Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 19.04.2021 16:30:27
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
_____Н.Г. Кузнецов
«01» июня 2018 г.

Рабочая программа дисциплины

Методы атакующего воздействия на информационные ресурсы

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	36	36	36	36
В том числе инт.	12	12	12	12
Итого ауд.	54	54	54	54
Контактная	54	54	54	54
Сам. работа	54	54	54	54
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____ 11.05.18

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____ 11.05.18

Методическим советом направления *к.ф.-м.н., декан, Карасёв Д.Н.* _____ 16.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2019-2020 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и)*к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2020-2021 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2021-2022 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования
учебного процесса Торопова Т.В.

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в 2022-2023 учебном году на заседании
кафедры **Информационные технологии и защита информации**

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): *к.ф.-м.н., доцент, Шейдаков Н.Е.* _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели освоения дисциплины: изучение и анализ способов нарушения информационной безопасности; потенциально опасные пути несанкционированного доступа к информации; модель поведения потенциального нарушителя, организации атак взломщиков и способы защиты от них, обучение студентов принципам и методам защиты информации в компьютерных сетях
1.2	Задачи дисциплины: ознакомить с программами и инструментами, используемыми хакерами, их стратегией; ознакомить с методами создания надежной и эффективной защиты от атак хакеров; дать рекомендации по созданию различных систем безопасности и примеры конкретных атак хакеров

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного осовения дисциплины являются навыки, знания и умения, полученные в результате изучения дисциплин:
2.1.2	Физико-технические основы обеспечения информационной безопасности
2.1.3	Методы и средства обеспечения информационной безопасности
2.1.4	Средства и методы защиты хранилищ и баз данных
2.1.5	Основы информационной безопасности
2.1.6	Теория информационной безопасности и методология защиты информации
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информационных процессов и систем
2.2.2	Защита от удаленных сетевых атак
2.2.3	Комплексное обеспечение защиты информации объекта информатизации
2.2.4	Компьютерная вирусология
2.2.5	Криптографические методы защиты информации
2.2.6	Организационное и правовое обеспечение информационной безопасности
2.2.7	Программно-аппаратные средства защиты информации
2.2.8	Специальные методы исследования аппаратных средств информационных систем

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
основные виды атакующих воздействий на операционные систе-мы; методы, применяемые для проникновения в операционные системы сете-вых и автономных ком-пьютеров; классификацию и назначение компьютер-ных вирусов и «червей»; методы антихакинга; ос-новные направления при-менения криптографиче-ских технологий при за-щите АС и примеры реа-лизующих их.
Уметь:
пользоваться интернет ресурсами; применять полученные знания при освоении последующих дисциплин по защите информации плане противодействия; реализовы-вать простейшие «вирусные» программы; самостоятельно работать с учебной, научной и справочной литературой; выбирать и использовать современные средства криптозащиты согласно области их применения; ис-пользовать стандартные алгоритмы криптографической защиты; выбирать и использовать средства обеспечения и проверки целостности данных в современной информационной системе.
Владеть:
навыками работы с диагностическими программами, анализа сетевых атак, администрирования локальных сетей
ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
Знать:
основные понятия: «идентификация», «аутентификация», «авторизация», «пароль» и др.; методы идентификации; механизм идентификации объектов и субъектов в компьютерных сетях
Уметь:
выбирать схему аутентификации, учитывая особенности объекта защиты; выполнять настройку параметров аутентификации. производить проверку целостности данных; производить оценку уязвимостей аутентификаций различных типов.
Владеть:

навыками установки антивирусного программного обеспечения; установки и настройки сетевых анализаторов

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
Знать:
методы мониторинга состояния сети
Уметь:
использовать встроенные возможности регистрации событий компонентов современных информационных систем в соответствии с целями защиты
Владеть:
навыками использования стандартных инструментов анализа сетей

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интеракт.	Примечание
	Раздел 1. Виды деструктивного воздействии на информационные ресурсы						
1.1	Тема 1. Введение. Классификация вредоносного программного обеспечения. Вторжениях в информационные системы (ИС). Сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты. Основные признаки. Назначение.	4	2	ПК-10 ПК-13	Л1.3 Э18 Э20	2	
1.2	Тема 1. Введение. Классификация хакерских атак. Определение хакерской атаки. Основные типы хакерских атак. Этапы под-готовки и проведения атак. /Лек/	4	2	ПК-10 ПК-13	Л1.3 Л2.3 Э18 Э20	0	
1.3	Тема 1. Введение. Классификация вредоносного программного обеспечения. Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни /Лаб/	4	2	ПК-1 ПК-13	Л1.3 Э1 Э2 Э3 Э19 Э20	2	
1.4	Тема 1. Введение. Классификация вредоносного программного обеспечения. Зарожение прямым действием (.COM .EXE) /Лаб/	4	4	ПК-1 ПК-13	Л1.3 Л3.1 Э9 Э20	0	
1.5	Тема 1. Введение. Языки программирования низкого уровня. Java; Assembler /Ср/	4	12	ПК-13	Л1.1 Л1.2 Л2.4 Л3.1 Э6 Э8	0	
	Раздел 2. Вирусы, троянские кони, почтовые черви, снифферы, Rootkit- ы и другие специальные						
2.1	Тема 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы. Сетевые компьютерные атаки. Цели сетевых атак. Классификация. Уязвимости ПО.Основных тенденций развития защиты информации от сетевых атак. /Лек/	4	2	ПК-10 ПК-13	Л1.3 Л1.5 Э5 Э7	2	

2.2	Тема 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы. Ботнеты - новый характер угроз. Ботнет как основная угроза интернетсетей. Способы создания ботсетей. Типы атак и применяемые шпионские программы. Цели атака. Инструмен-тальные и программные способы противодействия. /Лек/	4	2	ПК-10 ПК-13	Л1.3 Э7 Э11 Э12 Э17 Э18 Э20	2	
2.3	Тема 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы. "Пишем своего трояна". Разработка макета простейшей троянской программы для Windows /Лаб/	4	4	ПК-1	Л1.3 Л3.1 Э16	0	
2.4	Тема 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы. Зомби-сети-1 (моделирование сети ботнет). /Лаб/	4	6	ПК-1 ПК-13	Л1.3 Л3.1 Э7 Э11 Э12	2	
2.5	Тема 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы. Деструктивные программы и хакинг мобильных устройств. ОС iOS, Android и Windows Phon /Ср/	4	6	ПК-1 ПК-10	Л1.3 Э13	0	
	Раздел 3. Хакинг и антихагинг персональных компьютеров.						
3.1	Тема 3 Хакинг персональных компьютеров. Организация защиты ОС Windows Критерии оценки надежности системы. Компонеты защиты и их характери-стика. Работа и объекты системы защиты. Антихакинг. /Лек/	4	2	ПК-10 ПК-13	Л1.4 Л1.5 Л1.6 Э18 Э20	0	
3.2	Тема 3. Хакинг персональных компьютеров. Хакинг браузеров Web. Злонамеренный код HTML. Генерация диалогов. Переполнение памяти. Запуск программ. Тег IFRAME. Подмена Web-сайтов. Методы социальной инженерии. Методы защиты. /Лек/	4	2	ПК-10 ПК-13	Л1.4 Э18 Э20	0	
3.3	Тема 3 Хакинг персональных компьютеров. Хакинг почтовых клиентов. Почтовые клиенты как объект внимания хакеров. Введение в функционирование почтовых сервисов, технология вставки активного кода в почтовое вложение для запуска на атакованном компьютере, некоторые недостатки электронной почты, управляемой с Web-страниц. /Лек/	4	2	ПК-10 ПК-13	Л1.3 Л2.1	0	
3.4	Тема 3 Хакинг персональных компьютеров. Программы Mail Bombers, Spammers и Flooders, противодействие им. /Лаб/	4	4	ПК-1 ПК-10	Л1.6 Э18	0	

3.5	Тема 3 Хакинг персональных компьютеров. Хакинг почтовых клиентов. Введение в функционирование почтовых сервисов. /Лаб/	4	4	ПК-1 ПК-13	Л1.6 Л2.1 Л2.2 Л3.1 Э18	0	
3.6	Тема 3 Хакинг персональных компьютеров. Назначение и использование программ Backdoor Kits и Log Bashers. /Лаб/	4	4	ПК-1 ПК-13	Л1.6 Э18	2	
3.7	Тема 3 Хакинг персональных компьютеров. DDoS-атаки и методы борьбы с ними Man in the middle (MITM) Дефейс веб-сайтов и его классификация /Ср/	4	6	ПК-10 ПК-13	Л1.3 Э4 Э10 Э17	0	
3.8	Тема 3 Хакинг персональных компьютеров. Виртуальные машины: Установка; Настройка; Деинсталяция /Ср/	4	12	ПК-1 ПК-10 ПК-13	Л1.3	0	
	Раздел 4. Хакинг и антихагинг клиентов интернет-сервисов						
4.1	Тема 4. Хакинг и антихакинг браузеров. Хакинг брандмауэров. Компоненты брандмауэра. Настройка шлюзов с фильтрацией пакетов. Уязвимости шлюзов с фильтрацией пакетов. Программные посредники. Хакинг брандмауэра WinRoute Pro. Инвентаризацией брандмауэра. Отключение брандмауэра WinRoute Pro. Обход брандмауэра Win Route Pro. Нестрогие cnucku ACL. Рекомендации по антихакингу. /Лек/	4	2	ПК-1 ПК-10 ПК-13	Л1.4 Э18 Э20	0	
4.2	Тема 4. Хакинг и антихакинг браузеров. Хакинг брандмауэров. Перехват сетевых данных. Технологии сетевого хакинга, основанные на перехвате сетевых пакетов (прослушивания сетевого трафика с целью хищения ценной информации, для организации перехвата данных с целью атаки "человек посредине", для перехвата TCP-соединений) Программамы-сниферы для прослушивания сетевых пакетов. /Лек/	4	2	ПК-10 ПК-13	Л1.3 Э5 Э18	0	
4.3	Тема 4. Хакинг и антихакинг браузеров. Взлом паролей ОС Windows, использование программы PasswordCrackers /Лаб/	4	4	ПК-1	Л1.3 Э18	0	
4.4	Тема 4. Хакинг и антихакинг браузеров. Программы SafeSuite и SATAN. Назначение и использование /Лаб/	4	4	ПК-1	Л1.3 Э18	0	
4.5	Тема 4. Хакинг и антихакинг браузеров. Спуфинг (Spoofing) - имитация соединения iZombie USB-троян /Ср/	4	6	ПК-1 ПК-13	Л1.3 Л3.1 Э5 Э13 Э15	0	

4.6	Тема 4. Хакинг и антихакинг браузеров. Изучение специализированных пакетов диагностических программ attacker.exe ddosping.exe VMware-workstation-full-11.1.0-2496824.exe lcp504ru.exe UDPFlood 2.00 XSpider.exe /Ср/	4	12	ПК-1	Л1.3 Л2.3 Э15 Э18	0	
4.7	/Экзамен/	4	36	ПК-1 ПК-10 ПК-13	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Э14 Э15 Э16 Э17 Э18	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы кэкзамену
1. Основные классы вредоносного программного обеспечения.
2. Сетевые черви.
3. Классически вирусы
4. Троянские программы
5. Виды хакерских атак
6. Mailbombing
7. Переполнение буфера
8. Сниффинг пакетов
9. IP-спуфинг
10. Man-in-the-Middle
11. Инъекция
12. Отказ в обслуживании
13. Сетевые компьютерные атаки. Классификация.
14. Ботнеты, общая классификация.
15. Способы организации ботнетов.
16. Диагностика ботнетов, методы обнаружения и локализации.
17. Средства защиты на базе Windows 2000/XP.
18. Как работает зашита Windows 2000/XP?
19. Диспетчер SAM (Security Account Manager) и Служба AD (Active Directory)
20. Объекты системы зашиты
21. Регистрация в домене Windows 2000/XP
22. Антихакинг в системе защиты ОС Windows 2000/XP
23. Этапы проникновения в ОС автономного компьютера.
24. Применение утилиты NTFSDOS Pro для проникновения ОС автономного компьютера.
25. Взлом паролей BIOS и экранной заставки.
26. Взлом базы SAM и расширение привилегий.
27. Хакинг Web броузеров (генерация диалогов, злонамеренные HTML)
28. Хакинг Web броузеров (запуск программ, переполнение памяти)
29. Хакинг Web броузеров (запуск программ)
30. Хакинг Web броузеров (тег IFRAME)
31. Злонамеренные аплеты и сценарии при хакинге Web броузеров.
32. Считывание файлов “куки”.
33. Подмена Web-сайтов.
34. Хакинг SSL (протокол защищенных сокетов)
35. Методы социальной инженерии при защите от хакинга
36. Какие протоколы обеспечивают функционирование электронной почты?
37. Формат сообщение электронной почты.
38. Хакинг электронной почты, последовательность действий злоумышленника.
39. Установление удалённого контроля с помощью электронной почты.
40. Деструкция почтового клиента.
41. Этапы хакинга Web-сайта.
42. Сканирование и инвентаризация сервера.
43. Хакинг http.
44. Уязвимости сценариев Web-серверов.
45. Программы для офлайнового просмотра Web-сайтов.
46. Что даёт хакеру исследование кода HTML Web-сайта?\

47. Последовательность действий хакера при взломе пароля к страничке Web.
48. Разновидности атак DoS.

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в приложении 1 к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Веретенникова Е. Г., Савельева Н. Г.	Программирование на VB и VBA: учеб. пособие	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2010	54
Л1.2	Вязовик Н. А.	Программирование на Java: курс лекций : учеб. пособие	М.: Интернет-ун-т Информац. Технологий, 2003	99
Л1.3	Скудис Э.	Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: [пер. с англ.]	М.: ДМК Пресс, 2003	102
Л1.4	Левин М.	Хакинг Интернет	М.: Новый издат. дом, 2005	11
Л1.5	Левин М.	Руководство для хакеров 2 : Электронные корсары	М.: Новый издат. дом, 2005	11
Л1.6	Леонтьев Б. К.	Хакинг операционных систем Microsoft Windows XP b Linux не для дилетантов	М.: Новый издат. дом, 2005	11

6.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Михайлов А.	Электронная почта и ее защита . / https://biblioclub.ru/index.php?page=book_red&id=89287	Москва: Диалог-МИФИ, 2008	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.2	Блам Р.	Администрирование почтовых серверов sendmail: курс. / https://biblioclub.ru/index.php?page=book_red&id=233696	Москва: Интернет -Университет Информационных Технологий, 2006	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.3	Чепурнова Н. М., Ефимова Л. Л.	Правовые основы информатики: учебное пособие. / https://biblioclub.ru/index.php?page=book_red&id=426501	Москва: Юнити-Дана, 2015	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.4	Пильщиков В. Н.	Программирование на языке ассемблера IBM PC: учебное пособие. / https://biblioclub.ru/index.php?page=book_red&id=447687	Москва: Диалог-МИФИ, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.3. Методические разработки

	Авторы,	Заглавие	Издательство, год	Колич-во
Л3.1	Тищенко Е. Н.	Низкоуровневое программирование в задачах защиты информации: метод. указания	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2013	10

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Bing / http://www.bing.com
Э2	Google /https://www.google.ru/
Э3	Mail.ru/ http://go.mail.ru/
Э4	Синтаксический анализ web-страниц посредством языка программирования Python: выпускная квалификационная работа / Рычков А. О. Тобольск 2017 г. / https://biblioclub.ru/index.php?page=book_red&id=462614
Э5	Защита информации в инфокоммуникационных системах и сетях: учебное пособие / Голиков А. М. Томск: Томский государственный университет систем управления и радиоэлектроники, 2015 / https://biblioclub.ru/index.php?page=book_red&id=480637
Э6	Мобильные телекоммуникации. 2015. № 4/5(138) Москва: Профи-Пресс, 2015 / https://biblioclub.ru/index.php?page=book_red&id=336189
Э7	Антивирусная защита компьютерных систем [Электронный ресурс] / М.:Интернет-Университет Ин-формационных Технологий,2007. -282с. / http://biblioclub.ru/index.php?page=book&id=233568
Э8	Язык ассемблера : уроки программирования / Рудаков П., Финогенов К. Москва: Диалог-МИФИ, 2001 / https://biblioclub.ru/index.php?page=book_red&id=89393
Э9	Технология программирования на современных языках программирования / Лавлинский В. В. , Коровина О. В. Воронеж: ВГЛА, 2012 / https://biblioclub.ru/index.php?page=book_red&id=142453
Э10	Язык программирования Java / Баженова И. Ю. Москва: Диалог-МИФИ, 2008 / https://biblioclub.ru/index.php?page=book_red&id=54745

Э11	Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft: практикум / Ложников П. С. , Михайлов Е. М. Москва: Интернет-Университет Информационных Технологий, 2008 / https://biblioclub.ru/index.php?page=book_red&id=233194
Э12	Системный администратор. 2013. № 10 (131) Москва: Синдикат 13, 2013 / https://biblioclub.ru/index.php?page=book_red&id=227225
Э13	Защита информации : Конспект лекций: учебное пособие / Сергеева Ю. С. Москва: А-Приор, 2011 / https://biblioclub.ru/index.php?page=book_red&id=72670
Э14	Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft: практикум / Ложников П. С. , Михайлов Е. М. Москва: Интернет-Университет Информационных Технологий, 2008 / https://biblioclub.ru/index.php?page=book_red&id=233194
Э15	Защитные средства с открытыми исходными текстами : Практическое руководство по защитны м приложениям: учебное пособие / Хаулет Т. Москва: Интернет-Университет Информационных Технологий, 2007 / https://biblioclub.ru/index.php?page=book_red&id=233306
Э16	Языки программирования: лабораторный практикум, Ч. 1 / Малиновская Е.А., Рыскаленко Р.А. Ставрополь: СКФУ, 2016 / https://biblioclub.ru/index.php?page=book_red&id=467412
Э17	Системный администратор. 2004. № 1 (14) Москва: Издательский дом «Учительская газета», 2004 / https://biblioclub.ru/index.php?page=book_red&id=137868
Э18	Общие вопросы технической защиты информации / Скрипник Д. А. Москва: Национальный Открытый Университет «ИНТУИТ», 2016 / https://biblioclub.ru/index.php?page=book_red&id=429070
Э19	Яндекс / https://www.yandex.ru/
Э20	Прохорова О. В. Информационная безопасность и защита информации: учебник. - Самара: Самарский государственный архитектурно-строительный университет, 2014 / https://biblioclub.ru/index.php?page=author_red&id=96440
6.3. Перечень программного обеспечения	
6.3.1	OS Wndows
6.3.2	Lynux
6.4 Перечень информационных справочных систем	
6.4.1	Консультант +

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения, лабораторными установками. Для проведения лекционных занятий используется демонстрационное оборудование.

8. МЕТОДИЧЕСТКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по освоению дисциплины представлены в Приложении 1 к рабочей программе дисциплины.

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационные технологии и защита
информации
Протокол № 10 от «11» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Методы атакующего воздействия на информационные ресурсы
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Оглавление

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации			
Знать: основные виды атакующих воздействий на операционные системы; методы, применяемые для проникновения в операционные системы сетевых и автономных компьютеров; классификацию и назначение компьютерных вирусов и «червей»; методы антихакинга; основные направления применения криптографических технологий при защите АС и примеры реализующих их.	*поиск и сбор необходимой литературы, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1), Р – реферат,*
Уметь: пользоваться интернет ресурсами; применять полученные знания при освоении последующих дисциплин по защите информации плане противодействия; реализовывать простейшие «вирусные» программы; самостоятельно работать с учебной, научной и справочной литературой;	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 2) ЛР – лабораторная работа*

выбирать и использовать современные средства криптозащиты согласно области их применения; использовать стандартные алгоритмы криптографической защиты; выбирать и использовать средства обеспечения и проверки целостности данных в современной информационной системе.			
Владеть: навыками работы с диагностическими программами, анализа сетевых атак, администрирования локальных сетей	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 2)* *ЛР – лабораторная работа*
ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности			
Знать: основные понятия: «идентификация», «аутентификация», «авторизация», «пароль» и др.; методы идентификации; механизм идентификации объектов и субъектов в компьютерных сетях	*поиск и сбор необходимой литературы, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1),* *Р – реферат,*
Уметь: выбирать схему аутентификации, учитывая особенности объекта защиты; выполнять настройку параметров аутентификации. производить проверку целостности данных;	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной*	*О – опрос (вопрос 1),* *Р – реферат,*

производить оценку уязвимостей аутентификаций различных типов.		*работе*	
Владеть: навыками установки антивирусного программного обеспечения; установки и настройки сетевых анализаторов	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 1), Р – реферат,*
ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации			
Знать: методы мониторинга состояния сети	*поиск и сбор необходимой литературы, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов*	*соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации*	*О – опрос (вопрос 1), Р – реферат,*
Уметь: использовать встроенные возможности регистрации событий компонентов современных информационных систем в соответствии с целями защиты	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе*	*О – опрос (вопрос 1), Р – реферат,*
Владеть: навыками использования стандартных инструментов анализа сетей	*выполнение лабораторных экспериментов по тематике курса*	*объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в*	*О – опрос (вопрос 1), Р – реферат,*

		задании к лабораторной работе	

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

для экзамена:
84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы для теоретических опросов по темам лекций

1. Основные классы вредоносного программного обеспечения.
2. Сетевые черви.
3. Классически вирусы
4. Троянские программы
5. Виды хакерских атак
6. Mailbombing
7. Переполнение буфера
8. Сниффинг пакетов
9. IP-спуфинг
10. Man-in-the-Middle
11. Инъекция
12. Отказ в обслуживании
13. Средства защиты на базе Windows 2000/XP.
14. Как работает зашита Windows 2000/XP?
15. Диспетчер SAM (Security Account Manager) и Служба AD (Active Directory)
16. Объекты системы зашиты
17. Регистрация в домене Windows 2000/XP
18. Антихакинг в системе защиты ОС Windows 2000/XP
19. Этапы проникновения в ОС автономного компьютера

20. Хакинг Web броузеров (генерация диалогов, злонамеренные HTML)
21. Хакинг Web броузеров (запуск программ, переполнение памяти)
22. Хакинг Web броузеров (запуск программ)
23. Хакинг Web броузеров (тег IFRAME)
24. Злонамеренные аплеты и сценарии при хакинге Web броузеров
25. Хакинг электронной почты, последовательность действий злоумышленника.
26. Установление удалённого контроля с помощью электронной почты.
27. Деструкция почтового клиента.
28. Этапы хакинга Web-сайта.
29. Сканирование и инвентаризация сервера.
30. Хакинг http.
31. Уязвимости сценариев Web-серверов.
32. Программы для офлайнового просмотра Web-сайтов.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра **Информационных технологий и защиты информации**
(наименование кафедры)

Вопросы к экзамену

по дисциплине **Методы атакующего воздействия на информационные ресурсы**
(наименование дисциплины)

1. Основные классы вредоносного программного обеспечения.
2. Сетевые черви.
3. Классически вирусы
4. Троянские программы
5. Виды хакерских атак
6. Mailbombing
7. Переполнение буфера
8. Сниффинг пакетов
9. IP-спуфинг
10. Man-in-the-Middle
11. Инъекция
12. Отказ в обслуживании
13. Сетевые компьютерные атаки. Классификация.
14. Ботнеты, общая классификация.
15. Способы организации ботнетов.
16. Диагностика ботнетов, методы обнаружения и локализации.

17. Средства защиты на базе Windows 2000/XP.
18. Как работает зашита Windows 2000/XP?
19. Диспетчер SAM (Security Account Manager) и Служба AD (Active Directory)
20. Объекты системы зашиты
21. Регистрация в домене Windows 2000/XP
22. Антихакинг в системе защиты ОС Windows 2000/XP
23. Этапы проникновения в ОС автономного компьютера.
24. Применение утилиты NTFSDOS Pro для проникновения ОС автономного компьютера.
25. Взлом паролей BIOS и экранной заставки.
26. Взлом базы SAM и расширение привилегий.
27. Хакинг Web броузеров (генерация диалогов, злонамеренные HTML)
28. Хакинг Web броузеров (запуск программ, переполнение памяти)
29. Хакинг Web броузеров (запуск программ)
30. Хакинг Web броузеров (тег IFRAME)
31. Злонамеренные аплеты и сценарии при хакинге Web броузеров.
32. Считывание файлов “куки”.
33. Подмена Web-сайтов.
34. Хакинг SSL (протокол защищенных сокетов)
35. Методы социальной инженерии при защите от хакинга
36. Какие протоколы обеспечивают функционирование электронной почты?
37. Формат сообщение электронной почты.
38. Хакинг электронной почты, последовательность действий злоумышленника.
39. Установление удалённого контроля с помощью электронной почты.
40. Деструкция почтового клиента.
41. Этапы хакинга Web-сайта.
42. Сканирование и инвентаризация сервера.
43. Хакинг http.
44. Уязвимости сценариев Web-серверов.
45. Программы для офлайнового просмотра Web-сайтов.
46. Что даёт хакеру исследование кода HTML Web-сайта?\
47. Последовательность действий хакера при взломе пароля к страничке Web.
48. Разновидности атак DoS.

Составитель _____ Шейдаков Н.Е.
(подпись)

«____»_____20 г.

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра **Информационных технологий и защиты информации**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине **Методы атакующего воздействия на информационные ресурсы**

1. Виды хакерских атак
2. Взлом базы SAM и расширение привилегий

Составитель Н.Е. Шейдаков
(подпись)

Заведующий кафедрой

_____ Е.Н. Тищенко
(подпись)

«____»_____20 г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

по дисциплине **Методы атакующего воздействия на информационные ресурсы**

1. Снифинг пакетов
2. Хакинг Web броузеров (запуск программ)

Составитель Н.Е. Шейдаков
(подпись)

Заведующий кафедрой

_____ Е.Н. Тищенко
(подпись)

«____»_____20 г.

К комплекту экзаменационных билетов прилагаются разработанные преподавателем и утвержденные на заседании кафедры критерии оценивания по дисциплине.
Критерии оценивания:

- оценка «отлично» (84-100 баллов) выставляется, если изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на

практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- оценка хорошо» (67-83 баллов) – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, студент усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- оценка «удовлетворительно» (50-66 баллов) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- оценка неудовлетворительно» (0-49 баллов) ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Оформление тем рефератов (докладов, сообщений)

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра *Информационных технологий и защиты информации*

Темы рефератов (докладов, сообщений)

по дисциплине **Методы атакующего воздействия на информационные**

1. Защита от несанкционированного доступа к информации
2. Средства физической защиты информации
3. Основные типы атак на проводные и беспроводные компьютерные системы
4. Защита каналов связи
5. Выявление на компьютере вредоносных программ
6. iZombie
7. USB-троян
8. Кибертерроризм
9. Вирусные угрозы и проблемы информационной безопасности
10. DDoS-атаки и методы борьбы с ними
11. Man in the middle (MITM)
12. Дефейс веб-сайтов и его классификация
13. Основные виды и приемы хакерских атак
14. Спуфинг (Spoofing) - имитация соединения
15. Методы атакующего воздействия на информационные системы

16.Методы обнаружения атак
17.Сетевые черви и защита от них

Методические рекомендации по написанию, требования к оформлению

Содержание работы должно представлять обзор, анализ и обобщение материалов собранных из литературных источников сети Интернет, оформленных в соответствии с требованиями ГОСТ.

Критерии оценки:

- оценка «зачтено» выставляется студенту, *если работа соответствует полноте и содержательности проблемы исследования;, объем выполненных работы в полном объеме); соответствует требованиям по оформлению документа*
- оценка «не зачтено», *…если не выполнено одно из требований.*

Составитель _____ Н.Е. Шейдаков
(подпись)

«____»_____20 г.

Оформление лабораторных работ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра *Информационных технологий и защиты информации*
(наименование кафедры)

Лабораторные работы

по дисциплине **Методы атакующего воздействия на информационные**
(наименование дисциплины)

1.Тематика лабораторных работ по разделам и темам

Раздел 1 Виды деструктивного воздействии на информационные ресурсы
Лабораторная работа 1. Составление досье с использованием интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни
Лабораторная работа 2 Зарожение прямым действием (.COM .EXE)

Раздел 2 Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы.
Лабораторная работа 1. «Пишем своего трояна»
Лабораторная работа 2. Антивирус Касперского 5.5 для MS Exchange Server. Установка, настройка, управление
Лабораторная работа 3 Зомби-сети-1 (моделирование сети ботнет).

Раздел 3 Хакинг и антихагинг персональных компьютеров.

Лабораторная работа 1. Программы Mail Bombers, Spammers и Flooders, противодействие им.
Лабораторная работа 2. Использование программ Jakal и NMAP
Лабораторная работа 3 Использование программ Backdoor Kits и Log Bashers.

Раздел 4 Хакинг и антихагинг клиентов интернет-сервисов
Лабораторная работа 2. Взлом паролей ОС Windows, использование программы PasswordCrackers
Лабораторная работа 3. Программы SafeSuite и SATAN

2. Методические рекомендации по выполнению лабораторных работ

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

3. Критерии оценки:

- оценка «отлично» выставляется студенту, если . задание выполнено в полном объеме; сделан письменный вывод по заданию в полном объеме;
- оценка «хорошо». задание выполнено в объеме до 70 %; сделан письменный вывод по заданию в объеме до 70%;
- оценка «удовлетворительно» задание выполнено в объеме до 50%; сделан письменный вывод по заданию в объеме до 50%;
- оценка «неудовлетворительно» задание выполнено в объеме менее 50 % сделан письменный вывод по заданию в объеме менее 50%

Составитель _____ Н.Е. Шейдаков
(подпись)

«____»_____20 г.

4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация экзамена

Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 2. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры
Информационных технологий и защиты информации
Протокол № 10 от «11» мая 2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методы атакующего воздействия на информационные ресурсы
(наименование дисциплины)

10.03.01 Информационная безопасность

10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Шейдаков Н.Е., доцент каф. ИТиЗИ, к.ф.-м.н., доцент.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Методы атакующего воздействия на информационные ресурсы» адресованы студентам очной формы обучения.

Учебным планом по направлению подготовки «Информационная безопасность» предусмотрены следующие виды занятий:

- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы воздействия и противодействия атакам на информационные ресурсы, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины «Методы атакующего воздействия на информационные ресурсы» осуществляется в ходе занятий методом устного опроса, проверки выполненных индивидуальных заданий, контрольных работ, проверки подготовленных конспектов по выделенным для самостоятельного изучения темам дисциплины. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных, выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗаhttp://library.rsue.ru/ . Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.