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
«Безпека додатків ОС Windows»

факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри інженерії програмного забезпечення

28 __08__ 2024 р., протокол № 7

Завідувач кафедри

_____ Тетяна ВАКАЛЮК

Розробник: старший викладач кафедри інженерії програмного забезпечення
Олег ВЛАСЕНКО

Житомир
2024 – 2025 н.р.

Робоча програма вибіркової навчальної дисципліни «Безпека додатків ОС Windows» 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 – 7	**Лекції**
Змістових модулів – 16	32 год
Загальна кількість годин – 120	**Лабораторні**
	32 год
	Самостійна робота
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 3,5	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.

Метою вивчення навчальної дисципліни є формування знань і навичок у здобувачів вищої освіти щодо забезпечення безпеки додатків у операційній системі Windows.

Завданнями навчальної дисципліни є:

Ознайомлення з основами безпеки операційних систем, зокрема Windows.

Вивчення типових загроз і вразливостей додатків, що працюють в ОС Windows.

Розробка методів захисту даних і користувацьких налаштувань від несанкціонованого доступу.

Застосування методів аутентифікації та авторизації для контролю доступу до додатків.

Використання шифрування для захисту даних під час зберігання і передачі.

Розробка і впровадження механізмів для виявлення і блокування шкідливого коду.

Вивчення підходів до безпечного програмування та тестування додатків на вразливості.

Ознайомлення з інструментами та техніками для моніторингу та аудиту безпеки додатків.

Soft Skills, які здобувачі вищої освіти можуть отримати:

Комунікативні навички: вміння чітко презентувати та обговорювати питання безпеки, а також співпрацювати з іншими розробниками для забезпечення безпеки додатків.

Керування часом: здатність організовувати процес розробки з урахуванням безпекових аспектів, виконуючи проекти в межах заданих термінів.

Гнучкість і адаптивність: здатність швидко адаптуватися до нових загроз і технологій, ефективно реагувати на зміни у вимогах безпеки.

Особисті якості: здатність до аналітичного мислення при виявленні вразливостей, увага до деталей при розробці безпечного коду та креативний підхід до захисту додатків.

3. Програма навчальної дисципліни

Модуль 1. Вступ до безпеки додатків ОС Windows

Змістовий модуль 1. Основи безпеки операційних систем. Принципи захисту даних та програм у ОС Windows.
Змістовий модуль 2. Архітектура ОС Windows та безпека: ядро, користувацький простір, процеси та потоки.
Змістовий модуль 3. Відмінності між локальними та мережевими загрозами безпеці додатків.
Змістовий модуль 4. Встановлення середовища розробки для безпечних додатків: Visual Studio, Windows SDK, інструменти для аналізу безпеки.

Модуль 2. Захист від загроз і вразливостей в додатках

Змістовий модуль 5. Аутентифікація та авторизація користувачів в додатках для ОС Windows. Роль Active Directory та локальних облікових записів.
Змістовий модуль 6. Уразливості додатків: SQL ін’єкції, міжсайтові скрипти (XSS), міжсайтові підробки запитів (CSRF). Методи захисту.
Змістовий модуль 7. Захист пам’яті додатків: переповнення буфера та використання технологій ASLR (Address Space Layout Randomization) і DEP (Data Execution Prevention).
Змістовий модуль 8. Робота з файловими системами: доступ до файлів, шифрування, ACL (Access Control List).

Модуль 3. Безпека мережевих з’єднань та взаємодія додатків

Змістовий модуль 9. Захист даних при передачі через мережу: SSL/TLS, VPN, шифрування протоколів.
Змістовий модуль 10. Мережеві атаки: DOS, DDOS, Man-in-the-Middle (MITM). Захист від мережевих атак у додатках Windows.
Змістовий модуль 11. Контроль доступу та моніторинг активності додатків у мережі. Використання Windows Defender, Event Log та інших засобів.
Змістовий модуль 12. Безпека API та взаємодія додатків через COM, .NET, REST API.

Модуль 4. Практичні аспекти безпеки додатків для ОС Windows

Змістовий модуль 13. Безпечна розробка додатків для ОС Windows: принципи найменших прав, обробка помилок та захист від несанкціонованого доступу.
Змістовий модуль 14. Аналіз вразливостей додатків за допомогою інструментів безпеки: Burp Suite, Wireshark, Windows Sysinternals.
Змістовий модуль 15. Використання Windows Sandbox та віртуальних машин для тестування безпеки додатків.
Змістовий модуль 16. Завершальний проект: створення безпечного додатку для ОС Windows із використанням вивчених технік безпеки, тестування та аналіз вразливостей.

4. Структура (тематичний план) навчальної дисципліни

	Змістовні модулі	Кількість годин			
		Всього	Лекції	Лабораторні роботи	Самостійна робота
1	2	3	4	5	6
1	**Модуль 1. Вступ до безпеки додатків ОС Windows**				
	Змістовий модуль 1.				
	Тема 1. Основи безпеки операційних систем. Принципи захисту даних та програм у ОС Windows.		***2***	***1***	***3***
	Разом змістовий модуль 1				
	Змістовий модуль 2.				
	Тема 2. Архітектура ОС Windows та безпека: ядро, користувацький простір, процеси та потоки.		***2***	***2***	***3***
	Разом змістовий модуль 2				
2	**Модуль 2. Захист від загроз і вразливостей в додатках**				
	Змістовий модуль 3.				
	Тема 3. Відмінності між локальними та мережевими загрозами безпеці додатків.		***2***	***3***	***3***
	Разом змістовний модуль 3				
	Змістовий модуль 4.				
	Тема 4. Встановлення середовища розробки для безпечних додатків: Visual Studio, Windows SDK, інструменти для аналізу безпеки.		***2***	***2***	***3***
	Разом змістовний модуль 4				
	Змістовий модуль 5.				
	Тема 5. Аутентифікація та авторизація користувачів в додатках для ОС Windows. Роль Active Directory та локальних облікових записів.		***2***	***2***	***3***
	Разом змістовний модуль 5				
3	**Модуль 3. Безпека мережевих з'єднань та взаємодія додатків**				
	Змістовий модуль 6.				
	Тема 6. Уразливості додатків: SQL ін'єкції, міжсайтові скрипти (XSS), міжсайтові підробки запитів (CSRF). Методи захисту.		***2***	***2***	***3***
	Разом змістовний модуль 6				
	Змістовий модуль 7.				
	Тема 7. Захист пам'яті додатків: переповнення буфера та використання технологій ASLR (Address Space Layout Randomization) і DEP (Data Execution Prevention).		***2***	***2***	***4***
	Разом змістовний модуль 7				
	Змістовий модуль 8.				

	Тема 8. Робота з файловими системами: доступ до файлів, шифрування, ACL (Access Control List).		***2***	***2***	***3***
	Разом змістовний модуль 8				
	Змістовий модуль 9.				
	Тема 9. Захист даних при передачі через мережу: SSL/TLS, VPN, шифрування протоколів.		***2***	***2***	***3***
	Разом змістовний модуль 9				
4	**Модуль 4. Практичні аспекти безпеки додатків для ОС Windows**				
	Змістовий модуль 10.				
	Тема 10. Мережеві атаки: DOS, DDOS, Man-in-the-Middle (MITM). Захист від мережевих атак у додатках Windows.		***2***	***2***	***2***
	Разом змістовний модуль 10				
	Змістовий модуль 11.				
	Тема 11. Контроль доступу та моніторинг активності додатків у мережі. Використання Windows Defender, Event Log та інших засобів.		***2***	***2***	***2***
	Разом змістовний модуль 11				
	Змістовий модуль 12.				
	Тема 12. Безпека API та взаємодія додатків через COM, .NET, REST API.		***2***	***2***	***2***
	Разом змістовний модуль 12				
	Змістовий модуль 13.				
	Тема 13. Безпечна розробка додатків для ОС Windows: принципи найменших прав, обробка помилок та захист від несанкціонованого доступу.		***2***	***2***	***4***
	Разом змістовний модуль 13				
	Змістовий модуль 14.				
	Тема 14. Аналіз вразливостей додатків за допомогою інструментів безпеки: Burp Suite, Wireshark, Windows Sysinternals.		***2***	***2***	***4***
	Разом змістовний модуль 14				
	Змістовий модуль 15.				
	Тема 15. Використання Windows Sandbox та віртуальних машин для тестування безпеки додатків.		***2***	***2***	***4***
	Разом змістовний модуль 15				
	Змістовий модуль 16.				
	Тема 16. Завершальний проект: створення безпечного додатку для ОС Windows із використанням вивчених технік безпеки, тестування та аналіз вразливостей.		***2***	***2***	***4***
	Разом змістовний модуль 16				
	ВСЬОГО	***150***	***32***	***32***	***56***

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин
		денна форма
1.	Лабораторна робота №1. Ознайомлення з основами безпеки додатків ОС Windows. Встановлення середовища для аналізу безпеки додатків.	4
2.	Лабораторна робота №2. Виявлення вразливостей: SQL ін’єкції та XSS атаки. Методи захисту.	4
3.	Лабораторна робота №3. Використання технологій DEP та ASLR для захисту додатків від переповнення буфера.	4
4.	Лабораторна робота №4. Налаштування контролю доступу до файлів. Використання ACL та безпека файлової системи в ОС Windows.	4
5.	Лабораторна робота №5. Реалізація аутентифікації та авторизації користувачів у додатках за допомогою Active Directory.	4
6.	Лабораторна робота №6. Захист передавання даних через мережу: SSL/TLS, VPN в додатках для ОС Windows.	4
7.	Лабораторна робота №7. Аналіз вразливостей додатків за допомогою інструментів безпеки: Wireshark, Burp Suite.	4
8.	Лабораторна робота №8. Створення безпечного додатку для ОС Windows. Перевірка вразливостей та тестування захисту.	4
РАЗОМ		**32**

6. Завдання для самостійної роботи

№	**Назва теми**	Кількість годин
		денна форма
1.	Робота з привілеями користувачів в ОС Windows. Контроль доступу за допомогою групових політик та ACL.	3
2.	Виявлення та усунення вразливостей у мережевих додатках Windows. Методи захисту від DOS, DDOS атак.	3
3.	Реалізація та тестування різних методів аутентифікації: двофакторна, біометрія, паролі.	4
4.	Використання технології шифрування для захисту даних у додатках: Windows Data Protection API.	6
5.	Постобробка та аудит додатків за допомогою Windows Event Log та моніторингу системи безпеки.	6
6.	Реалізація безпеки API: захист від несанкціонованого доступу до інтерфейсів додатків за допомогою токенів.	6
7.	Тестування та усунення вразливостей у клієнт-серверних додатках за допомогою аналізу мережевих з’єднань.	10
8.	Розробка додатків з використанням Windows Sandbox для тестування безпеки в ізольованому середовищі.	12
РАЗОМ		**56**

7. Індивідуальні завдання

Індивідуальні заняття не передбачено 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 практичних 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 під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання та захист лабораторних робіт	48	–
Відповіді (виступи) за виконане домашнє завдання	12	–
Разом за виконання завдань поточного контролю	**60**	**–**

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

$$Р_{НЗ} = (Р_{ЛР_{100}} \times ВК_{ЛР} + Р_{ПТ_{100}} \times ВК_{ПТ} + Р_{ЛЕК_{100}} \times ВК_{ЛЕК} + Р_{ІТЕ_{100}} \times ВК_{ІТЕ}) \times К_{НЗ}, \qquad (1)$$

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

$Р_{ЛР_{100}}$, $Р_{ПТ_{100}}$, $Р_{ЛЕК_{100}}$, $Р_{ІТЕ_{100}}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за виконання та захист лабораторних робіт, виконання поточних тестів, участь у лекційних заняттях, проходження курсу IT Essentials (кожний окремо вид робіт на навчальних заняттях оцінюється за 100бальною шкалою);

$ВК_{ЛР}$, $ВК_{ПТ}$, $ВК_{ЛЕК}$, $ВК_{ІТЕ}$ – вагові коефіцієнти відповідно за виконання та захист лабораторних робіт, виконання поточних тестів, участь у лекційних заняттях, проходження курсу IT Essentials. 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[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».

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.	Захист від SQL-ін'єкцій	SQL Injection Protection
2.	Аутентифікація та авторизація	Authentication and Authorization
3.	Використання Active Directory	Active Directory Usage
4.	Контроль доступу за допомогою ACL	Access Control List (ACL)
5.	Захист від атак переповнення буфера	Buffer Overflow Protection
6.	Шифрування даних	Data Encryption
7.	Мережевий моніторинг безпеки	Network Security Monitoring
8.	Використання SSL/TLS для захисту передавання даних	SSL/TLS Protocol for Data Transmission
9.	Захист передавання паролів	Password Transmission Protection
10.	Виявлення уразливостей у додатках	Application Vulnerability Detection
11.	Безпека API	API Security
12.	Двофакторна аутентифікація	Two-Factor Authentication
13.	Використання шифрування на рівні диска	Disk-Level Encryption
14.	Безпека файлової системи	File System Security
15.	Аудит безпеки Windows	Windows Security Auditing

12. Рекомендована література

1. Вебер, Г. (2020). Windows Internals, Part 1: System architecture, processes, threads, memory management, and more (8th Edition). Microsoft Press. – 1032 с.
2. Кох, Б., Макконнелл, С. (2019). Secure Coding in C and C++ (2nd Edition). Addison-Wesley. – 672 с.
3. Кросбі, С., Шоу, К. (2021). Windows Security: Essential Techniques for Securing the Operating System. O'Reilly Media. – 602 с.
4. Готліб, А. (2018). Mastering Windows Security and Hardening (5th Edition). Packt Publishing. – 426 с.
5. Хаффман, С. (2022). Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations. Wiley. – 304 с.

Допоміжна література

6. Сміт, Р. (2020). The Windows Security Log: A Practitioner’s Guide to Collecting, Analyzing, and Responding to Security Events. Elsevier. – 250 с.
7. Ерікссон, А. (2019). Practical Windows Forensics. Packt Publishing. – 308 с.
8. Міллер, Л. (2020). Hacking Windows Applications: Techniques for Automating Windows OS Vulnerabilities. Wiley. – 432 с.
9. Лоренц, Т. (2021). The Art of Windows Debugging: Advanced Techniques and Tools for Developers. Apress. – 320 с.
10. Майклс, В. (2021). Advanced Windows Security. A K Peters/CRC Press. – 440 с.

12. Інформаційні ресурси в Інтернеті

11. Офіційна документація Microsoft Windows Security: https://docs.microsoft.com/en-us/windows/security/
12. Ресурси для розробників Windows безпеки: https://devblogs.microsoft.com/security/
13. Форум безпеки Microsoft: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/
14. Ресурси для Windows API та безпеки: https://learn.microsoft.com/en-us/windows/win32/api/
15. Блог по безпеці Windows від Sysinternals: https://docs.microsoft.com/en-us/sysinternals/
16. Ресурси для тестування безпеки додатків на Windows: https://owasp.org/www-project-windows-security/