ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 серпня 2024 р., протокол №8

Голова Вченої ради

_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни фахової підготовки «Інфраструктура відкритих ключів»

факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри комп'ютерної інженерії та кібербезпеки
26 серпня 2024 р., протокол №6

Завідувач кафедри

_____ Андрій ЄФІМЕНКО

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Наталія ЩУР

Житомир
2024 – 2025 н.р.

Робоча програма вибіркової навчальної дисципліни «Інфраструктура відкритих ключів» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни
	денна форма навчання
Кількість кредитів 4	Вибіркова
Модулів – 1	Лекції
	32 год.
Змістових модулів – 2	Практичні
	–
Загальна кількість годин – 120	Лабораторні
	32 год.
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи – 3,5	Самостійна робота
	56 год.
	Вид контролю: залік

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.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни є формування у студентів теоретичних знань та практичних навичок у галузі створення, впровадження та експлуатації інфраструктури відкритих ключів, а також розуміння їх застосування для захисту конфіденційних даних.

Завданнями навчальної дисципліни є:

– надання студентам базових теоретичних знань щодо принципів роботи та архітектури інфраструктури відкритих ключів;

– формування практичних навичок проєктування, впровадження та супроводу систем інфраструктури відкритих ключів.

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен *знати:*

– загальні принципи побудови інфраструктури відкритих ключів та їх роль у забезпеченні інформаційної безпеки;

– засади правового регулювання електронних довірчих послуг і забезпечення правового режиму електронного цифрового підпису;

– основні нормативні документи та міжнародні стандарти з інформаційної безпеки, вимоги до побудови захищених систем і процес підтвердження їх відповідності;

– принципи побудови політики безпеки інфраструктури відкритих ключів та її складові;

– характеристики технологічних рішень для захисту інформації, їх типи та призначення;

– основи оцінювання ефективності та стійкості систем захисту елементів інфраструктури відкритих ключів.

вміти:

– проєктувати та реалізовувати архітектуру інфраструктури відкритих ключів з урахуванням завдань, вихідних даних і технологічних факторів;

– здійснювати аналіз параметрів інфраструктури відкритих ключів, її організаційної структури та взаємозв’язків елементів;

– використовувати на практиці національні та міжнародні стандарти для аналізу, проєктування та оцінки інфраструктури відкритих ключів;

– застосовувати сучасні технології для побудови, налаштування та супроводу інфраструктури відкритих ключів, оцінювати їх ефективність;

– проводити порівняння технологічних рішень і підходів до створення інфраструктури відкритих ключів, розробляти рекомендації з їх оптимізації.

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

– комунікативні навички: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію;

– керування часом: уміння справлятися із завданнями вчасно;

– гнучкість і адаптивність: гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

– особисті якості: креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

МОДУЛЬ 1

Змістовий модуль 1. Теоретичні основи інфраструктури відкритих ключів

Тема 1. Призначення інфраструктури відкритих ключів (ІВК) та сфери застосування

Роль ІВК у сучасних інформаційних системах. Сфери використання: електронний документообіг, фінансові послуги, електронна комерція, захищені комунікації.

Тема 2. Основні криптографічні примітиви та механізми інфраструктури відкритих ключів

Принципи асиметричного шифрування. Криптографічні алгоритми: RSA, ECC. Використання цифрових підписів, автентифікації та шифрування.

Тема 3. Теоретичні основи застосування ІВК

Ключові компоненти ІВК: сертифікаційні центри, реєстраційні органи, довірчі відносини. Основи взаємодії між компонентами.

Тема 4. Формати сертифікатів та життєвий цикл

Формати сертифікатів (X.509). Процеси генерування, оновлення, відкликання, призупинення дії та закінчення терміну дії сертифікатів.

Тема 5. Механізми відкликання сертифікатів та публікація списків

Механізми періодичної публікації CRL (Certificate Revocation List). Використання OCSP (Online Certificate Status Protocol). Проблеми управління списками відкликаних сертифікатів.

Тема 6. Розповсюдження інформації в ІВК

Організація публікації сертифікатів. Використання міждоменних сховищ, колективних сховищ, пограничних сховищ. Проблеми, що виникають при реалізації ІВК.

Змістовий модуль 2. Практичні аспекти впровадження інфраструктури відкритих ключів

Тема 7. Завдання та шляхи розгортання ІВК

Визначення основних завдань при проєктуванні ІВК. Критерії вибору технологій, програмних і апаратних засобів.

Тема 8. Політики безпеки та вибір постачальника технологій або сервісів

Основні положення політики безпеки. Розробка документів для забезпечення інформаційної безпеки. Проблеми вибору технологій або сервісів для реалізації ІВК.

Тема 9. Планування та створення інфраструктури

Процеси планування, створення, адміністрування та управління ІВК. Особливості впровадження ІВК у різних організаціях.

Тема 10. Нормативно-законодавча база в галузі ІВК

Огляд законів України у сфері створення та використання ІВК. Вимоги міжнародних стандартів (ISO/IEC, ETSI).

Тема 11. Державне регулювання впровадження ІВК та криптосистем

Роль державних органів у розробці та впровадженні ІВК. Особливості використання криптографічних систем у державному секторі.

Тема 12. Типові технології використання ІВК в інформаційно-комунікаційних системах

Використання ІВК у корпоративних системах. Інтеграція ІВК у вебсервери, захищені мережі та електронні платформи.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин			
	денна форма			
	усього	лекції	лабораторні	самостійна робота
МОДУЛЬ 1				
Змістовий модуль 1. Теоретичні основи інфраструктури відкритих ключів				
Тема 1. Призначення інфраструктури відкритих ключів (ІВК) та сфери застосування	10	2	2	6
Тема 2. Основні криптографічні примітиви та механізми інфраструктури відкритих ключів	10	4	4	2
Тема 3. Теоретичні основи застосування ІВК	10	2	2	6
Тема 4. Формати сертифікатів та життєвий цикл	10	4	4	2
Тема 5. Механізми відкликання сертифікатів та публікація списків	10	2	2	6
Тема 6. Розповсюдження інформації в ІВК	10	2	2	6
Разом за змістовий модуль 1	60	16	16	28
Змістовий модуль 2. Практичні аспекти впровадження інфраструктури відкритих ключів				
Тема 7. Завдання та шляхи розгортання ІВК	10	2	4	4
Тема 8. Політики безпеки та вибір постачальника технологій або сервісів	10	2	2	6
Тема 9. Планування та створення інфраструктури	10	4	4	2
Тема 10. Нормативно-законодавча база в галузі ІВК	10	4	2	4
Тема 11. Державне регулювання впровадження ІВК та криптосистем	10	2	2	6
Тема 12. Типові технології використання ІВК в інформаційно-комунікаційних системах	10	2	2	6
Разом за змістовий модуль 2	60	16	16	28
ВСЬОГО	120	32	32	56

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин
		денна форма
МОДУЛЬ 1		
Змістовий модуль 1. Теоретичні основи інфраструктури відкритих ключів		
1	Ознайомлення з інструментами для створення та управління сертифікатами в інфраструктурі відкритих ключів	4
2	Генерація ключових пар та формування сертифікатів X.509 за допомогою криптографічних інструментів	4
3	Управління життєвим циклом сертифікатів: генерування, відкликання, призупинення дії та перевірка статусу	4
4	Розгортання сертифікаційного центру для управління сертифікатами та забезпечення довіри	4
Змістовий модуль 2. Практичні аспекти впровадження інфраструктури відкритих ключів		
5	Організація зберігання сертифікатів і списків відкликаних сертифікатів у сховищах	4
6	Розробка політики безпеки для управління сертифікатами та захисту ключів	4
7	Інтеграція сертифікатів ІВК у захищені системи для автентифікації, підписів і шифрування	4
8	Аналіз ефективності та стійкості ІВК, перевірка відповідності стандартам безпеки	4
	РАЗОМ	**32**

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
		денна форма
МОДУЛЬ 1		
Змістовий модуль 1. Теоретичні основи інфраструктури відкритих ключів		
1	Тема 1. Призначення інфраструктури відкритих ключів (ІВК) та сфери застосування Застосування ІВК у системах безпечного електронного голосування	4
2	Тема 2. Основні криптографічні примітиви та механізми інфраструктури відкритих ключів Порівняння алгоритмів RSA та ECC за продуктивністю в мобільних додатках	4
3	Тема 3. Теоретичні основи застосування ІВК Моделі довірчих відносин у багаторівневих інфраструктурах	6
4	Тема 4. Формати сертифікатів та життєвий цикл Аналіз ключових полів сертифікатів формату X.509 і їхнього призначення	6
5	Тема 5. Механізми відкликання сертифікатів та публікація списків Використання OCSP для перевірки статусу сертифікатів у реальному часі.	6
6	Тема 6. Розповсюдження інформації в ІВК Роль міждоменних сховищ у глобальних мережах з розподіленою архітектурою	6
Змістовий модуль 2. Практичні аспекти впровадження інфраструктури відкритих ключів		
7	Тема 7. Завдання та шляхи розгортання ІВК Оцінка критеріїв вибору апаратного та програмного забезпечення для ІВК	6
8	Тема 8. Політики безпеки та вибір постачальника технологій або сервісів Аналіз ризиків, пов’язаних із вибором стороннього постачальника технологій для ІВК	6
9	Тема 9. Планування та створення інфраструктури Планування інтеграції ІВК із системами інтернету речей (IoT)	6
10	Тема 10. Нормативно-законодавча база в галузі ІВК Аналіз вимог міжнародного стандарту ISO/IEC 27001 для ІВК	6
11	Тема 11. Державне регулювання впровадження ІВК та криптосистем Роль держави у забезпеченні відповідності національних ІВК міжнародним стандартам.	4
12	Тема 12. Типові технології використання ІВК в інформаційно-комунікаційних системах Інтеграція ІВК у вебсервери для забезпечення захищених HTTPS-з’єднань	4
	РАЗОМ	**56**

7. Індивідуальні самостійні завдання

Індивідуальні завдання не передбачені навчальним планом.

8. Методи навчання

Під час викладання навчальної дисципліни використовуються наступні методи навчання.

- Вербальні методи (лекція, пояснення)
- Наочні методи (спостереження, демонстрація, ілюстрація)
- Практичні методи (виконання лабораторних завдань)
- Дискусійний метод
- Метод активного навчання (мозковий штурм)
- Ситуаційний метод
- Методи самостійної роботи (проведення розрахунків)

9. Методи контролю

Перевірка досягнення результатів навчання здійснюється з використанням наступних методів.

- Усне опитування, участь у дискусії, відповіді на проблемні запитання
- Перевірка виконання та захист лабораторних робіт
- Експрес-тестування
- Перевірка виконання завдань модульного контролю
- Залік

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 та підсумковий контроль.

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.

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 заліку. Процедура складання заліку 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
	денна форма
Виконання завдань поточного контролю	100
Підсумкова семестрова оцінка	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Виконання завдань під час навчальних занять	100
Виконання та захист індивідуальних самостійних завдань	–
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт (наводиться перелік інших видів робіт)	–
Разом за виконання завдань поточного контролю	**100**

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Виконання тестових завдань	40
Виконання та захист лабораторних робіт	60
Разом за виконання завдань під час навчальних занять	**100**

З метою застосування цілих чисел для оцінювання активностей здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$Р_{НЗ} = (Р_{ТЗ^{100}} \times ВК_{ТЗ} + Р_{ЛР^{100}} \times ВК_{ЛР}) \times К_{НЗ}, \qquad (1)$$

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

$Р_{ТЗ100}$, $Р_{ЛР100}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за виконання тестових завдань, виконання та захист лабораторних робіт (за 100-бальною шкалою);

$ВК_{ТЗ}$, $ВК_{ЛР}$ – вагові коефіцієнти відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання іншого виду робіт, визначеного викладачем. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, які встановлені за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання цих робіт (дані для розрахунку вагових коефіцієнтів наведено в табл. «Розподіл балів за виконання завдань під час навчальних занять»);

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

Якщо здобувач вищої освіти набрав за поточний контроль 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 під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35–49 балів, він отримує право за власною заявою опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. 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 34 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.

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».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1	Інфраструктура відкритих ключів	Public key infrastructure (PKI)
2	Сертифікат	Certificate
3	Сертифікаційний центр	Certification authority (CA)
4	Реєстраційний орган	Registration authority (RA)
5	Відкритий ключ	Public key
6	Закритий ключ	Private key
7	Цифровий підпис	Digital signature
8	Список відкликаних сертифікатів	Certificate revocation list (CRL)
9	Протокол перевірки статусу сертифікатів	Online certificate status protocol (OCSP)
10	Довірчі відносини	Trust relationships
11	Політика сертифікації	Certificate policy
12	Пограничне сховище	Boundary repository

№ з/п	Термін державною мовою	Відповідник англійською мовою
13	Міждоменне сховище	Cross-domain repository
14	Політика безпеки	Security policy
15	Життєвий цикл сертифіката	Certificate lifecycle
16	Формат сертифікатів	Certificate format
17	Електронний цифровий підпис	Electronic digital signature (EDS)
18	Хешування	Hashing
19	Криптографічний алгоритм	Cryptographic algorithm
20	Асиметричне шифрування	Asymmetric encryption

12. Рекомендована література

Основна література

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
2. Горобець В.П., Стельмах І.О. Інфраструктура відкритих ключів: основи та практичні аспекти. – Львів: Видавництво Львівської політехніки, 2021. – 320 с.
3. Пономаренко І.В., Лисак О.Г., Шелест М.Є. Захист інформації в інформаційних системах: підручник. – Харків: ХНЕУ, 2020. – 280 с.

Допоміжна література

1. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко, І.Д. Горбенко; Харк. нац. ун-т радіоелектрон., ЗАТ Ін-т інформ. технологій. – Х.: Форт, 2010. – 593 с.
2. Гнатюк С.П., Остроградський І.В. Цифрові підписи: технології та їх використання. – Вінниця: ВНТУ, 2017. – 180 с.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – John Wiley & Sons, 2015. – 784 p.
4. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. – Wiley Publishing, 2010. – 384 p.

13. Інформаційні ресурси в Інтернеті

1. The CrypTool Portal. URL: http://www.cryptool.org/en
2. Let's Encrypt: Free SSL/TLS Certificates. URL: https://letsencrypt.org/
3. OpenSSL: Cryptography and SSL/TLS Toolkit. URL: https://www.openssl.org/