Національний університет біоресурсів і природокористування України

Кафедра комп'ютерних наук

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації

Спеціальність – 122 «Комп'ютерні науки та інформаційні технології»

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

Київ – 2019

1. Опис навчальної дисципліни

Технології захисту інформації

Галузь знань, спеціальність, освітньо-кваліфікаційний рівень	
Галузь знань	12 Інформаційні технології
Спеціальність	122 “Комп’ютерні науки та інформаційні технології”
Освітній ступінь	бакалавр
Характеристика навчальної дисципліни	
Вид	вибіркова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	
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 самостійної роботи студента −	3 год.

2. Мета та завдання навчальної дисципліни

Основна мета дисципліни – 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.

Вивчення дисципліни “Захист 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»

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.

Після вивчення дисципліни ***студент повинен 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.

Міждисциплінарні зв'язки навчальної дисципліни

Вивчення дисципліни "Захист 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»

3. Програма навчальної дисципліни

Модуль №1 „Захист програмного забезпечення шляхом блокування доступу до комп'ютера."

Тема1 Поняття інтелектуальної власності. Важливість захисту програмного забезпечення в сучасних умовах. Література, методичні рекомендації щодо дисципліни.

Тема 2 Причини існування комп'ютерних злодіїв. Методи проникнення до інформації у комп'ютері (хакінґ, крекінг, фрікінг). Класифікація методів та засобів захисту програмного забезпечення. Апаратні, програмні та програмно-апаратні засоби захисту інформації. Носії ключової інформації (дискети, електронні ключі, SMART-карти, пристрої Touch-Memory). Прив'язка програмного забезпечення до унікальних характеристик комп'ютерної системи та BIOS.

Тема 3 Основні складові програми BIOS. Принципи хешірования та зберігання паролів доступу. Інженерний пароль, старий та новий формат паролю, місце зберігання інженерного паролю в BIOS. Програмний пароль, місце знаходження програмних паролів (SUPERVISOR та USER) в CMOS-пам'яті.

Тема 4 Засоби аналізу парольного хеша. Методи зняття, взлому та підбору паролю. Програмні засоби хакерів для зняття та взлому паролю BIOS. Рекомендації щодо унеможливлення несанкціонованого доступу до комп'ютеру.

Модуль №2 „Захист основних операційних систем (ОС)”.

Тема1 Побудова захисту ОС WINDOWS 2k (NT). Файлова система NTFS, її роль у захисті інформації. Принципи адміністрування у ОС WINDOWS 2k. Створення системи облікових записів.

Тема 2 Особливості функціонування ОС *NIX. Система доступу та реєстрації користувачів у ОС UNIX та LINUX. Базові консольні команди *NIX та система каталогів

Тема 3 Класифікація засобів, що використовують при зломі програм. Методи аналізу програм із допомогою HEX-редакторів, дизасемблерів та відладчиків. Послідовність дій при зломі програмного продукту. Виготовлення CRACK-файлів.

Тема 4 Прийоми захисту програм шляхом динамічного генерування програмного коду. Ускладнення дизасемблювання програм шляхом використання самомодіфікуючогося коду Методи виявлення роботи програми під відладчиком

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. „Захист програмного забезпечення”													
Тема 1. Складові «Інформаційної безпеки»		17	2		4		9						
Тема 2. Огляд методів та засобів захисту інформації.		17	2		4		9						
Тема 3. Система захисту комп'ютера з допомогою BIOS		14	1		4		9						
Тема 4. Методи захисту програмних продуктів		15	1		4		10						
Модульна контрольна робота №1		2	2										
Разом за змістовим модулем 1		61	8		16		37						
Змістовий модуль 2. Захист основних операційних систем (ОС)”.													
Тема 1. Побудова системи безпеки ОС WINDOWS 2k.		15	2		4		9						
Тема 2. Побудова системи безпеки ОС UNIX		14	1		4		9						
Тема 3. Методи протидії штучно занесеним руйнівним комп'ютерним програмам		15	1		4		10						
Тема 4. Програмні засоби підвищення рівня захисту		13	1		2		10						

комп'ютерної системи													
Модульна контрольна робота №2		2	2										
Разом за змістовим модулем 2		59	7		14		38						
Усього годин за дисципліною		120	15		30		75						

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Огляд складових інформаційної безпеки	4
2	Огляд методів та засобів захисту інформації.	4
3	Дослідження системи захисту комп'ютера з допомогою BIOS	4
4	Структура PE-файлів	4
5	Дослідження захисту операційної системи WINDOWS 2k.	4
6	Адміністрування безпеки операційної системи WINDOWS 2k.	4
7	Дослідження атак з допомогою штучно занесених програм класу SpyWare.	4
8	Мереживі сканери та екрани	2
Всього		30

6. Методи навчання

Форми навчання – лекції, та практичні заняття.

7. Форми контролю

ІСПИТ

8. 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

$$R_{НР} = \frac{0{,}7 \cdot (R^{(1)}_{ЗМ} \cdot К^{(1)}_{ЗМ} + ... + R^{(n)}_{ЗМ} \cdot К^{(n)}_{ЗМ})}{К_{ДИС}} + R_{ДР} - R_{ШТР},$$

де $R^{(1)}_{ЗМ}, \dots R^{(n)}_{ЗМ}$ − рейтингові оцінки змістових модулів за 100-бальною шкалою; **n** − кількість змістових модулів;

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

$К_{ДИС} = К^{(1)}_{ЗМ} + \dots + К^{(n)}_{ЗМ}$ − 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 $К^{(1)}_{ЗМ} = \dots = К^{(n)}_{ЗМ}$. Тоді вона буде мати вигляд

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

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.

Оцінка національна	Рейтинг здобувача вищої освіти, бали
Відмінно	90-100
Добре	74-89
Задовільно	60-73
Незадовільно	0-59

14. Рекомендована література

Основна література.

1. АНИН Б.Ю. Защита компьютерной информации. – СПб.: BHV, 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.

2. ГРУШО А., ТИМОНИНА Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. - 188 с.
3. МЕЛЬНИКОВ В. Защита информации в компьютерных системах. – М.: Финансы и Статистика, 1997 г., 368 стр.
4. ЗЕГЖДА П. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996. - 300 с.
5. МАГАУЕНОВ Р. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. – М.: ИД Мир безопасности, 1997. - 112 с.
6. ГАЙКОВИЧ В.Ю., ЕРШОВ Д.В. Основы безопасности информационных технологий. – М.: МИФИ, 1995. - 96 с.
7. УХЛИНОВ Л.М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1996. - 112 с.
8. КУРИЛО А.П., УХЛИНОВ Л.М. Проектирование систем контроля доступа к ресурсам сетей ЭВМ. – М.: МИФИ, 1996. - 128 с.
9. БАРИЧЕВ С.Г., ГОНЧАРОВ В.В., СЕРОВ Р.Е. Основы современной криптографии: Учебный курс для вузов Изд. 2-е, перераб., доп. – М.: Озон, 2002.
10. ТОРРЕС Скрипты для администратора Windows. Спец.справочник – СПб.: Питер, 2002.
11. ДОМАШЕВ А. В., ГРУНТОВИЧ М. М. и др. Программирование алгоритмов защиты информации – М.: Нолидж, 2002.
12. ЗАВГОРОДНИЙ В. И. Комплексная защита информации в компьютерных системах: Уч. пос. – М.: Логос. 2001.
13. ИВАНОВ М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц-образ, 2001.
14. БРАГГ Р. Система безопасности Windows 2000. – СПб.: Вильямс, 2001.
15. СКЕМБРЕЙ Д., МАК-КЛАР С. Секреты хакеров. Безопасность Windows 2000 - готовые решения. – СПб.: Вильямс, 2002.
16. Безопасность сети на основе Microsoft Windows 2000. Учебный курс MCSE. – М.: Русская Редакция, 2001.

17. МЕДВЕДОВСКИЙ И. Д., СЕМЬЯНОВ Б. В. И др. Атака из Internet – М.: Солон, 2002.
18. НОРТКАТТ С., НОВАК Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу. – М.: Лори, 2001.
19. СТОЛЛИГС В. Основы защиты сетей. Приложения и стандарты. – СПб.: Вильямс, 2002.
20. ТОЛСТОЙ А.И. Интрасети: обнаружение вторжений. – М.: Юнити-Дана. 2001.
21. ШРЕЙН Д. Антихакинг. – М.: Майор, 2002.
22. КОУЛ Э. Руководство по защите от хакеров. – СПб.: Вильямс, 2002.
23. СКУДИС Э. Противостояние хакерам. Пошаговое руководство. – М.: ДМК Пресс, 2003.
24. ШИФФМАН М. Защита от хакеров. Анализ 20 сценариев взлома. СПб.: Вильямс, 2002.