1. Міністерство освіти і науки України
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Програмний захист інформації

Методичні вказівки
до виконання розрахунково-графічних робіт
для студентів напряму підготовки (спеціальність)
6.170103 "Управління інформаційною безпекою",
125 «Кібербезпека»

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного моделювання
Протокол № _8__
від «19 » 02 2019 р.

Чернігів ЧНТУ 2019

Програмний захист інформації. Методичні вказівки до виконання розрахунково-графічної роботи для студентів напряму підготовки (спеціальність) 6.170103 "Управління інформаційною безпекою", 125 «Кібербезпека» / Укл.: Усов Я.Ю. – Чернігів: ЧНТУ, 2018. – 14с.

Укладачі: Усов Ярослав Юрійович, викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск: Ткач Юлія Миколаївна,

завідувач кафедри кібербезпеки та математичного моделювання,

доктор педагогічних наук, доцент

Рецензент: Ткач Юлія Миколаївна, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, доцент

ЗМІСТ

ПЕРЕДМОВА

Метою викладання дисципліни є надання основних відомостей про принципи та методи розробки і використання програмних та програмно-апаратних засобів для захисту інформації в інформаційно-телекомунікаційних системах (ІТС).

Завданнями вивчення навчальної дисципліни є:

- засвоєння основних відомостей з принципів побудови та функціонування руйнівних програмних засобів, за допомогою яких здійснюється несанкціонований доступ до програмного забезпечення;
- оволодіння принципами побудови та способами застосування основних програмних та програмно-апаратних засобів захисту програмного забезпечення та іншої інформації в комп'ютерних системах в практичній діяльності;
- оволодіння методами комплексного підходу з метою використання відповідного програмного забезпечення в системах захисту інформації.

Запропоновані завдання для індивідуальної (розрахунково-графічної) роботи студентів включають методичні вказівки до виконання, завдання для розрахунку, критерії оцінювання. За допомогою розрахунково-графічної роботи та запропонованих завдань досягається більш глибоке опанування теорії, що здійснюється за допомогою розвитку логічного мислення через вирішення задач та дає змогу студентам осмислити нові для них поняття. Завдання для розрахунку скомпоновані відповідно до розділів робочої програми «Програмний захист інформації», 7 семестр навчання, що полегшує і робить більш зручною організацію навчального процесу і викладачам, і студентам.

Завдання для розрахунково-графічної роботи студентів можуть використовуватися як для аудиторної, так і домашньої роботи. Вони спрямовані на розвиток у студентів організаційних та аналітичних здібностей, а також уміння користуватися теоретичними посиланнями у вирішенні практичних ситуацій та вміння користуватися статистикою і спеціальною літературою.

Завдання для розрахунково-графічної роботи студентів можуть значною мірою полегшити вивчення дисципліни студентами очної форми навчання.

Під час виконання розрахунково-графічної роботи студенти повинні ознайомитися та вивчити лекційний матеріал, запропонований викладачем. Основою для вивчення є літературні джерела, наведені в даній методичній розробці. За наявності незрозумілих питань студентам рекомендується звернутись за консультаціями до викладача з метою отримання всіх необхідних пояснень щодо організації розрахунково-графічної роботи, виконання розрахункових завдань та пошуку додаткових літературних джерел. Викладачем надаються додаткові роз'яснення та індивідуальні консультації для підвищення компетентності студентів та розширення спектру їх знань з даної дисципліни.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин для денної форми навчання					
	денна форма					
	усього	у тому числі				
		л	пр	лаб	інд	с.р.
Модуль 1						
Змістовий модуль 1.						
1. Загальний огляд систем захисту програмного забезпечення.	69	8		6		55
2. Сучасний стан засобів подолання систем захисту.	52	6		6		40
3. Захист від несанкціонованого копіювання	32	6		6		20
4. Основні поняття ос, необхідні для створення систем захисту програмного забезпечення.	25	4		6		15
Модульна контрольна робота №1	12			2		
Разом за змістовим модулем 1	180	24		26		130
Усього годин за дисципліну	180	24		26		130

КРИТЕРІЇ ОЦІНЮВАННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Розрахунково-графічні завдання виконуються за окремим графіком. Студент самостійно готується до такого заняття за індивідуальним завданням. Обсяг розрахунково-графічної роботи визначається навчальним планом з дисципліни.

З даного курсу розрахунково-графічної робота проводиться у формі виконання індивідуальних завдань з розв'язування різноманітних задач.

Шкала оцінювання знань студентів при виконанні розрахунково-графічної роботи

Рівень виконання розрахункової роботи	**Кількість балів**	
- завдання розв'язані повністю і правильно, містять пояснення до розрахунків; - здійснено посилання на нормативну базу; - показано вміння самостійно формулювати висновки за результатами проведеного дослідження; - присутній творчий підхід та використано новітні інформаційні технології.	9…	10
- завдання виконані повністю, але при розв'язуванні допущені незначні помилки; - не аргументовано викладено матеріал; - у висновках містяться помилки та недоречності	6…	8
- завдання розв'язані, але містять грубі помилки; - завдання розв'язані не у повному обсязі та допущено значні помилки; - не сформульовані висновки за результатами розрахунків	3…	5
- завдання виконані частково і неякісно; - записані тільки формули	0…	2

У зв'язку з тим що, розрахунково-графічна робота містить завдання для розрахунку з різних тем, і може бути виконана після вивчення всіх тем курсу, оцінюється вона після закінчення другого модуля і оцінка за виконання розрахунково-графічної роботи, додається до підсумкової модульної оцінки, переведеної за шкалою ECTS.

ВИМОГИ ДО ОФОРМЛЕННЯ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

Робота оформляється на листах А4 з однієї сторони, поля: з лівого боку – 20 мм, з правого боку – 10 мм, зверху – 20 мм, знизу – 20 мм. Завдання повинні бути виконані акуратно, розбірливим почерком (або надруковані), з детальними поясненнями та всіма проміжними розрахунками. В кінці розрахункового завдання пишеться висновок (відповідь).

Вимоги до комп'ютерного набору розрахункової роботи:

– текстовий редактор – WORD;

– гарнітура шрифту – Times New Roman;

– кегль шрифту (розмір) – 14;

– міжрядковий інтервал – полуторний;

– абзац – 1,25 см;

– розташування тексту роботи – вирівнювання по ширині;

– міжрядковий інтервал між заголовком (назвою розділу чи підрозділу) і текстом повинна дорівнювати 1 інтервалу.

Приклад оформлення титульної сторінки розрахунково-графічної роботи наведено у Додатку А.

Повністю оформлена і виконана розрахункова робота подається на кафедру в термін, що визначений у плані-графіку виконання розрахункової роботи для перевірки її викладачем. Якщо робота виконана не вчасно без поважних причин, то студенту ставиться 0 балів («незадовільно») і він повинен виконати додатково один з варіантів, який вкаже викладач. Розрахункова робота оцінюється після особистої співбесіди з викладачем. В разі зауважень з боку викладача, робота повинна бути доопрацьована в зазначений термін і подана на перевірку. До підсумкового контролю допускаються лише студенти, що вчасно здали і захистили свою роботу.

Варіант розрахунково-графічної роботи видається студенту викладачем (згідно порядкового номеру в списку академічної групи або в інший спосіб).

Варіант: 1

1. Навести загальний порядок здійснення зламу захисту.
2. Охарактеризувати програми-монітори звернень до файлів. Їх призначення.
3. Дати характеристику програмам стеження за системним реєстром. Їх використання дл аналізу систем захисту.

Варіант: 2

1. Дати характеристику програмам для моніторингу процесів і вікон.
2. Охарактеризувати програми-монітори API-викликів. Де і як їх можна застосувати?
3. Охарактеризувати особливості використання програм сканування портів, програм моніторингу мережевого обміну.

Варіант: 3

1. Для чого можуть бути використані вказані програми при покращенні роботи операційних систем?
2. Як можуть бути використані програми моніторингу при дослідженні роботи систем захисту програмного забезпечення?
3. В чому різниця між архіваторами та пакувальниками?.

Варіант: 4

1. Який принцип діії програм-пакувальників?
2. Які позитивні і негативні риси пакувальників?
3. Назвіть декілька програ для пакування виконуваних файлів.

Варіант: 5

1. Наведіть приклади програм для ідентифікації пакування файлів. Яке їх призначення?
2. Яке програмне забезпечення виконує злам програмних продуктів, захищених пакувальниками?
3. Назвіть основні методи, що їх використовують розпакувальники.

Варіант: 6

1. Навести характеристику сучасних технологій захисту програмного за безпечення від копіювання.
2. Охарактеризувати рівні роботи з дисковою системою комп’ютерів.
3. Навести перелік методів захисту від НСК шляхом прив’язки до дистрибутивного носія.

Варіант: 7

1. Що означає поняття нестандартного форматування і яким чином воно використовується для захисту від НСК? Навести приклади.
2. Що означає метод, що базується на опитуванні довідника? Що таке електронні ключі, які типи елекронних ключів?
3. Що таке ключі ідентифікації, який принцип захисту вон використовують і чим відрізняються від електронних ключів?

Варіант: 8

1. Знайти в інтернеті програмні продукти, використовувані для захисту від копіювання. Навести їх можливості, способи захисту, використовувані методи.
2. Розкажіть про методи захисту програм, які базуються на прив'язках.
3. Вкажіть методи доступу до файлової системи комп'ютера.

Варіант: 9

1. Наведіть засоби для отримання довідкової інформації про дискову систему.
2. Охарактеризуйте засоби для роботи з каталогами файлової системи.
3. Дайте характеристику засобам для пошуку інформації у каталогах. Як це можна використати для побудови системи захисту?

Варіант: 10

1. Програмні засоби для роботи з файлами (записування, зчитування, позиціювання тощо).
2. Засоби для доступу до дескрипторів файлів і можливість їх зміни.

реєстр, яке його призначення, його структура?

3. Охарактеризувати методи прив'язки до вінчестера як захист від несанкціонованого копіювання.

Варіант: 11

1. Способи визначення параметрів системи. Дати коротку харак-теристику кожному з них.
2. Вимірювання продуктивності апаратури комп'ютера як метод захисту. Охарактеризуйте його.
3. Які програмні засоби для отримання логічних параметрів комп'ютера ви знаєте?

Варіант: 12

1. Якими способами можна отримати інформацію про дискову систему комп'ютера?
2. Яким чином можна встановити, отримати та модифікувати атрибути файлів?
3. Як заблокувати (розблокувати) доступ до файлів?

Варіант: 13

1. Як можна отримати значення фізичних параметрів комп'ютера?
2. З чого складаються ключі реєстру?
3. Для чого використовують реєстр операційної системи в задачах захисту програмного забезпечення?

Варіант: 14

1. Які основні програмні функції для роботи з реєстром ви можете навести?
2. Які програмно-апаратні методи захисту ви знаєте? Яким чином здійснюється такий захист?
3. Для чого використовують електронні ключі захисту?

Варіант: 15

1. Для чого використовуються ключі ідентифікації? Який принцип їх роботи?
2. В чому полягає захист за допомогою довідників?
3. Яким чином можна здійснити прив'язку до кількості запусків програмного забезпечення?

Варіант: 16

1. Як можна прив'язатися до часу дії програми?
2. Охарактеризуйте структуру виконуваних файлів
3. Що таке заголовки виконуваних файлів, які їх види є?

Варіант: 17

1. Для чого операційна система використовує заголовки?
2. Що таке таблиця об'єктів (розділів виконуваного файлу)?
3. Які об'єкти (розділи) існують у програмах від різних виробників?

Варіант: 18

1. Які способи впровадження захисних механізмів у виконувані файли ви можете запропонувати?
2. Що таке статичне та синтаксичне дослідження програм?
3. Які інструменти статичного дослідження програм ви знаєте?

Варіант: 19

1. Для чого служать декомпілятори?
2. Від чого залежить якість роботи декомпіляторів?
3. Наведіть приклади декомпіляторів різних мов і охарактеризуйте їх.

Варіант: 20

1. Обгрунтуйте відмінності у роботі різних декомпіляторів, здійснивши їх порівняльний аналіз.

2. Для чого використовують редактори ресурсів?

8. У яких випадках робота редакторів ресурсів є задовільною, а у яких – ні? Чому?

Варіант: 21

1. Наведіть відомі вас редактори ресурсів.

2. Які програмні засоби необхідні для здійснення статичного дослідження виконуваних модулів?

3. В чому полягає захист програм паролем? Де може бути збережений пароль?

Варіант: 22

1. Як здійснюють захист за допомогою обмеження часу використання? Для якої категорії програм цей захист доцільно використовувати?

2. Де можна зберігати час використання програм? Яким чином можна здійснювати злам такого захисту?

3. В чому полягає захист обмеженням кількості запусків? Як можна приховувати змінні, які містять кількість запусків? Де її можна зберігати?

Варіант: 23

1. Які групи методів використовують для захисту від несанкціонованого дослідження коду програм? Дайте загальну характеристику цим методам.

2. Що таке обфускація і які рівні обфускації існують?

3. Як здійснюється лексична обфускація? З яких етапів вона складається?

Варіант: 24

1. Що означає обфускація даних? Які види обфускації даних існують?

2. Наведіть приклади обфускації даних.

3. В чому сутність маскування програм і яка його мета?

Варіант: 25

1. Які заплутуючи перетворення функцій можна здійснити для реалізації захисту програм від дослідження?

2. Що означає поняття непрозорих предикатів? Де використовуються непрозорі змінні і непрозорі предикати?

3. Де і як у програмах можна використати комбінаторні тотожності?

ВАРІАНТИ ЗАВДАНЬ РОЗРАХУНКОВО-ГРАФІЧНОЇ РОБОТИ

ДОДАТОК А

Титульна сторінка розрахунково-графічної роботи

Чернігівський національний технологічний університет
Кафедра кібербезпеки та математичного моделювання

Розрахунково-графічна робота

з дисципліни „ Програмний захист інформації ”

***варіант* №** _____

виконав(ла)
студент(ка) _____
(прізвище, ім’я, по-батькові)
перевірив
_____
оцінка _____ балів

Підпис викладача _____

Чернігів 201

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Базова

1. Дудатьєв А.В. Захист програмного забезпечення. Ч.1 : навчальний посібник / Андрій Дудатьєв, Валентина Каплун, Василь Семеренко – Вінниця: ВНТУ, 2005. – 140 с.
2. Каплун В. А. Захист програмного забезпечення. Ч.2 : навчальний посібник / Юрій Баришев, Олександр Дмитришин – Вінниця: ВНТУ, 2013. – 151 с.
3. Казарин О.В. Теория и практика защиты программ / Олег Казарин – М.: МГУЛ, 2004. – 450 с.- ISBN 5-93517-178-6.
4. Соколов А. Защита от компьютерного терроризма : [Справочное пособи] / Алексей Соколов, Ольга Степанюк – БХВ-Петербург: Арлит, 2002. – 496 с.
5. Щеглов А. Ю. Защита компьютерной информации от несанкциони-рованного доступа : учебное пособие / Александр Щеглов – Санкт-Петербург: Наука и Техника, 2004. – 384 с. – ISBN 5-318-00244-7.
6. Щербаков А. Защита от копирования: построение программных средств – М.: Эдель, 1992.
7. Румянцев П. В. Работа с файлами в Win 32 API. – 2-е изд. доп. / Павел Румянцев – М.: Горячая линия-Телеком, 2002. – 216 с. – ISBN 5-93517-097-3.
8. Румянцев П.В. Исследование программ Win32: до дизассемблера и отладчика – 2-е изд. доп. / Павел Румянцев – М.: Горячая линия-Телеком, 2004. – 367 с. – ISBN 5-93519-178-3.
9. Абашев А.А. Ассемблер в задачах защиты информации / Алексей Абашев, Иван Жуков, Михаил Иванов – М.: Кудиц-Образ, 2004. – 544 с. - ISBN 5-9579-0027-3.
10. Касперски К. Компьютерные вирусы изнутри и снаружи / Крис Касперски – СПб.: Питер, 2006. – 527 с. - ISBN 5-93519-178-3.
11. Касперски К. Техника и философия хакерских атак / Кри Касперски – М.: Солон-Р, 1999. – 272 с. - ISBN 5-93455-015-2.
12. Войтович О. П. Методичні вказівки до виконання курсового проекту з дисципліни "Захист програмного забезпечення" для студентів напряму підготовки 6.170101 “Безпека інформаційних і комунікаційних сис-тем” / Олеся Войтович, Валентина Каплун – Вінниця: ВНТУ, 2010. - 57 с.
13. Чернов А.В. Интегрированная среда для исследования "обфускации" программ. Доклад на конференции, посвящённой 90-летию со дня рождения А.А.Ляпунова. Россия, Новосибирск, 8-11 октября 2001 года // Електронний ресурс: http://www.ict.nsc.ru/ws/Lyap2001.
14. Домашев А.В. Программирование алгоритмов защиты информации : Учебное пособие / Алексей Домашев, Михаил Грунтович, Владимир Попов – М.: Нолидж, 2002. – 416 с. - ISBN 5-93519-024-8.

Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України "КПІ", 2001. – № 4. – С. 43-48.

32. http://uk.wikipedia.org/wiki/Інформаційна_безпека_України

33. Постанова Верховної Ради України "Про прийняття за основу проекту Закону України про Концепцію державної інформаційної політики". [Електронний ресурс]. – Доступний з http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=2897-17.

34. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.