,6</td><td rowspan="10">Освітній ступінь «бакалавр»</td><td>16 год.</td><td>4 год.</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>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>78 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання − 13 % аудиторних занять, 87 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки та захисту інформації в інформаційно-комунікаційних системах, методологічними та законодавчими основами організації, планування та впровадження систем кібербезпеки та захисту інформації в сучасних бізнес-процесах, а також основним аспектам практичної діяльності по їх створенню, забезпеченню функціонування та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданнями навчальної дисципліни є:

–оволодіння принципами побудови систем кіберзахисту;

– розуміння головних задач та сервісів кібербезпеки;

– оволодіння загальними теоретичними поняттями та основними нормативно-правовими документами у сфері кібербезпеки;

–отримання знань щодо основних складових інформаційної безпеки;

– отримання знань щодо існуючих моделей загроз та порушника, основних причин порушення безпеки;

– отримання знань щодо класифікації засобів кібербезпеки, організаційних та технічних заходів забезпечення кіберзахисту;

– оволодіння принципами захисту інформації від несанкціонованого доступу, методами аутентифікації, ідентифікації та авторизації користувачів інформаційно-комунікаційних систем, методами контролю доступу в тому числі безпеки доступу до хмарних ресурсів, основи IAM (Identity and Access Management), служби аутентифікації та керування доступом;

– оволодіння теоретичними основами криптографічних та стеганографічних методів захисту інформації, у тому числі захист даних у застосунку, захист даних під час передачі;

– оволодіння методами та засобами здійснення процедури оцінки ефективності систем кіберзахисту;

– оволодіння технологіями реалізації криптографічних алгоритмів захисту інформації;

– оволодіння методами розробки моделі загроз та моделі порушників інформаційної безпеки;

– оволодіння методами та технологіями моніторингу та реагування на інциденти.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 121 «Інженерія програмного забезпечення» та освітньо-професійною програмою «Інженерія програмного забезпечення»:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

СК06. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (у тому числі кібербезпеки).

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 121 «Інженерія програмного забезпечення»:

ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати додатково наступні Soft skills:

- *керування часом:* уміння справлятися із завданнями вчасно;
- *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;
- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;
- *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

МОДУЛЬ 1

Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі.

Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту (ЗК01, ЗК02, СК06, ПР21).

Дефініція основних понять і визначень у сфері кібербезпеки. Основні нормативно-правові документи із захисту інформації.

Тема 2. Загрози безпеці інформаційних систем (ЗК01, ЗК02, СК06, ПР21).

Джерела загроз інформаційній безпеці. Системна класифікація і загальний аналіз загроз безпеці інформації.

Тема 3. Інциденти у сфері високих технологій (ЗК01, ЗК02, СК06, ПР21).

Основні поняття та визначення. Класифікація кібернетичних втручань і загроз.

Особливості найпоширеніших кібератак

Тема 4. Методи та засоби захисту інформації від НСД (ЗК01, ЗК02, СК06, ПР21).

Способи та методи НСД в сучасних ІТС. Основні принципи захисту інформації від НСД. Класичні моделі розмежування доступу. Ідентифікація і аутентифікація користувачів. Безпека доступу та хмарні ресурси. Налаштування безпеки доступу до ресурсів хмари. Основи IAM (Identity and Access Management). Автентифікація та авторизація. Служби аутентифікації та керування доступом.

Змістовий модуль 2. Основи криптографічних методів кіберзахисту

Тема 5. Криптографічні методи захисту інформації (ЗК01, ЗК02, СК06, ПР21).

Історична довідка. Основні поняття криптографії. Загальна класифікація алгоритмів шифрування. Методи заміни і перестановки. Реалізація алгоритмів шифрування

Тема 6. Системи шифрування з відкритим ключем (ЗК01, ЗК02, СК06, ПР21).

Основні відомості. Алгоритм RSA. Алгоритм Діффі Хеллмана. Алгоритм Ель-Гамаля.

Тема 7. Кваліфікований електронний підпис (ЗК01, ЗК02, СК06, ПР21).

Історичний ракурс. Відмінності КЕП та ЕЦП. Процедури отримання КЕП. Особливості формування КЕП.

Тема 8. Стеганографія (ЗК01, ЗК02, СК06, ПР21).

Поняття стеганографії. Вимоги до стегосистем. Додатки стеганографії. Стеганографічні методи захисту.

Змістовий модуль 3. Організація захисту інформації

Тема 9. Технології віртуалізації (ЗК01, ЗК02, СК06, ПР21).

Ключові терміни. Переваги та недоліки. Типи віртуалізації. Платформи віртуалізації.

Тема 10. Шкідливе програмне забезпечення та захист від нього (ЗК01, ЗК02, СК06, ПР21).

Класифікація. Способи розповсюдження. Програмні закладки. Утиліти віддаленого адміністрування. Комп'ютерні віруси. Спеціальні хакерські утиліти.

Тема 11. Політика безпеки (ЗК01, ЗК02, СК06, ПР21).

Приклади кібератак та методи протидії. Поняття політики безпеки. Види політик безпеки. Організація секретного діловодства.

Тема 12. Основні моделі теорії захисту інформації (ЗК01, ЗК02, СК06, ПР21).

Рівні інформаційно-комунікаційної системи. Несанкціонований доступ на різних рівнях інформаційно-комунікаційної системи. Логування та моніторинг. Реагування на інцидент та їх обробка.

Змістовий модуль 4. Побудова захищених систем

Тема 13. Основні способи ведення промислового шпигунства (ЗК01, ЗК02, СК06, ПР21).

Види та методи конкуренції. Основні напрями забезпечення захищеності і попередження погроз безпеки компанії. Інформаційна безпека компанії. Комп'ютерна безпека. Поняття і призначення корпоративної розвідки.

Тема 14. Організаційно-технічні заходи забезпечення захисту інформації (ЗК01, ЗК02, СК06, ПР21).

Основні види технічних каналів і джерел витоку інформації. Способи запобігання витоку інформації по технічним каналам. Захист даних під час передачі

Тема 15. Аспекти створення захищених систем (ЗК01, ЗК02, СК06, ПР21).

Основні вимоги, що ставляться до систем захисту інформації та її підсистем.

Налаштування публічних та приватних підмереж та internet-протоколів. Використання груп безпеки. Використання списків управління доступом мережі. Використання балансувальників навантаження.

Аналіз систем захисту периметру території особливо важливих об'єктів від несанкціонованого доступу. Аналіз методів та засобів ідентифікації особистості в системах охорони периметру.

Тема 16. Оцінка ефективності систем захисту інформації (ЗК01, ЗК02, СК06, ПР21).

Підходи до оцінки ефективності систем 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. Принципи організації захисту інформації в кіберпросторі								
Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.	5	1	2	2	5	0,25	0,5	4,25
Тема 2. Загрози безпеці інформаційних систем	7	1	2	4	7	0,25	0,5	6,25
Тема 3. Інциденти у сфері високих технологій	3	1		2	3	0,25	0	2,75
Тема 4. Методи та засоби захисту інформації від НСД	8	1	3	4	9	0,25	1	7,75
Модульний контроль 1	1	-	1	-	-	-	-	-
Разом за змістовий модуль 1	***24***	***4***	***8***	***12***	***24***	***1***	***2***	***21***
Змістовий модуль 2. Основи криптографічних методів кіберзахисту								
Тема 5. Криптографічні методи захисту інформації	5	1	2	2	5	0,25	0,5	4,25
Тема 6. Системи шифрування з відкритим ключем	5	1	2	2	5	0,25	0,5	4,25
Тема 7. КЕП	5	1	2	2	5	0,25	0,5	4,25
Тема 8. Стеганографія	6	1	1	4	7	0,25	0,5	6,25
Модульний контроль 2	1	-	1	-	-	-	-	-
Разом за змістовий модуль 2	***22***	***4***	***8***	***10***	***22***	***1***	***2***	***19***
Змістовий модуль 3. Організація захисту інформації								
Тема 9. Технології віртуалізації	5	1	2	2	5	0,25	0,5	4,25
Тема 10. Шкідливе програмне забезпечення та захист від нього	3	1		2	3	0,25	0	2,75
Тема 11. Політика безпеки	7	1	2	4	7	0,25	0,5	6,25
Тема 12. Основні моделі теорії захисту інформації	8	1	3	4	9	0,25	1	7,75
Модульний контроль 3	1	-	1	-	-	-	-	-
Разом за змістовий модуль 3	***24***	***4***	***8***	***12***	***24***	***1***	***2***	***21***
Змістовий модуль 4. Побудова захищених систем								
Тема 13. Основні способи ведення промислового шпигунства	5	1	2	2	5	0,25	0,5	4,25
Тема 14. Організаційно-технічні заходи	5	1	2	2	5	0,25	0,5	4,25

забезпечення захисту інформації								
Тема 15. Аспекти створення захищених систем	5	1	2	2	5	0,25	0,5	4,25
Тема 16. Оцінка ефективності систем захисту інформації.	4	1	1	2	5	0,25	0,5	4,25
Модульний контроль 4	1	-	1	-	-	-	-	-
Разом за змістовий модуль 4	***20***	***4***	***8***	***8***	***20***	***1***	***2***	***17***
ВСЬОГО	***90***	***16***	***32***	***42***	***90***	***4***	***8***	***78***

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі			
1	Дослідження методів соціальної інженерії.	4	1
2	Дослідження процесів проникнення та OSINT-розвідки	3	1
3	**Модульний контроль 1**	1	-
Змістовий модуль 2. Основи криптографічних методів кіберзахисту			
4	Дослідження процесів захисту інформації за допомогою симетричних криптографічних алгоритмів	4	1
5	Дослідження процесів застосування асиметричних криптосистем та нанесення цифрових водяних знаків у зображення просторовим методом LSB	3	1
6	**Модульний контроль 2**	1	-
Змістовий модуль 3. Організація захисту інформації			
7	Дослідження процесів налаштування параметрів безпеки операційної системи Windows 10 із застосуванням програми VirtualBox	4	1
8	Дослідження процесу розробки політики безпеки	3	1
9	**Модульний контроль 3**	1	-
Змістовий модуль 4. Побудова захищених систем			
10	Дослідження методів, засобів та технологій технічного захисту інформації	4	1
11	Дослідження процесів визначення міцності захисту інформації	3	1
12	**Модульний контроль 4**	1	-
	РАЗОМ	**32**	**8**

6. Завдання для самостійної роботи

Передбачається, що в період вивчення дисципліни студент самостійно опрацьовує теоретичні основи прослуханого лекційного матеріалу, вивчає окремі питання, що передбачені для самостійного опрацювання, поглиблено вивчає літературу на задану тему та здійснює пошук додаткової інформації, систематизує вивчений матеріал перед екзаменом.

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі			
1	Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.	2	4,25
2	Тема 2. Загрози безпеці інформаційних систем	4	6,25
3	Тема 3. Інциденти у сфері високих технологій	2	2,75
4	Тема 4. Методи та засоби захисту інформації від НСД	4	7,75
Змістовий модуль 2. Основи криптографічних методів кіберзахисту			
5	Тема 5. Криптографічні методи захисту інформації	2	4,25
6	Тема 6. Системи шифрування з відкритим ключем	2	4,25
7	Тема 7. КЕП	2	4,25
8	Тема 8. Стеганографія	4	6,25
Змістовий модуль 3. Організація захисту інформації			
9	Тема 9. Технології віртуалізації	2	4,25
10	Тема 10. Шкідливе програмне забезпечення та захист від нього	2	2,75
11	Тема 11. Політика безпеки	4	6,25
12	Тема 12. Основні моделі теорії захисту інформації	4	7,75
Змістовий модуль 4. Побудова захищених систем			
13	Тема 13. Основні способи ведення промислового шпигунства	2	4,25
14	Тема 14. Організаційно-технічні заходи забезпечення захисту інформації	2	4,25
15	Тема 15. Аспекти створення захищених систем	2	4,25
16	Тема 16. Оцінка ефективності систем захисту інформації.	2	4,25
	РАЗОМ	**42**	**78**

7. Індивідуальні самостійні завдання

Індивідуальні завдання не передбачені навчальним планом.

8. Методи навчання

Під час викладання навчальної дисципліни використовуються методи навчання, що сприяють досягненню відповідних програмних результатів.

Результат навчання	Методи навчання
ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	– Вербальні методи (лекція, пояснення) – Наочні методи (демонстрація, ілюстрація) – Практичні методи (Виконання та захист лабораторних робіт) – Дискусійний метод – Метод активного навчання (мозковий штурм, командна робота) – Ситуаційний метод – Методи самостійної роботи (вирішення задач, підготовка доповідей)

9. Методи контролю

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	– Усне опитування, участь у дискусії, відповіді на проблемні запитання – Перевірка виконання та захист лабораторних робіт – Експрес-тестування – Самооцінювання та взаємооцінювання – Перевірка виконання завдань модульного контролю – Екзамен

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає:

– поточний, модульний та підсумковий контроль – для здобувачів денної форми навчання;

– поточний та підсумковий контроль – для здобувачів заочної форми навчання.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Модульний контроль проводиться з метою оцінювання результатів навчання здобувачів вищої освіти за модуль (змістові модулі) навчальної дисципліни. Модульний контроль проводиться під час навчального заняття після завершення вивчення матеріалу модуля (змістових модулів) навчальної дисципліни. Модульний контроль здійснюється у формі комп’ютерного тестування.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі екзамену. Процедура складання екзамену визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр
Для здобувача денної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань модульного або підсумкового контролю	40
Підсумкова семестрова оцінка	**100**
Для здобувача заочної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань підсумкового контролю	40
Підсумкова семестрова оцінка	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	60	60
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**):	**сумарно не більше 10**	**сумарно не більше 10**
1. Призове місце (1, 2, 3) або участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах	10/8/6 (4)	10/8/6 (4)
2. Підготовка наукових статей	10 (одноразово)	10 (одноразово)
3. Підготовка тез доповідей наукових конференцій	4 (одноразово)	4 (одноразово)
3. Інші види робіт:		
- активна участь в опитуваннях, обговореннях, дискусіях під час лекцій протягом семестру	5 (одноразово)	5 (одноразово)
- участь у вебінарах та заходах від ІТ-компаній	2 (за кожен)	2 (за кожен)
Разом за виконання завдань поточного контролю	**60**	**60**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Відповіді (виступи) на заняттях, у т.ч. дискусії	5	5
Виконання та захист лабораторних робіт	30	30
Виконання поточних тестових завдань	25	25
Разом за виконання завдань під час навчальних занять	**60**	**60**

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів під час навчальних занять може використовуватися 100-бальна шкала оцінювання щодо кожного окремо виду робіт. Розрахунок загальної кількості балів, які здобувач може набрати за результатами роботи під час навчальних занять протягом семестру, проводиться за формулою:

$$Р_{НЗ} = \sum(Р_i \times ВК_i) \times К_{НЗ}, \quad (1)$$

де $Р_{НЗ}$ – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

$Р_i$ – кількість набраних здобувачем балів за семестр за виконання і-го виду робіт під час навчальних занять (за 100-бальною шкалою);

$ВК_i$ – ваговий коефіцієнт за виконання і-го виду робіт під час навчальних занять. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості

балів, яка передбачена за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що передбачена за виконання завдань під час навчальних занять за семестр, на 100 балів.

Розподіл балів за виконання завдань модульного контролю

Види робіт здобувача вищої освіти денної форми навчання[1]	Кількість балів за семестр
Виконання завдань модульного контролю 1	10
Виконання завдань модульного контролю 2	10
Виконання завдань модульного контролю 3	10
Виконання завдань модульного контролю 4	10
Разом за виконання завдань модульного контролю	**40**

[1] Зарахування балів за виконання завдань модульного контролю здійснюється за умови, що здобувач вищої освіти набрав не менше 60% від максимальної кількості балів, які передбачені для даного виду контролю.

Якщо здобувач вищої освіти денної форми навчання виконав завдання модульного контролю і з урахуванням отриманих балів за поточний контроль набрав у сумі 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти денної форми навчання під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі екзамену. Набрані бали за виконання завдань підсумкового контролю, а також бали за поточний контроль сумуються і формується семестрова оцінка з навчальної дисципліни. Бали, які здобувач вищої освіти набрав за виконання завдань модульного контролю, при цьому не враховуються під час розрахунку семестрової оцінки з навчальної дисципліни.

У здобувача вищої освіти заочної форми навчання семестрова оцінка за вивчення навчальної дисципліни формується як сума кількості балів за поточний контроль і кількості балів за підсумковий контроль.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі екзамену, якщо за виконання завдань поточного контролю набрав 20 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 15–19 балів, він отримує право за власною заявою опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми[1]. Вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 14 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми[1].

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Рекомендовані курси на онлайн-платформах:

№п/п	Платформа	Назва курсу	Посилання
1	Cisco	Вступ до кібербезпеки	https://www.netacad.com/launch?id=ec71a201-4e44-43b0-8225-4767e26b0e9b
2	Udacity	Introduction to Cybersecurity	https://click.linksynergy.com/deeplink?id=bt30QTxEyjA&mid=53187&murl=https%3A%2F%2Fwww.udacity.com%2Fcourse%2Fintro-to-cybersecurity-nanodegree--

[1] Положення щодо вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, не поширюється на останній семестр навчання на всіх рівнях вищої освіти.

			nd545&u1=cyber9security9certifications9courses
3	Udacity	Інженер з безпеки	https://click.linksynergy.com/deeplink?id=bt30QTxEyjA&mid=53187&murl=https%3A%2F%2Fwww.udacity.com%2Fcourse%2Fsecurity-engineer-nanodegree--nd698&u1=cyber9security9certifications9courses
4	Skillshare	Кібербезпека: перейдіть від нуля до героя	https://guru99.click/3ia5gw
5	Coursera	Кібербезпека для всіх	https://imp.i384100.net/eKrPeD
6	Coursera	Вступ до спеціалізації з кібербезпеки	https://imp.i384100.net/gb7Wk0

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	Авторизація	Authorization
2	Авторське право	Copyright / author’s right
3	Академічна доброчесність	Academic integrity
4	Аутентифікація	Authentication
5	Впровадження	Implementation
6	Гіпотеза	Hypothesis
7	Доступність	Accessibility
8	Евристично-орієнтований	Heuristics-based
9	Експеримент	Experiment
10	Ефект	Effect
11	Ідентифікація	Identification
12	Інформація	Information
13	Кібербезпека	Cybersecurity
14	Конфіденційність	Confidentiality

№ з/п	Термін державною мовою	Відповідник англійською мовою
15	Метод дослідження	Research method
16	Моделювання	Modelling
17	Наука	Science
18	Орієнтований на поведінку	Behavior-based
19	Посвідчення особи	Know Your Customer (KYC)
20	Приватний ключ	Private key
21	Публічний ключ	Public key
22	Сигнатурно-орієнтований	Signature-based
23	Транзакція	Transaction
24	Хеш	Hesh
25	Хеш-дерево, дерево Меркла	Merkle tree
26	Цілісність	Integrity
27	Шифрування	Encryption

12. Рекомендована література

Основна література

1. ДСТУ ISO/IEC 27001:2023. Інформаціна безпека, кібербезпека та захист конфіденційності. Системи керування безпекою. Вимоги.

2. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

4. Дудикевич, В. Б. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.

5. Інформаційна безпека та гібридні загрози: навчальний посібник. Укл. Мухін В.Є., Завгородній В.В., Завгородня Г.А. Київ : ТОВ «ТРОПЕА», 2024. 104 с. DOI: https://doi.org/10.32703/978-617-8268-36-7.

6. Oleksandr O. Nonik, Nadiia M. Lobanchykova, Tetiana A. Vakaliuk, Viacheslav V. Osadchyi and Oleksandr V. Farrakhov. Approaches to solving proxy performance problems for HTTP and SOCKS5 protocols for the case of multi-port passwordless access. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems. Kyiv, Ukraine, February 28, 2024. Edited by Volodymyr Sokolov, Vasyl Ustimenko, Tamara Radivilova, Mariya Nazarkevych. CEUR Workshop Proceedings, 2024. Vol. 3654. Pp. 189–200. – Режим доступу: https://ceur-ws.org/Vol-3654/paper16.pdf

7. Lobanchykova N. M., Vakaliuk T. A., Osadchyi V. V., Medvediev M. G., Pilkevych I. A. Study of Cyber Security Approaches in Organizing Digital Voting. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023), Kyiv, Ukraine, February 28, 2023. Edited by Volodymyr Sokolov, Tamara Radivilova, Vasyl Ustimenko, Mariya Nazarkevych. CEUR Workshop Proceedings, Vol-3421, 2023. Pp. 198-205. – Режим доступу: https://ceur-ws.org/Vol-3421/short5.pdf

8. Lobanchykova N., Kredentsar S., Pilkevych I., Medvediev M. Information technology for mobile perimeter security systems creation. Journal of Physics: Conference Series. 2021. Vol. 1840 (1). Art. no. 012022. DOI: 10.1088/1742-6596/1840/1/012022. Режим доступу: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103522219&doi=10.1088%2f1742-6596%2f1840%2f1%2f012022&partnerID=40&md5=8d5fda39b672fb3bf33a951aa8f94578

9. Lobanchykova, N., Pilkevych, I., Korchenko, O. Analysis of attacks on components of IoT systems and cybersecurity technologies. Joint Proceedings of the Workshops on Quantum Information Technologies and Edge Computing (QuaInT+doors 2021), Zhytomyr, Ukraine, April 11, 2021. Edited by Serhiy O. Semerikov. (CEUR-WS.org). pp. 83-96.

10. Lobanchykova N., Kredentsar S., Pilkevych I., Medvediev M. Information technology for mobile perimeter security systems creation. Journal of Physics: Conference Series, Volume 1840, 012051, XII International Conference on Mathematics, Science and Technology Education (ICon-MaSTEd 2020) 15-17 October 2020, Kryvyi Rih, Ukraine. pp.1-9.

11. Законодавство України: https://zakon.rada.gov.ua/

12. Вакалюк Т. А., Фант М. О., Єфремов Ю.М., Лобанчикова Н.М., Жиляєв Є. В. Огляд алгоритмів виявлення аномалій в роботі комп'ютерних систем. Вісник Кременчуцького національного університету імені Михайла Остроградського, № 6 (149), 2024. С. 94-101. – Режим доступу: https://doi.org/10.32782/1995-0519.2024.6.11.

13. Лобанчикова Н.М. Модель побудови мобільної систем охорони периметру території .Сучасний захист інформації, 2020.Вип №1(41). С.42 – 48.

14. Digitalization of economics : inter-disciplinary and inter-branch approach : manual. Zhytomyr : Publishing House "Book-Druk", 2023. 540 p.

15. Методичні рекомендації до виконання лабораторних робіт. з навчальної дисципліни «Основи кібербезпеки» для студентів освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека»ю Частина 2. (автори: Н.М. Лобанчикова, О.В. Пірог), 2021. 36 с. Електронне видання (Протокол НМР №6 від 21.01.2021 р.). – Режим доступу: https://learn.ztu.edu.ua/course/view.php?id=1994

16. Методичні рекомендації до виконання лабораторних робіт. з навчальної дисципліни «Основи кібербезпеки» для студентів освітнього ступеня «бакалавр» спеціальності 125 «Кібербезпека». Частина 1 (автори: Н.М. Лобанчикова, О.В. Пірог), 2021. 56 с. Електронне видання (Протокол НМР №6 від 21.01.2021 р.). – Режим доступу: https://learn.ztu.edu.ua/course/view.php?id=1994

17. Опорний конспект лекцій з дисципліни «Технічні засоби захисту інформації» для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. – Тернопіль 2023. – 88 с.

Допоміжна література

18. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

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

20. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation crite¬ria for IT security – Part 2: Security functional requirements.

21. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation crite¬ria for IT security – Part 3: Security assurance requirements.

22. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01–01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).

12. Інформаційні ресурси в Інтернеті

23. Макс Бонк. Розуміння різних типів технік виявлення антивірусів – від сигнатурних до поведікових аналізаторів. MEDIACOM: світ новин. 08 квітня 2024. URL: https://mediacom.com.ua/rozuminnya-riznix-tipiv-texnik-viyavlennya-antivirusiv/

24. Сайт бібліотеки Державного університету «Житомирська політехніка». URL: http://lib.ztu.edu.ua.

25. Освітній портал Державного університету «Житомирська політехніка». URL: http://learn.ztu.edu.ua.

26. globalEDGE / Michigan State University. URL: https://globaledge.msu.edu.

27. Сайт Національної бібліотеки України ім. Вернадського. URL: http://www.nbuv.gov.ua.

28. Сервіс Google Академія. URL: https://scholar.google.com.ua.

Наукометрична база Scopus. URL: https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=searchbasic#basic.