НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»
Декан факультету інформаційних технологій
_____ Олена ГЛАЗУНОВА
«__» _____ 2023 р.

«СХВАЛЕНО»
на засіданні кафедри комп'ютерних наук
Протокол № 12 від «01» 06 2023 р.
Завідувач кафедри
_____ Белла ГОЛУБ

«РОЗГЛЯНУТО»
Гарант ОП_«Комп'ютерні науки»_
Гарант ОП
_____ Олена ГЛАЗУНОВА

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації

спеціальність 122 «Комп'ютерні науки**»**
освітня програма «Комп'ютерні науки**»**
Факультет інформаційних технологій

Розробник: к.т.н., доцент, доцент кафедри комп'ютерних наук , Пархоменко І. І.

Київ – 2023

Опис навчальної дисципліни

Технології захисту інформації

Галузь знань, спеціальність, освітньо-кваліфікаційний рівень	
Освітній ступінь	Бакалавр
Спеціальність	122 «Комп’ютерні науки»
освітня програма	Комп’ютерні науки
Характеристика навчальної дисципліни	
Вид	Вибіркова
Загальна кількість годин	150
Кількість кредитів ECTS	5
Кількість змістових модулів	2
Форма контролю	Іспит
Показники навчальної дисципліни для денної та заочної форм навчання	
	денна форма навчання
Рік підготовки	4
Семестр	7
Лекційні заняття	30 год
Практичні, семінарські заняття	
Лабораторні заняття	60 год
Самостійна робота	60 год
Кількість тижневих годин	
для денної форми навчання:	4 год.

1. Мета та завдання навчальної дисципліни

1.1. Мета викладання дисципліни

Метою викладання дисципліни є ознайомити з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та іншої інформації в комп'ютерних системах.

Головна задача дисципліни – надати основні відомості з принципів побудови систем захисту інформації та методів протидії спробам несанкціонованого доступу до неї з боку сторонніх осіб, привласнення привілей тощо.

1.2. Завдання вивчення навчальної дисципліни

Завданнями вивчення навчальної дисципліни є:

- використання технологій захисту інформаційно-комунікаційних систем;
- забезпечення цілісності, доступності та конфіденційності інформації; - використання принципів функціонування систем захисту.

Вивчення дисципліни «Технології захисту інформації» сприяє формуванню у студентів наступних компетентностей.

Загальні компетентності:

ЗК2. Здатність застосовувати знання у практичних ситуаціях;

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями;

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел;

ЗК11. Здатність приймати обґрунтовані рішення;

ЗК12. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові, предметні) компетентності:

СК12. Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Це забезпечує досягнення програмних результатів навчання ПР1, ПР14.

1.3 Місце навчальної дисципліни в системі професійної підготовки фахівця

Вивчення дисципліни “Технології захисту інформації” базується на знанні таких дисциплін: «Основи програмування та алгоритмічні мові», «Архітектура комп’ютера», «Комп’ютерна схемотехніка», «Методи і засоби комп’ютерних інформаційних технологій», «Технічні засоби передачі інформації», «Комп’ютерні мережі».

1.4 Інтегровані вимоги до знань і умінь з навчальної дисципліни

Після вивчення дисципліни студент повинен *знати:*

- об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;
- принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентифікація користувачів в операційних системах WINDOWS 9x,

WINDOWS 2k (NT) та UNIX, методи хакерів з несанкціонованого проникнення до інформації, привласнення привілей адміністратора тощо;

- методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цим спробам;
- методи побудови захисту окремих програмних продуктів;
- основні прийоми і програмні засоби для аналізу та дизасемблювання програмних продуктів з метою їх подальшого несанкціонованого використання, методи захисту від дизасемблювання. *вміти:*
- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп’ютерної системи з метою перешкоди призначення невиправданих привілей;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.

2. Програма та структура навчальної дисципліни

Модуль №1 «Безпека інформаційних систем»

Тема1 *Актуальність проблеми забезпечення безпеки в інформаційних системах*. Поняття інтелектуальної власності. Важливість захисту програмного забезпечення в сучасних умовах. Основні загрози для КМ. Можливі місця вторгнення в комп'ютерну мережу Література, методичні рекомендації щодо дисципліни.

Тема 2 *Поняття інформаційної безпеки*. Основні складові інформаційної безпеки. Важливість і складність проблеми інформаційної безпеки. Причини існування комп'ютерних злодіїв. Законодавчий, адміністративний і процедурний рівні. Класифікація методів та засобів захисту програмного забезпечення. Програмно-технічні заходи.

Тема 3 *Стандарти та специфікації в галузі інформаційної безпеки*. Оціночні стандарти і технічні специфікації. "Помаранчева книга" як оцінний стандарт. Політика безпеки. Рівень гарантованості. Механізми безпеки. Класи безпеки. Інформаційна безпека розподілених систем. Рекомендації X.800. Стандарт ISO/IEC 15408 "Критерії оцінки безпеки інформаційних технологій".

Тема 4 *Основні програмно-технічні заходи*. Основні поняття програмнотехнічного рівня інформаційної безпеки. Особливості сучасних інформаційних систем, які є важливими з точки зору безпеки. Архітектурна безпека. Сервіси безпеки.

Модуль №2 «Криптографічні основи захисту інформації».

Тема 5. *Основи криптографії та шифрування даних*. Створення системи облікових записів. Ключ. Шифр. Цілі криптозахисту. Стійкість криптосистеми. Маршрутні перестановки. Блокові шифри простої заміни. Симетричні алгоритми.

Тема 6. *Шифрування*. Основні концепції шифрування. Атаки на систему шифрування. Шифрування з секретним ключем. Шифри підстановки. Одноразові блокноти. Шифрування паролів.

Тема 7. *Шифруюча файлова система (Encrypting file system - EFS).* Технологія шифрування. Взаємодія з користувачем. Відновлення даних. Інтерфейси взаємодії з EFS. Інтерфейс командного рядка.

Тема 8. *Теоретичні відомості ЦС.* Асиметричні алгоритми шифрування. Криптографічні операції в ОС Windows. Криптографічні провайдери. Сертифікати. Стандарт ITU X509. Структура сертифіката X509. Відмінності між сертифікатами перший і третій версій.

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1		2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. «**Безпека інформаційних систем**»													
Тема 1. Актуальність проблеми забезпечення безпеки в інформаційних системах		14	2		6		6						
Тема 2. Поняття інформаційної безпеки		20	4		8		8						
Тема 3. Стандарти та специфікації в галузі інформаційної безпеки		20	4		8		8						
Тема 4. Основні програмно-технічні заходи захисту інформації		20	4		8		8						
Модульна контрольна робота №1		2	2										
Разом за змістовим модулем 1		76	16		30		30						
Змістовий модуль 2. «**Криптографічні основи захисту інформації**»													
Тема 1. Основи криптографії та шифрування даних.		14	2		6		6						
Тема 2. Шифрування		18	2		8		8						
Тема 3. Шифруюча файлова система (Encrypting file system - EFS)		20	4		8		8						
Тема 4. Теоретичні відомості ЦС		20	4		8		8						
Модульна контрольна робота №2		2	2										
Разом за змістовим модулем 2		74	14		30		30						
Усього годин за дисципліною		**150**	**30**		**60**		**60**						

3. Теми семінарських занять

4. Теми практичних занять

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження структури та складових BIOS	8
2	Робота з паролями облікових записів Windows	8
3	Парольні зломщики програмних продуктів	8
4	Управління системним реєстром Windows	8
5	Методи симетричного шифрування інформації	8
6	Дослідження атак з допомогою штучно занесених програм класу SpyWare	8
7	Адміністрування захищених систем та мереж на базі ОС Windows	8
8	Центри сертифікації	4
Всього годин		60

6. Самостійна робота студентів

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з вітчизняною та іноземною спеціальною літературою. Самостійна робота є основним засобом оволодіння навчальним матеріалом у вільний від обов'язкових аудиторних навчальних занять час.

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Кінцеві поля	4
2	Послідовності регістрів зсуву	8
3	Теорія Шенона	8
4	Коди Хоффмана	8
5	Криптографія з публічними ключами	8
6	Системи, що засновані на дискретних алгоритмах	8
7	Системи, що засновані на методі RSA	8
8	Системи, що засновані на еліптичних кривих	8
	Разом	60

7. Зразки контрольних питань, тестів для визначення рівня засвоєння знань студентами

1. Інформація як об’єкт захисту.
2. Характеристика загроз безпеці інформації.
3. Основні означення та поняття теорії захисту інформації.
4. Інформаційна безпека комп’ютерів і комп’ютерних систем.
5. Вразливість комп’ютерів і комп’ютерних систем.
6. Генерація ключів.
7. Загрози безпеці інформації в комп’ютерних системах.
8. Канали несанкціонованого отримання інформації в КС
9. Завдання захисту інформації.
10. Проблеми захисту інформації в комп’ютерних системах.
11. Види комп’ютерних злочинів.
12. Причини поширення комп’ютерної злочинності.
13. Поняття і класифікація комп’ютерних вірусів
14. Стратегія та архітектура захисту інформації.
15. Політика безпеки інформації.
16. Види забезпечення безпеки інформації.
17. Засоби захисту інформації в комп’ютерних системах.
18. Методи і системи захисту інформації.
19. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.
20. Особливості захисту інформації в ПК.
21. Загрози інформації в ПК.
22. Захист ПК від несанкціонованого доступу.
23. Основні положення та визначення криптографії.
24. Симетричні, асиметричні та комбіновані криптосистеми.
25. Основні положення та визначення криптографії
26. Тайнопис, криптографія з ключем.
27. Симетричні та асиметричні криптоалгоритми.
28. Канальне, наскрізне та комбіноване шифрування.
29. Абонементне шифрування
30. Зберігання і розподілення ключів
31. Захист інформації на мережевому рівні.
32. Поняття електронного цифрового підпису.
33. Стандарти електронних цифрових підписів.
34. Основні алгоритми електронного цифрового підпису і їх класифікація.

Комплект тестових завдань

1. Захищеність даних та ІС від випадкових або навмисних пошкоджень та несанкціонованих посягань називається

1. національна безпека
2. власна безпека
3. інформаційна безпека
4. інтернет небезпека

2. Які засоби та методи підтримують інформаційну безпеку?

1. програмні засоби
2. правові методи
3. засоби навчання
4. технічні засоби

3. Що може свідчити про приналежність електронного документа певній особі?

1. Електронний підпис
2. Двофакторна авторизація
3. Власний логін облікового запису
4. Надійний пароль

4. Який пароль серед наведених є найнадійнішим?

1. qwertyuiopasdfgh
2. Hello World!
3. 1234567890
4. H#76&4Waя

5. Який метод використовують деякі сайти для захисту пароля облікового запису від зламу?

1. Електронний підпис
2. Багатофакторна авторизація
3. Антивірусні програми
4. Логін облікового запису

6. Які параметри щодо захисту інформації повинна забезпечувати надійна інформаційна система?

1. Доступність
2. Конфіденційність
3. Правдивість
4. Цілісність

7. Забезпечення користувачів системою безперешкодного та своєчасного доступу до інформації або здійснення між ними своєчасного обміну інформацією - це...

1. Конфіденційність інформації
2. Цілісність даних
3. Доступність інформації
4. Важливість інформації

8. Публікація повідомлень і статей провокаційного характеру, що мають на меті розпалювання конфлікту між читачами та/або співрозмовниками, спантеличити та/або викликати негативну зворотну реакцію

1. Ігроманія
2. Соціоманія
3. Тролінг
4. Веб-серфінг

9. До біометричних систем захисту відносять

1. Ідентифікацію за райдужною оболонкою ока
2. Антивірусний захист
3. Захист паролем
4. Ідентифікацію за відбитками пальців

10. Процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою називається

1. Аутентифікація
2. Доступність
3. Ідентифікація
4. Реєстрація

8. Методи навчання

При викладанні дисципліни використовуються наступні методи навчання:

М1. Лекція (проблемна, інтерактивна)

М3. Проблемне навчання – створення проблемної ситуації для зацікавленого і активного сприйняття матеріалу

М4. Проектне навчання(індивідуальне, малі групи, групове)

М5. Онлайн навчання

М7. Практичне навчання – практична робота для використання набутих знань до розв’язування практичних завдань

М8. Дослідницький метод

9. Форми контролю

МК1. Тестування
МК2. Контрольне завдання
МК3. Розрахункова робота
МК4. Методи усного контролю
МК5. Екзамен

10. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 03.03.2021 р. протокол № 7)

Рейтинг студента, бали	**Оцінка національна за результати складання**	
	екзаменів	**заліків**
90-100	Відмінно	Зараховано
74-89	Добре	
60-73	Задовільно	
0-59	Незадовільно	Не зараховано

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $\mathbf{R_{ДИС}}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $\mathbf{R_{НР}}$ (до 70 балів): $\mathbf{R_{ДИС} = R_{НР} + R_{АТ}}$.

11. Навчально-методичне забезпечення

Технології захисту інформації (Електронний навчальний курс) – https://elearn.nubip.edu.ua/enrol/index.php?id=28

12. Рекомендовані джерела інформації

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах/ А. О. Антонюк. – К.: КМ Академія, 2006. – 244 с.

2. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. - К.: Держстандарт України, 1998

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». – К.: Відомості Верховної Ради України, 1994. - N 31. - Ст. 286.

4. Пономаренко В. С. Основи захисту інформації. Навчальний посібник / В. С. Пономаренко, І. В. Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.

5. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Бак, 2003. – 144 с

6. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

7. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії : навч. посібн. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.

8. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с