

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ**

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»

Декан факультету інформаційних технологій

_____ О. Г. Глазунова

«_____» _____ 20__р.

«СХВАЛЕНО»

на засіданні кафедри комп'ютерних наук

Протокол № _____ від «_» _____ 20__р.

Завідувач кафедри

_____ Б. Л. Голуб

”РОЗГЛЯНУТО ”

Гарант ОП «Комп'ютерні науки»

_____ д.пед.н., проф. Глазунова О. Г

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 – 2021

1.

Опис навчальної дисципліни

Технології захисту інформації

Галузь знань, спеціальність, освітньо-кваліфікаційний рівень

Галузь знань	12 Інформаційні технології
Спеціальність	122 “Комп’ютерні науки ”
освітня програма	“Комп’ютерні науки ”
Освітній ступінь	бакалавр

Характеристика навчальної дисципліни

Вид	Вибіркова
Загальна кількість годин	120
Кількість кредитів ECTS	4
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	15 год.
Практичні, семінарські заняття	
Лабораторні заняття	30 год.
Самостійна робота	75 год.
Кількість тижневих годин	
для денної форми навчання:	
аудиторних	3 год.
самостійної роботи студента –	

2. Мета та завдання навчальної дисципліни

2.1. 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 привілеїв тощо.

2.2. 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.

2.3 Місце навчальної дисципліни в системі професійної підготовки фахівця

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

2.4 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 невинуватених 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.

3. Програма 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 програмно-технічного рівня інформаційної безпеки. Особливості сучасних інформаційних систем, які є важливими з точки зору безпеки. Архітектурна безпека. Сервіси безпеки.

Модуль №2 «Криптографічні основи захисту інформації».

Тема1 *Основи криптографії та шифрування даних.* Створення системи облікових записів. Ключ. Шифр. Цілі криптозахисту. Стійкість криптосистеми. Маршрутні перестановки. Блокові шифри простої заміни. Симетричні алгоритми.

Тема 2 *Шифрування.* Основні концепції шифрування. Атаки на систему шифрування. Шифрування з секретним ключем. Шифри підстановки. Одноразові блокноти. Шифрування паролів.

Тема 3 *Шифруюча файлова система (Encrypting file system - EFS).* Технологія шифрування. Взаємодія з користувачем. Відновлення даних. Інтерфейси взаємодії з EFS. Інтерфейс командного рядка.

Тема 4 *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.

4. Програма та 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»													
<i>Тема 1. Актуальність проблеми забезпечення безпеки в інформаційних системах</i>		26	2		4		20	17					17
<i>Тема 2. Поняття інформаційної безпеки</i>		26	2		4		20	19	2				17
<i>Тема 3. Стандарти та специфікації в галузі інформаційної безпеки</i>		26	1		4		21	17					17
<i>Тема 4. Основні програмно-технічні заходи</i>		26	1		4		21	17					17
Модульна контрольна робота №1		2	2										
Разом за змістовим модулем 1		106	8		16		82	70	2				68
Змістовий модуль 2. «Криптографічні основи захисту інформації»													
<i>Тема 1. Основи криптографії та шифрування даних.</i>		26	2		4		20	21	2		2		17
<i>Тема 2. Шифрування</i>		26	1		4		21	19			2		17
<i>Тема 3. Шифруюча файлова система (Encrypting file system - EFS)</i>		26	1		4		21	19			2		17
<i>Тема 4. Теоретичні відомості ЦС</i>		24	1		2		21	21			4		17
Модульна контрольна робота №2		2	2										
Разом за змістовим модулем 2		104	7		14		83	80	2		10		68
Усього годин за дисципліною		120	15		30		75	150	4		10		136

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження структури та складових BIOS	4
2	Робота з паролями облікових записів Windows	4
3	Парольні зломщики програмних продуктів	4
4	Управління системним реєстром Windows	4
5	Методи симетричного шифрування інформації	4
6	Дослідження атак з допомогою штучно занесених програм класу SpyWare	4
7	Адміністрування захищених систем та мереж на базі ОС Windows	4
8	Центри сертифікації	2
Всього годин		30

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.

7. Методи навчання

При викладанні дисципліни використовуються наступні методи навчання:

М1. Лекція (проблемна, інтерактивна)

М2. Лабораторна робота – для використання набутих знань до розв'язування практичних завдань;

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

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

М5. Он-лайн навчання

8. Форми контролю

При викладанні дисципліни передбачені такі форми контролю:

МК1. Тестування

МК2. Контрольне завдання

МК4. Методи усного контролю

МК5. Екзамен

МК7. Звіт

Для студентів денної форми навчання: усне опитування (МК4) та експрес контроль (МК1) на лабораторних заняттях, захист індивідуальних лабораторних завдань (МК7), аудиторні модульні контрольні роботи (МК2).

9. Розподіл балів, які отримують студенти

Поточний контроль				Рейтинг з навчальної роботи $R_{НР}$	Рейтинг з додаткової роботи $R_{ДР}$	Рейтинг штрафний $R_{ШТР}$	Підсумкова атестація (екзамен чи залік)	Загальна кількість балів
Змістовий модуль 1	Змістовий модуль 2	Змістовий модуль 3	Змістовий модуль 4					
0-100	0-100	0-100	0-100	0-70	0-20	0-5	0-30	0-100

Примітки. 1. Відповідно до «Положення про кредитно-модульну систему навчання в НУБіП України», затвердженого ректором університету 03.04.2009 р., рейтинг студента з навчальної роботи $R_{НР}$ стосовно вивчення певної дисципліни визначається за формулою

$$0,7 \cdot (R_{ЗМ}^{(1)} \cdot K_{ЗМ}^{(1)} + \dots + R_{ЗМ}^{(n)} \cdot K_{ЗМ}^{(n)})$$

$$R_{НР} = \frac{\dots}{K_{Дис}} + R_{ДР} - R_{ШТР},$$

де $R_{ЗМ}^{(1)}, \dots, R_{ЗМ}^{(n)}$ – рейтингові оцінки змістових модулів за 100-бальною шкалою;

n – кількість змістових модулів;

$K_{ЗМ}^{(1)}, \dots, K_{ЗМ}^{(n)}$ – кількість кредитів ECTS, передбачених робочим навчальним планом для відповідного змістового модуля;

$K_{Дис} = K_{ЗМ}^{(1)} + \dots + K_{ЗМ}^{(n)}$ – кількість кредитів ECTS, передбачених робочим навчальним планом для дисципліни у поточному семестрі;

$R_{ДР}$ – рейтинг з додаткової роботи;

$R_{ШТР}$ – рейтинг штрафний.

Наведену формулу можна спростити, якщо прийняти $K_{ЗМ}^{(1)} = \dots = K_{ЗМ}^{(n)}$. Тоді вона буде мати вигляд

$$R_{НР} = \frac{0,7 \cdot (R_{ЗМ}^{(1)} + \dots + R_{ЗМ}^{(n)})}{n} + R_{ДР} - R_{ШТР}.$$

Рейтинг з додаткової роботи $R_{ДР}$ додається до $R_{НР}$ і не може перевищувати 20 балів. Він визначається лектором і надається студентам рішенням кафедри за виконання робіт, які не передбачені навчальним планом, але сприяють підвищенню рівня знань студентів з дисципліни.

Рейтинг штрафний R_{штр} не перевищує 5 балів і віднімається від **R_{нр}**. Він визначається лектором і вводиться рішенням кафедри для студентів, які матеріал змістового модуля засвоїли невчасно, не дотримувалися графіка роботи, пропускали заняття тощо.

2. Згідно із зазначеним Положенням **підготовка і захист курсового проекту (роботи)** оцінюється за 100 бальною шкалою і далі переводиться в оцінки за національною шкалою та шкалою ECTS.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

10 Рекомендована література

Основна література:

1. АНИН Б.Ю. Защита компьютерной информации. – СПб.: ВНУ, 2000. – 384 с.
2. БУРДАЕВ О.В., ИВАНОВ М.А., ТЕТЕРИН И.И. Ассемблер в задачах защиты информации. - М.: КУДИЦ-ОБРАЗ, 2002. -318 с.
3. МАК-КЛАР С., СКЕМБРЕЙ Д., КУРЦ Д. Секреты хакеров. Безопасность сетей - готовые решения. - М.: Вильямс, 2002. - 730 с.
4. КАСПЕРСКИ К. Фундаментальные основы хакерства. Искусство дизассемблирования. - М.: Солон, 2002. - 443 с.

5. КАСПЕРСКИ К. Техника и философия хакерских атак. – М.: Солон, 2001. - 272

Додаткова література.

1. ЯРОЧКИН В.И. Безопасность информационных систем. – М.: Ось-89, 1996. - 320 с. ГРУШО А., ТИМОНИНА Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. - 188 с.
2. МЕЛЬНИКОВ В. Защита информации в компьютерных системах. – М.: Финансы и Статистика, 1997 г., 368 стр.
3. ЗЕГЖДА П. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996. - 300 с.
4. МАГАУЕНОВ Р. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. – М.: ИД Мир безопасности, 1997. - 112 с.
5. ГАЙКОВИЧ В.Ю., ЕРШОВ Д.В. Основы безопасности информационных технологий. – М.: МИФИ, 1995. - 96 с.
6. УХЛИНОВ Л.М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1996. - 112 с.
7. КУРИЛО А.П., УХЛИНОВ Л.М. Проектирование систем контроля доступа к ресурсам сетей ЭВМ. – М.: МИФИ, 1996. - 128 с.
8. БАРИЧЕВ С.Г., ГОНЧАРОВ В.В., СЕРОВ Р.Е. Основы современной криптографии: Учебный курс для вузов Изд. 2-е, перераб., доп. – М.: Озон, 2002.
9. ТОРРЕС Скрипты для администратора Windows. Спец. справочник – СПб.: Питер, 2002.
10. ДОМАШЕВ А. В., ГРУНТОВИЧ М. М. и др. Программирование алгоритмов защиты информации – М.: Нолидж, 2002.
11. ЗАВГОРОДНИЙ В. И. Комплексная защита информации в компьютерных системах: Уч. пос. – М.: Логос. 2001.
12. ИВАНОВ М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц-образ, 2001.

13. БРАГГ Р. Система безопасности Windows 2000. – СПб.: Вильямс, 2001.
14. СКЕМБРЕЙ Д., МАК-КЛАР С. Секреты хакеров. Безопасность Windows 2000 - готовые решения. – СПб.: Вильямс, 2002.
15. Безопасность сети на основе Microsoft Windows 2000. Учебный курс MCSE. – М.: Русская Редакция, 2001.
16. МЕДВЕДОВСКИЙ И. Д., СЕМЬЯНОВ Б. В. И др. Атака из Internet – М.: Солон, 2002.
17. НОРТКАТТ С., НОВАК Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу. – М.: Лори, 2001.
18. СТОЛЛИГС В. Основы защиты сетей. Приложения и стандарты. – СПб.: Вильямс, 2002.
19. ТОЛСТОЙ А.И. Интрасети: обнаружение вторжений. – М.: Юнити-Дана. 2001.
20. ШРЕЙН Д. Антихакинг. – М.: Майор, 2002.
21. КОУЛ Э. Руководство по защите от хакеров. – СПб.: Вильямс, 2002.
22. СКУДИС Э. Противостояние хакерам. Пошаговое руководство. – М.: ДМК Пресс, 2003.
23. ШИФФМАН М. Защита от хакеров. Анализ 20 сценариев взлома. СПб.: Вильямс, 2002.