

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Навчально-науковий інститут комп'ютерних наук та управління проектами

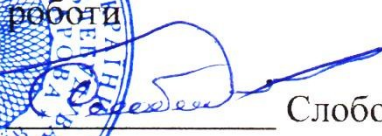
Кафедра програмного забезпечення автоматизованих систем

Код РПНД



ЗАТВЕРДЖЕНО

Проректор з науково-педагогічної
роботи


Слободян С.О.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Program of the Discipline

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Software and Data Security

рівень вищої освіти: _____ перший (бакалаврський) _____

тип дисципліни: _____ обов'язкова _____

мова(и) викладання: _____ українська _____

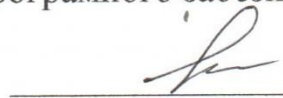
Робоча програма навчальної дисципліни "Безпека програм та даних" є однією із складових комплексної підготовки здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 "Інформаційні технології" спеціальності 121 "Інженерія програмного забезпечення" освітньої програми "Інженерія програмного забезпечення".

"10" листопада 2024 року. – 18 с.

Розробник: Пухалевич А.В., к.т.н., доцент, доцент кафедри програмного забезпечення автоматизованих систем.

Проект робочої програми навчальної дисципліни "Безпека програм та даних" узгоджено з гарантом освітньої програми.

Гарант освітньої програми «Інженерія програмного забезпечення» к.т.н., доцент

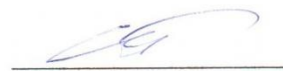


Макарова Л.М.

Проект робочої програми навчальної дисципліни "Безпека програм та даних" розглянуто на засіданні кафедри програмного забезпечення автоматизованих систем.

Протокол №4 від "27" листопада 2024 р.

Завідувач кафедри



Приходько С.Б.

Проект робочої програми навчальної дисципліни "Безпека програм та даних" розглянуто Науково-методичною комісією Навчально-наукового інституту комп'ютерних наук та управління проектами.

Протокол №4 від "28 листопада 2024 р.

Голова



Фаріонова Т.А.

Проект робочої програми навчальної дисципліни "Безпека програм та даних" погоджено з навчальним відділом.

Начальник відділу



Лабарткава А.В.

Робоча програма навчальної дисципліни "Безпека програм та даних" затверджена Навчально-методичною радою НУК.

Протокол №10 від "23" грудня 2024 р.

Голова НМР НУК



Слободян С.О.

© НУК, 2024 рік

Зміст

Вступ.....	4
1. Опис навчальної дисципліни.....	6
2. Мета вивчення навчальної дисципліни.....	7
3. Передумови для вивчення дисципліни	7
4. Очікувані результати навчання.....	7
5. Програма навчальної дисципліни.....	8
6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування	12
7. Форми поточного та підсумкового контролю	12
8. Критерії оцінювання результатів навчання	17
9. Рекомендовані джерела інформації.....	18

Вступ

Анотація

Програма навчальної дисципліни "Безпека програм та даних" складена на підставі навчального плану та є однією із складових комплексної підготовки здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 "Інформаційні технології" спеціальності 121 "Інженерія програмного забезпечення" освітньої програми "Інженерія програмного забезпечення".

Предметом вивчення навчальної дисципліни є формування у студентів знань щодо сучасних стандартів, підходів, методів та засобів захисту програм та даних. Програма дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо програмно-технічного захисту інформації, ідентифікації та аутентифікації користувачів комп'ютерних систем, засобів і методів обмеження доступу до програм, методів та засобів криптографічного захисту інформації, захисту програм від несанкціонованого копіювання, захисту програмних засобів від дослідження. Ця дисципліна відноситься до дисциплін циклу професійної та практичної підготовки. Знання основ дисципліни «Безпека програм та даних» на даний час одним із важливих показників рівня кваліфікації фахівця з програмної інженерії. Студенти при вивченні дисципліни повинні сформуватись вміння класифікувати, ідентифікувати і захищати засоби обробки інформації від несанкціонованого доступу та комп'ютерних вірусів, захищати інформацію персонального комп'ютера та розроблене програмне забезпечення, розробляти індивідуальні системи управління доступом і захистом інформації. Вивчення курсу "Безпека програм та даних" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

Ключові слова: загрози безпеки інформації, криптоалгоритми, симетричні шифри, асиметричні шифри, електронний цифровий підпис, хеш-функція.

Abstract

The curriculum of the program "Software and Data Security" is based on the curriculum and is one of the components of comprehensive training of applicants for the first (bachelor's) level of higher education 12 "Information Technology" specialty 121 "Software Engineering" educational program "Software Engineering" software".

The subject of study of the discipline is the formation of students' knowledge of modern standards, approaches, methods and means of protection of programs and data. The program of the discipline is focused on deep and thorough mastering by students of basic concepts of software and hardware information protection, identification and authentication of users of computer systems, means and methods of restricting access to programs, methods and means of cryptographic protection of information, protection of programs from unauthorized copying and from reverse engineering. This discipline belongs to the disciplines of the cycle of professional and practical training. Knowledge of the basics of the discipline "Software and Data Security" is currently one of the important indicators of the level of qualification of a specialist in software engineering. Students in the discipline must develop the ability to classify, identify and protect information processing tools from unauthorized access and computer viruses, protect personal computer information and software, develop individual access control systems and information security. Studying the course "Security of programs and data" requires purposeful work on the study of special literature, active work in lectures and practical classes, independent work and individual tasks.

Keywords: information security threats, cryptographic algorithms, symmetric ciphers, asymmetric ciphers, electronic digital signature, hash function.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність (освітня програма), освітній рівень	Характеристика навчальної дисципліни	
		Денна форма навчання	Заочна форма навчання
Кількість кредитів – 4	Галузь знань: 12 "Інформаційні технології"	Обов'язкова	
Модулів – 1		Рік підготовки:	
Змістових модулів – 1		2	3
Електронний адрес РПНД на сайті Університету:	Спеціальність 121 "Інженерія програмного забезпечення"	Семестр	
Індивідуальне науково-дослідне завдання (не заплановано)		3	5
		Лекцій	
		15 год.	6 год.
		Практичні, семінарські	
		- год.	- год.
Загальна кількість годин – 120	Освітня програма "Інженерія програмного забезпечення"	Лабораторні	
		30 год.	6 год.
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи студента – 5	Освітній рівень: перший (бакалаврський)	Самостійна робота	
		75 год.	108 год.
		Індивідуальні завдання: - год.	
		Вид контролю: екзамен	
		Форма контролю: комбінована	

2. Мета вивчення навчальної дисципліни

Робоча програма навчальної дисципліни "Безпека програм та даних" складена відповідно до освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12 "Інформаційні технології" спеціальності 121 "Інженерія програмного забезпечення" освітньої програми (ОП) "Інженерія програмного забезпечення". Для зазначеної ОП дисципліна є обов'язковою.

Метою вивчення дисципліни "Безпека програм та даних" є формування у студентів відповідно до освітньо-професійної програми таких компетентностей:

K05. Здатність вчитися і оволодівати сучасними знаннями.

K06. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

K18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

3. Передумови для вивчення дисципліни

Передумовами для вивчення дисципліни "Безпека інформаційних систем, програм та даних" є вивчення дисциплін: «Основи дискретної математики», «Алгоритми та структури даних».

4. Очікувані результати навчання

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів таких результатів навчання:

ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

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.

5. Програма навчальної дисципліни

Модуль 1. Безпека програм та даних

Змістовий модуль 1. Принципи безпеки та захисту інформації в інформаційних системах.

Тема 1. Основні аспекти захисту інформації в АС. Класифікація загроз безпеки програм та даних. Рівні забезпечення безпеки інформації. Сервіси та механізми програмно-технічного рівня захисту інформації. Ідентифікації та аутентифікації користувачів інформаційних систем.

Основні визначення теорії інформаційної безпеки та захисту інформації. Важливість та складність проблеми інформаційної безпеки. Джерела загроз безпеки інформації. Класифікація загроз безпеки програм та даних. Рівні забезпечення безпеки інформації. Законодавчі, правові та організаційні рівні захисту інформації. Основи принципи та механізми програмно-технічного рівня захисту інформації. Сервіси програмно-технічного рівня. Захист від НСД: сервіс ідентифікації і аутентифікації користувача. Основні принципи та методи аутентифікації. [1] – стор. 34-43, 82-91, 92-103, 133-142, 5-9, 250-256, 173-179, [2] стор. 150-166, [3] – стор. 5-12, [6] стор. 5-13.

Тема 2. Сервіси та механізми програмно-технічного рівня захисту інформації. Управління доступом. Міжмережеві екрани.

Політики розмежування прав доступу. Механізми контролю за доступом. Основні моделі управління доступом. Рольове управління доступом. Протоколювання і аудит. Активний аудит. Призначення та функції брандмауерів. Типи брандмауерів. [1] – стор. 119-126, 179-185, 257-260, 270-278, [2] стор. 146-150, 515-525.

Тема 3. Механізми забезпечення конфіденційності. Сервіс криптографічного захисту даних (шифрування).

Основи криптографічного захисту даних. Вимоги до криптографічних систем. Основні поняття і класифікація засобів криптографічного захисту інформації. Класичні техніки шифрування. Підстановки та перестановки. [1] – стор. 262-268, [2] стор. 167-186, [4] стор. 18-34, [5] стор. 40-54, 118-135, [6] стор. 13-31.

Тема 4. Симетричні шифри.

Класифікація симетричних шифрів. Крипостійкість симетричних шифрів. Принципи побудови симетричних шифрів. Мережа Фейстеля. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, Rijndael. [2] – стор. 192-247, 271-282, 433-436, [4] стор. 40-54, [5] стор. 155-169, [6] стор. 31-40.

Тема 5. Асиметричні шифри.

Основні властивості асиметричних шифрів. Принцип побудови асиметричних шифрів. Однонаправлені функції. Математичні основи побудови асиметричних шифрів. Прості та взаємно прості числа. Теорема Ферма. Тест Міллера-Рабіна перевірки числа на простоту. Генерування великих простих чисел та зведення великого цілого числа до цілої степені за модулем n . [2] стор. 396-407, [4] стор. 105-117, [5] стор. 61-63, 71-74, 191-220, [6] стор. 40-50.

Тема 6. Механізми забезпечення автентичності та цілісності даних.

Функції хешування та електронний цифровий підпис. Основні властивості хеш-функцій. Функція хешування SHA, MD5. Однонаправлені хеш-функції на основі симетричних блокових алгоритмів. Ключові і безключові функції хешування. Основні властивості цифрового підпису. Алгоритм цифрового підпису RSA. [2] стор. 408-411, [4] стор. 182-193, 201-209, [5] стор. 284-291, 296-299, [6] стор. 50-58.

Тема 7. Вступ в теорію забезпечення безпеки програмного забезпечення. Методи захисту програмного забезпечення від дослідження. Методи та засоби забезпечення цілісності і достовірності використовуваного програмного коду. Основні підходи до захисту програм від несанкціонованого копіювання.

Загрози безпеки програмного забезпечення. Моделі погроз безпеки програмного забезпечення. Класифікація засобів дослідження програм. Способи захисту програм від дослідження. Способи вбудовування захисних механізмів в програм-

не забезпечення. Обфускація програм. Методи захисту програм від несанкціонованих змін. Основні функції засобів захисту від копіювання. Основні методи захисту від копіювання. [2] – стор. 461-481, [4] – стор. 239-248, [5] – стор. 463-473, 492-496.

Тема 8. Основні принципи та особливості захисту баз даних

Базові способи та засоби захисту баз даних. Захист від SQL ін'єкцій. [3] – стор. 15-36, [6] стор. 58-64.

Тематичний план навчальної дисципліни

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		лек	практ	лаб	с.р.		лек	практ	лаб	с.р.
Модуль 1 Безпека програм та даних										
Змістовий модуль 1. Принципи безпеки та захисту інформації в інформаційних системах										
Тема 1 Основні аспекти захисту інформації в АС. Класифікація загроз безпеки програм та даних. Рівні забезпечення безпеки інформації. Сервіси та механізми програмно-технічного рівня захисту інформації. Ідентифікації та аутентифікації користувачів інформаційних систем.	15	2		4	9	14,5	0,5		1	13
Тема 2. Сервіси та механізми програмно-технічного рівня захисту інформації. Управління доступом. Міжмережеві екрани.	15	2		4	9	14	0,5		0,5	13
Тема 3. Механізми забезпечення конфіденційності. Сервіс криптографічного захисту даних. Класичні техніки шифрування.	15	2		4	9	14	0,5		0,5	13
Тема 4.Симетричні шифри	15	2		4	9	14,5	1		0,5	13
Тема 5. Асиметричні шифри	15	2		4	9	15	1		1	13
Тема 6. Механізми забезпечення автентичності та цілісності даних	15	2		4	9	15	1		1	13
Тема 7. Вступ в теорію забезпечення безпеки програмного забезпечення.	15	2		4	9	15	1		1	13
Тема 8. Основні принципи та особливості захисту баз даних	15	1		2	12	18	0,5		0,5	17
Разом за змістовим модулем 1	120	15		30	75	120	6	-	6	108
Усього годин	120	30		30	75	120	6	-	6	108

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Типові схеми ідентифікації та аутентифікації користувачів комп'ютерної системи	4	1
2	Біометрична аутентифікація за допомогою клавіатурного почерку	4	0,5
3	Криптографічні методи захисту інформації. Табличні перестановки	4	0,5
4	Криптографічні методи захисту інформації. Підстановки	4	0,5
5	Вивчення роботи асиметричних шифрів.	4	1
6	Створення цифрового підпису	4	1
7	Захист даних за допомогою стеганографії	4	1
8	Обфускація	2	0,5
	Разом	30	6

Теми практичних занять

Не заплановані.

Самостійна робота

Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Підготовка до лекцій	15	15
2	Підготовка до лабораторних робіт	30	30
3	Підготовка до модульних контрольних робіт	15	30
4	Підготовка до екзамену	15	33
	Разом	75	108

Індивідуальне науково-дослідне завдання

Не заплановано.

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Набуття здобувачами компетенцій забезпечується через засвоєння навчального матеріалу у вигляді лекційних, лабораторних занять, самостійної роботи студентів та контрольних тестових робіт програмованого типу.

Основними методами навчання з дисципліни є:

1. Пояснювально-ілюстративний метод, за допомогою повідомлення та засвоєння інформації на лекційних та лабораторних заняттях словесними й наочними засобами.

2. Проблемний метод, коли на лабораторних заняттях утворюються пошукові ситуації, розвивається активність, самостійність, творчі здібності здобувачів освіти.

Як наочний матеріал на лекціях застосовуються мультимедійні слайди та лекційні демонстрації.

Засобами діагностики результатів навчання та методами їх демонстрування є:

- виконання завдань лабораторних робіт;
- оформлення звітів лабораторних робіт, захист лабораторних робіт;
- контрольні тестові роботи.

7. Форми поточного та підсумкового контролю

Досягнення студента оцінюються за 100-бальною системою університету.

Система оцінювання знань студентів з дисципліни включає в себе оцінки з поточного контролю, поточного модульного контролю, оцінки за складання екзамену та додаткових заохочувальних балів:

Поточний контроль здійснюється протягом семестру під час проведення лекційних та практичних занять і оцінюється сумою набраних балів. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) та набутих практичних навичок під час виконання завдань практичних робіт;

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку результатів знань студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

Семестровий контроль проводиться у формі екзамену.

Додаткові (заохочувальні) бали студент може отримати за дострокове якісне виконання поточних лабораторних робіт, виконання додаткових завдань, активну участь в обговоренні тем на лекційних заняттях (максимальна кількість 10 балів).

Підсумкова кількість балів за змістовий модуль виставляється як сума балів за всіма формами контролю плюс оцінка підсумкової модульної контрольної. Передбачено проведення однієї модульної контрольної. За ці види робіт протягом семестру студент може набрати від 60 балів до 100 балів.

Семестровий контроль у формі екзамену - підсумкова кількість балів з дисципліни (максимум 100 балів), яка визначається як сума балів за змістовим модулем, безпосередньо екзамену (він не є обов'язковим) та, за наявності, додаткових (заохочувальних) балів. Екзамен виставляється за результатами роботи студента впродовж усього семестру. Студент може бути звільненим від складання екзамену у разі, якщо набрав необхідну кількість балів протягом семестру (60 – 100 балів). Питома вага екзамену (при його наявності) в загальній системі оцінок - 10 балів.

Таким чином, за всі контрольні заходи протягом семестру студент може отримати від 0 до 100 балів. Умовою допуску студента до екзамену є мінімальна сума балів, яку студент повинен набрати у разі виконання всіх елементів змістового модуля. Ця сума складає 50 балів. Якщо студент не набрав мінімальну суму балів, то він не допускається до екзамену і йому рекомендується набрати цю кіль-

кість за рахунок виконання додаткового індивідуального завдання. Складання екзамену не є обов'язковим. Студент, який отримав за всі контрольні заходи протягом семестру не менше 60 балів вважається таким, що склав екзамен.

Форми контролю результатів навчальної діяльності студентів та їх оцінювання

Критерії оцінювання лабораторної роботи

Виконання лабораторних робіт	Критерії оцінювання
5	Робота виконана у встановлений термін. Виконана самостійно, чітко сформульовані цілі, завдання та гіпотеза досліджень. Застосовувалися коректні методи обробки отриманих результатів. У висновках проведена коректна інтерпретація результатів
4	Робота виконана у встановлений термін. Студент виконує лабораторну роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; в цілому правильно складає звіт та робить висновки.
3	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну роботу згідно з інструкцією, іноді після консультації викладача; описує спостереження; складає звіт, що містить неточності у висновках та помилки.
2	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну згідно з інструкцією; складений звіт містить неточності у висновках та помилки.
1	Робота виконана з порушенням встановлених термінів. Студент виконує лабораторну під керівництвом викладача; складений звіт містить неточності у висновках та помилки.
0	Робота не виконувалася.

Максимальна оцінка студента за лабораторні роботи 40 балів (8 лабораторних робіт по 5 балів).

Форми контролю модульних контрольних тестових робіт та їх оцінювання

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
Бал	50	45	40	35	30	25	20	15	10	5

Максимальна оцінка студента за модульну контрольну роботу 50 балів.

Додаткові (заохочувальні) бали

Дострокове якісне виконання поточних лабораторних робіт	По 1 балу за одну роботу
Виконання додаткових завдань	5 балів
Участь в обговоренні на лекційних заняттях	0,5 балів за одне заняття

Розподіл балів за формами контролю

Форма контролю	Максимальна кількість балів	
	Денна форма	Заочна форма
Виконання лабораторних робіт	8 x 5 балів = 40 балів	8 x 5 балів = 40 балів
Виконання модульної контрольної роботи	50 балів	50 балів
Додаткові бали (за наявності)	Максимальна кількість 10	Максимальна кількість 10
Підсумковий контроль	10	10
Всього	100	100

Підсумковий контроль

Підсумковий контроль складається з письмового виконання 2 завдань.

Письмова відповідь (2 завдання - по 5 балів).

Бал	Критерії оцінювання
5	Здобувач вільно володіє матеріалом, демонструє уміння на рівні свідомого вибору способу дії в нових ситуаціях (нестандартних) ситуаціях, аналізує, класифікує, узагальнює об'єкти, які охоплюються засвоєними поняттями, ілюструє прикладами та обґрунтовує власні відповіді, судження.
4	Здобувач достатньо вільно володіє матеріалом, демонструє уміння на рівні свідомого вибору способу дії в нових ситуаціях (нестандартних) ситуаціях, аналізує, класифікує, узагальнює об'єкти, які охоплюються засвоєними поняттями, ілюструє прикладами власні відповіді, судження.
3	Здобувач здатний повторити за зразком певну операцію, дію; будує відповідь у засвоєній послідовності; виконує навчальні дії за алгоритмом, у разі утруднення звертається по допомогу; здатний частково внести коректні уточнення і зробити виправлення помилок.
2	Здобувач здатний повторити за зразком певну операцію, дію; будує відповідь у засвоєній послідовності; виконує навчальні дії за алгоритмом, у разі утруднення звертається по допомогу; не завжди здатний внести коректні уточнення і зробити виправлення помилок.
1	Здобувач здатний повторити за зразком певну операцію, дію; будує відповідь у засвоєній послідовності; виконує навчальні дії за алгоритмом, у разі утруднення звертається по допомогу; не здатний внести коректні уточнення і зробити виправлення помилок.
0	Здобувач не надає відповіді

8. Критерії оцінювання результатів навчання

		Денна форма		Заочна форма	
		Вид роботи	Бали	Вид роботи	Бали
ЗМ1	T1	Лабораторна робота № 1	5	Лабораторна робота № 1	5
	T2	Лабораторна робота № 2	5	Лабораторна робота № 2	5
	T3	Лабораторна робота № 3	5	Лабораторна робота № 3	5
	T4	Лабораторна робота № 4	5	Лабораторна робота № 4	5
	T5	Лабораторна робота № 5	5	Лабораторна робота № 5	5
	T6	Лабораторна робота № 6	5	Лабораторна робота № 6	5
	T7	Лабораторна робота № 7	5	Лабораторна робота № 7	5
	T8	Лабораторна робота № 8	5	Лабораторна робота № 8	5
	МК	Модульна контрольна робота	50	Модульна контрольна робота	50
Підсумковий контроль		Письмова відповідь	10	Письмова відповідь	10

9. Рекомендовані джерела інформації

Література

1. Дудикевич В.Б., Хорошко В.О., Яремчук Ю. Є. Основи інформаційної безпеки. Навчальний посібник. – Вінниця : ВНТУ, 2018. – 316 с.
2. Єсін В.І., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій. Навчальний посібник. – Харків : ХНУ імені В.Н. Каразіна, 2013. – 632 с.
3. Кавун С.В, Носов В.В., Манжай О.В. Інформаційна безпека. Навчальний посібник. Частина 1. – Харків. Вид. ХНЕУ, 2008.– 351 с.
4. Сенів М.М., Яковина В.С. Безпека програм та даних. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2015. – 256 с.
5. Бобало Ю.Я., Горбатий І.В., Кіселичник М.Д. та ін. Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
6. Устенко І.В. Системи захисту інформації. Навчальний посібник. – Миколаїв: НУК, 2006. – 68 с.

Інформаційні ресурси

7. Устенко І.В. Методичні вказівки до виконання лабораторних робіт з дисципліни «Безпека програм та даних» [Електронний ресурс]. Режим доступу: <https://eir.nuos.edu.ua/handle/123456789/4438>

Розробник:

к.т.н., доцент, доцент кафедри
програмного забезпечення
автоматизованих систем



Пухалевич А.В.