ПВНЗ УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА
Кафедра інформаційних технологій та програмної інженерії

Робоча програма навчальної дисципліни

Засоби захисту інформації

ОБОВ'ЯЗКОВА ДИСЦИПЛІНА

Освітньо-професійна програма «Інженерія програмного забезпечення» підготовки здобувачів другого (магістерського) рівня вищої освіти – спеціальності 121 Інженерія програмного забезпечення

Розробник:
Стисло Т.Р. викладач кафедри інформаційних технологій та програмної інженерії кандидат технічних наук.

Робоча програма затверджена на засіданні кафедри інформаційних технологій та програмної інженерії факультету інформаційних технологій 29 серпня 2018 року (протокол № 1).

Завідувач кафедри
доктор технічних наук, доцент
_____С.І. Мельничук
29.серпня 2018 р.

ВСТУП

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

Навчання проводиться у формі лекцій та практичних занять із використанням комп'ютера. Освоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень вивчення і аналізу фахових дисциплін за рахунок ефективного використання сучасних технологій програмної інженерії.

Для досягнення мети поставлені такі основні **завдання**:

- принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх взлому;
- методи несанкціонованого зйому та навмисного пошкодження інформації та засоби протидії цiїм спробам;
- методи побудови захисту окремих програмних продуктів.

До задач вивчення дисципліни входить формування теоретичних знань та практичних навичок у відповідності з поставленою метою.

Результати навчання. Згідно з вимогами освітньо-професійних та освітньо-кваліфікаційних програм студенти повинні **знати:**

- об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентіфікація користувачів в операційних системах WINDOWS 9x, WINDOWS 2k (NT) та UNIX, методи хакерів з несанкціонованого проникнення до інформації, привласнення привілей адміністратора тощо;

Вміти:

- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи
- несанкціонованого доступу;
- здійснити організаційни та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до компьютерной системи з метою перешкоди призначення невиправданих привілей;
- виконувати постійний моніторінг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби хакерів для перевірки надійності зіхисту інформації та стійкості його щодо хакерських атак.

Пререквізити: вивчення даної навчальної дисципліни студент розпочинає, прослухавши такі навчальні дисципліни як:

- якість програмного забезпечення та тестування;
- інженерія програмного забезпечення;
- захист програмних продуктів.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Освітньо-професійна програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ESTS – 5</td><td rowspan="9">121 Інженерія програмного забезпечення, магістр</td><td colspan="2">Обов’язкова (базова)</td></tr>
<tr><td rowspan="2">Кількість модулів – 2</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>1-й</td><td>-</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td colspan="2" rowspan="2">Лекції</td></tr>
<tr><td rowspan="6">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи – 6</td></tr>
<tr><td>28 год.</td><td>- год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>26 год.</td><td>- год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>66 год.</td><td>- год.</td></tr>
<tr><td colspan="2">Вид контролю: екзамен 30 год.</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної роботи становить:
для денної форми навчання – 1/2,5
для заочної форми навчання – 1/8.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Поточне оцінювання студентів на семінарських заняттях здійснюється за чотирьох бальною шкалою, де «2» - незадовільно; «3» - задовільно; «4» - добре; «5» - відмінно.

Підсумковий контроль у вигляді екзамену проводиться у тестовій формі і оцінюється відповідно до шкали оцінювання знань студентів за ЄКТС

Шкала в балах	Національна шкала	Шкала ЄКТС
90-100 балів	5 «відмінно»	A
80-89 балів	4 «дуже добре»	B
65-79 балів	4 «добре»	C
55-64 бали	3 «задовільно»	D
50-54 бали	3 «достатньо»	E
35-49 балів	2 «незадовільно»	FX
1-34 бали	2 «неприйнятно»	F

МЕТОДИ НАВЧАННЯ ТА ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

За призначенням і характером контроль поділяють на попередній, поточний, періодичний, підсумковий, взаємоконтроль, самоконтроль.

Попередній контроль проводять, щоб визначити рівень підготовленості студентів на початку нового навчального року чи періоду. Результати цього контролю суттєво впливають на з'ясування початкової ситуації для подальшої організації навчального процесу у вищому навчальному закладі, конкретизування, оптимізації та більш цілеспрямованого визначення його змістового компонента, обґрунтування послідовності опрацювання розділів і частин навчальних предметів, визначення основних методів, форм і засобів його проведення та ін.

Поточний контроль застосовують для перевірки і окремих студентів, і академічних груп, як правило, у повсякденній навчальній діяльності, насамперед, на планових заняттях. Педагог систематично спостерігає за навчальною роботою студентів, перевіряє рівень опанування програмного матеріалу, формування практичних навичок та вмінь, їхньої міцності, а також виставляє відповідні оцінки за усні відповіді, контрольні роботи, практичне виконання певних нормативів, передбачених збірниками нормативів і програмою навчальних дисциплін.

Періодичний контроль має системний, плановий і цілеспрямований характер. Він полягає у визначенні рівня та обсягу оволодіння знаннями, навичками і вміннями наприкінці тижня, місяця, кварталу, півріччя, навчального року. Цей контроль здійснюють і у процесі планових занять (навчань), і в спеціально відведений резервний час.

Підсумковий контроль спрямовано на визначення рівня реалізації завдань, сформульованих у навчальних програмах, планах підготовки та в інших документах, які регламентують навчально-виховний процес. Він охоплює і теоретичну, і практичну підготовку студентів, проводять його, як правило,

наприкінці зимового й літнього періодів навчання, під час спеціальних заходів перевірки.

У процесі викладання навчальної дисципліни для активізації навчально-пізнавальної діяльності студентів передбачене застосування як активних, так і інтерактивних навчальних технологій, серед яких: лекції проблемного характеру, робота в малих групах, презентації, дослідницький метод, частинно-пошуковий (евристичний) метод.

Діагностика (моніторинг і перевірка) результатів навчання здійснюється шляхом виконання студентами:

1) практичних робіт;
2) підсумкового екзамену у тестовій формі.

Перелік тестових питань та варіантів відповідей можна переглянути на сайті – [Електронний ресурс] режим доступу: https://drive.google.com/file/d/1VAywEp9zVo9N9lkK8oSsdJG0g_ysGmyk/view

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль І. Захист програмного забезпечення шляхом блокування доступу до комп'ютера

Тема1. Складові "Інформаційної безпеки".

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

Тема 2. Огляд метолів та засобів захисту інформації.

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. Система захисту компютера з допомогою BIOS.

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. Методи захисту програмних продуктів.

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.

Змістовий модуль ІІ . Захист основних операційних систем (ОС)

Тема5. Побудова системи безпеки ОС WINDOWS 2k.

Файлова система NTFS, її роль у захисті інформації. Принципи адміністрування у ОС WINDOWS 2k. Створення системи облікових записів.

Тема 6. Побудова системи безпеки ОС UNIX.

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

Тема 7. Методи протидії штучно занесеним руйнівним комп'ютерним програмам.

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 8. Програмні засоби підвищення рівня захисту.

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

ТЕМАТИЧНИЙ ПЛАН

Назви розділів і тем	Кількість годин									
	денна форма					заочна форма				
	Всього	у тому числі				Всього	у тому числі			
		л	п	с	с.р.		л	п	с	с.р.
1	2	3	4	5	6	7	8	9	10	11
Змістовий модуль І. Захист програмного забезаечення										
Тема 1.Складові "Інформаційної безпеки"	12	2	2		6					
Тема 2. Огляд метолів та засобів захисту інформації.	14	4	4		8					
Тема 3. Система захисту компютера з допомогою BIOS.	14	4	4		8					
Тема 4. Методи захисту програмних продуктів.	14	4	4		8					
Разом за змістовим модулем 1	**54**	**14**	**14**		**30**					
Змістовий модуль ІІ. Захист основних операційних систем										
Тема 5. Побудова системи безпеки ОС	12	4	2		8					

WINDOWS 2k.										
Тема 6. Побудова системи безпеки ОС UNIX.	18	4	4		8					
Тема 7. Методи протидії штучно занесеним руйнівним комп'ютерним програмам.	18	4	4		10					
Тема 8. Програмні засоби підвищення рівня захисту.	18	2	2		10					
Разом за змістовим модулем 2	**66**	**14**	**12**		**36**					
Підсумковий контроль	**30**									
Усього годин	**150**	**28**	**26**		**66**					

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1.	Огляд складових інформаційної безпеки	2
2.	Огляд метолів та засобів захисту інформації	2
3.	Дослідження системи захисту комп'ютера з допомогою BIOS	2
4.	Дослідження захисту операційної системи WINWOWS 2k	4
5.	Адміністрування безпеки операційної системи WINDOWS 2k	4
6.	Дослідження атак з допомогою штучно занесених програм класу SpyWare	4
7.	Мережеві сканери та екрани	4
8.	Структура PE-файлів	4
	Разом:	**26**

САМОСТІЙНА РОБОТА

Питання на самостійне опрацювання:

Необхідним елементом успішного засвоєння навчального матеріалу дисципліни є самостійна робота студентів з вітчизняною та закордонною спеціальною літературою з вивчення й використання сучасних мобільних технологій при вирішенні економічних задач. Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Самостійна робота студентів передбачає поглиблене вивчення тем з використанням рекомендованої літератури, пошук інформації в Інтернеті, а також додаткову роботу в комп'ютерних класах для виконання індивідуальних завдань (доповідей).

Основні види самостійної роботи, які запропоновані студентам:

1. Вивчення лекційного матеріалу.
2. Робота з вивчення рекомендованої літератури.
3. Вивчення термінів і основних понять з тем навчальної дисципліни.
4. Підготовка до лабораторних занять і розробка ескізів документів з кожної лабораторної роботи.
5. Контрольна перевірка кожним студентом знань за питаннями для самодіагностики.

6. Підготовка доповіді для виступу на лабораторному занятті.

7. Підготовка до тестового контролю.

8. Підготовка до виконання контрольних робіт з модулів навчальної дисципліни.

9. Робота з опрацювання та вивчення рекомендованої літератури.

10. Систематизація вивченого матеріалу.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

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:

6. МЕЛЬНИКОВ В. Защита информации в компьютерных системах. – М.: Финансы и Статистика, 1997 г., 368 стр.
7. ЗЕГЖДА П. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996. - 300 с.
8. МАГАУЕНОВ Р. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации. – М.: ИД Мир безопасности, 1997. - 112 с.
9. ГАЙКОВИЧ В.Ю., ЕРШОВ Д.В. Основы безопасности информационных технологий. – М.: МИФИ, 1995. - 96 с.
10. УХЛИНОВ Л.М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1996. - 112 с.
11. КУРИЛО А.П., УХЛИНОВ Л.М. Проектирование систем контроля доступа к ресурсам сетей ЭВМ. – М.: МИФИ, 1996. - 128 с.
12. БАРИЧЕВ С.Г., ГОНЧАРОВ В.В., СЕРОВ Р.Е. Основы современной криптографии: Учебный курс для вузов Изд. 2-е, перераб., доп. – М.: Озон, 2002.
13. ТОРРЕС Скрипты для администратора Windows. Спец.справочник – СПб.:Питер, 2002.