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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Т.К. Платонова
«25» мая 2026 г.

Рабочая программа дисциплины
Методы защиты от удаленных сетевых атак

Направление подготовки
10.04.01 Информационная безопасность

Направленность (профиль) программы магистратуры
10.04.01.02 Программно-аппаратные методы расследования компьютерных преступлений

Для набора 2026 года

Квалификация
магистр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам / курсам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Практические	32	32	32	32
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Учебный план утвержден учёным советом Университета (протокол № 9 от 03.03.2026 г.).

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

Зав. кафедрой: к.э.н., доцент Ю.В. Радченко

Методический совет направления: д.э.н., профессор Е.Н. Тищенко

Директор института магистратуры: д.э.н., профессор Е.А. Иванова

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением защищенности информационных систем от удаленных сетевых атак; развитие профессиональных компетенций для нахождения оптимальных решений при построении защищенных информационных систем; привитие навыков использования специализированных средств защиты.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ПК-4. Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации

В результате освоения дисциплины обучающийся должен:

Знать:

процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения.(соотнесено с индикатором УК-1.1.)
формальные модели информационной безопасности объектов информатизации;основные характеристики и показатели эффективности средств и систем обеспечения информационной безопасности;
источники и классификацию угроз информационной безопасности;основные характеристики технических средств обеспечения информационной безопасности от утечек по техническим каналам;
методы обработки данных мониторинга информационной безопасности объектов информатизации;порядок создания и структуру отчета, создаваемого по результатам исследования (соотнесено с индикатором ПК-4.1.)

Уметь:

принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий.(соотнесено с индикатором УК-1.2.)
формализовать задачу обеспечения информационной безопасности объекта информатизации; анализировать и прогнозировать критерии эффективности обеспечения информационной безопасности объекта информатизации;классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы информационной безопасности;определять виды и типы технических средств обеспечения информационной безопасности; применять инструментальные средства мониторинга защищенности объекта информатизации;структурировать аналитическую информацию для включения в отчет(соотнесено с индикатором ПК-4.2.)

Владеть:

методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения;методиками разработки стратегий действий при проблемных ситуациях. (соотнесено с индикатором УК-1.3.)
навыками разработки модели информационной безопасности объекта информатизации; навыками определения класса защищенности информационных систем;навыками оценки критериев эффективности системы обеспечения информационной безопасности; навыками подготовки аналитических отчетов по результатам проведенного анализа (соотнесено с индикатором ПК-4.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Методы и средства защиты от удалённых сетевых атак

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
1.1	Анализ существующих методов и моделей противодействия компьютерным атакам. Структура методов и моделей противодействия компьютерным атакам. Подход к разработке методов и моделей противодействия компьютерным атакам.	Лекционные занятия	3	2	УК-1 ПК-4
1.2	Формирование модели нарушителя компьютерных сетей на базе модели ФСТЭК	Практические занятия	3	2	УК-1 ПК-4
1.3	Основные понятия в области информационной безопасности	Самостоятельная работа	3	2	УК-1 ПК-4
1.4	Способы реализации компьютерных атак и обобщённый сценарий противодействия им. Классификация компьютерных атак на критически важные информационные системы.	Лекционные занятия	3	2	УК-1 ПК-4
1.5	Атаки типа "отказ в обслуживании": практические занятия по теме лекции.	Практические занятия	3	2	УК-1 ПК-4
1.6	Анализ средств противодействия компьютерным атакам. Технология противодействия компьютерным атакам на критически важные	Лекционные занятия	3	2	УК-1 ПК-4

	информационные системы.				
1.7	Логические объекты – адресная книга (Address Book), сервисы (Services), интерфейсы (Interfaces). Правила (Rules). Шлюз уровня приложений (Application Layer Gateway).LibreOffice	Практические занятия	3	2	УК-1 ПК-4
1.8	Механизмы защиты информации. Программно-аппаратные средства обеспечения безопасности информационных сетей.	Лекционные занятия	3	2	УК-1 ПК-4
1.9	" Механизмы защиты информации", выполнение тестов	Практические занятия	3	2	УК-1 ПК-4
1.10	Подключение и основные настройки межсетевого экрана, управление через консоль, Web-интерфейс, SSH. Сброс межсетевого экрана к заводским настройкам по умолчанию. Обновление прошивки, сохранение конфигурации. Режимы admin, audit.	Лабораторные занятия	3	4	УК-1 ПК-4
1.11	Подключение и основные настройки межсетевого экрана посредством Web-интерфейса. Конфигурирование межсетевого экрана посредством Webинтерфейса	Практические занятия	3	2	УК-1 ПК-4
1.12	Настройка DHCP-сервера, DHCP-клиента, PPPoE-клиента Маршрутизация	Практические занятия	3	2	УК-1 ПК-4
1.13	Резервирование маршрутов (Route Failover). Настройка маршрутизации на основе правил (Policy-Based Routing)	Практические занятия	3	2	УК-1 ПК-4
1.14	Настройка сетевой защиты с помощью системы IDP/IPS для прозрачного режима работы интерфейсов межсетевого экрана	Лабораторные занятия	3	4	УК-1 ПК-4
1.15	Управление маршрутизацией, протокол OSPF на межсетевом экране. На межсетевом экране серии DFL может быть настроена динамическая маршрутизация на основе протокола OSPF. Таким образом, можно обеспечить автоматический выбор оптимального маршрута в крупных сетях или настроить межсетевой экран, как маршрутизатор OSPF в некоторой отдельной области сети.	Лабораторные занятия	3	4	УК-1 ПК-4

Раздел 2. Аппаратные и программные технологии защиты от сетевых атак

№	Наименование темы, краткое содержание	Вид занятия / работы / форма ПА	Семестр / Курс	Количество часов	Компетенции
2.1	Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах. Протоколы IGMP и UPnP. Качество обслуживания и Технология SharePort.	Лекционные занятия	3	2	УК-1 ПК-4
2.2	Технологии безопасности беспроводных сетей и унифицированные решения	Самостоятельная работа	3	10	УК-1 ПК-4
2.3	Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах, выполнение тестов	Практические занятия	3	2	УК-1 ПК-4
2.4	Настройка Syslog-сервера. SNMP Trap. LibreOffice	Лабораторные занятия	3	4	УК-1 ПК-4
2.5	Фильтрация трафика и виртуальные сети. Технология преобразования сетевых адресов, механизмы PAT и NAT	Лекционные занятия	3	2	УК-1 ПК-4
2.6	Технология преобразования сетевых адресов, выполнение тестов	Практические занятия	3	4	УК-1 ПК-4
2.7	DHCP-клиент, DHCP-сервер, DHCP Relay, IP Pool.	Лабораторные занятия	3	4	УК-1 ПК-4
2.8	Особенности применения межсетевых экранов и маршрутизаторов D-Link. Управление межсетевыми экранами D-Link NetDefend.	Лекционные занятия	3	2	УК-1 ПК-4
2.9	Управление межсетевыми экранами D-Link NetDefend, выполнение тестов	Практические занятия	3	4	УК-1 ПК-4
2.10	Ограничение размера пакетов транспортных и диагностических протоколов, запрет и разрешение ICMP. Поддержка IPv6. LibreOffice	Лабораторные занятия	3	4	УК-1 ПК-4
2.11	Априорный метод противодействия компьютерным атакам в терминах расширенных сетей петри.	Лекционные занятия	3	2	УК-1 ПК-4
2.12	Широковещательные рассылки. Multicast Routing. IGMP. Multicast GRE over IPSec. Управление широковещательным трафиком в современных сетях – необходимая составляющая обеспечения информационной безопасности. Межсетевые экраны D-Link предоставляют механизмы управления широковещательным трафиком.	Практические занятия	3	4	УК-1 ПК-4
2.13	Фильтрация трафика и виртуальные сети. Виртуальные локальные сети VLAN. Виртуальные частные сети (VPN)	Практические занятия	3	4	УК-1 ПК-4
2.14	Нстройка VLAN в межсетевом экране. Создание PPTP-соединения Создание IPSec-туннеля с использованием ключей	Лабораторные занятия	3	4	УК-1 ПК-4
2.15	Настройка NAT, NAT Pool, SAT, PAT, DNS Relay, перенаправление портов. Фильтрация по MAC-адресу. Создание нескольких подсетей на интерфейсе	Лабораторные занятия	3	4	УК-1 ПК-4
2.16	Настройка NAT, NAT Pool, SAT, PAT, DNS Relay, перенаправление портов. Фильтрация по MAC-адресу. Создание нескольких подсетей на интерфейсе	Самостоятельная работа	3	16	УК-1 ПК-4
2.17	Подготовка к промежуточной аттестации	Экзамен	3	36	УК-1

					ПК-4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Учебные, научные и методические издания

	Авторы, составители	Заглавие	Издательство, год	Библиотека / Количество
1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС «Университетская библиотека онлайн»
2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	ЭБС «Университетская библиотека онлайн»
3	Голиков А. М.	Защита информации в инфокоммуникационных системах и сетях: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015	ЭБС «Университетская библиотека онлайн»
4	Прохорова, О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014	ЭБС «IPR SMART»

5.2. Профессиональные базы данных и информационные справочные системы

Официальный сайт ФСТЭК России / fstec.ru
ИСС "КонсультантПлюс"
ИСС "Гарант" http://www.internet.garant.ru/
ЭБС «IPR Books» http://www.iprbookshop.ru/
Библиоклуб.ру http://biblioclub.ru/
Архив журналов РАН https://www.elibrary.ru/, https://www.libnauka.ru

5.3. Перечень программного обеспечения

Операционная система РЕД ОС
LibreOffice

5.4. Учебно-методические материалы для обучающихся с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет, и/или в специализированных лабораториях, предусмотренных образовательной программой.
Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
УК-1:Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий			
З процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения	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* , *Т*, Э (1-33)
У. принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий	решение тематических задач по соответствующим разделам курса; выполнение лабораторных экспериментов по тематике курса	объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе и ПЗ	*ЛР*, *Т*, ПЗ (вопросы 4, 9-10)
В. методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях	решение тематических задач по соответствующим разделам курса; выполнение лабораторных экспериментов по тематике курса	объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в задании к лабораторной работе и ПЗ	*ЛР* ПЗ
ПК-4:Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации			
З. формальные модели информационной безопасности объектов	поиск и сбор необходимой литературы,	соответствие проблеме исследования;	О – , *Т*, ПЗ Э (1-33)

информатизации;основные характеристики и показатели эффективности средств и систем обеспечения информационной безопасности; источники и классификацию угроз информационной безопасности;основные характеристики технических средств обеспечения информационной безопасности от утечек по техническим каналам; методы обработки данных мониторинга информационной безопасности объектов информатизации; порядок создания и структуру отчета, создаваемого по результатам исследования	использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	полнота и содержательность ответа; умение приводить примеры; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации	
У. формализовать задачу обеспечения информационной безопасности объекта информатизации; анализировать и прогнозировать критерии эффективности обеспечения информационной безопасности объекта информатизации; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы информационной безопасности; определять виды и типы технических средств обеспечения информационной безопасности; применять инструментальные средства мониторинга защищенности объекта информатизации; структурировать аналитическую информацию для включения в отчет	указывается вид работы, который должен сделать студент (составленный обзор, аннотация, письменный перевод, поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов, проведение моделирования …)	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям…	*Т* ПЗ ЛР
В. навыками разработки модели информационной безопасности объекта информатизации; навыками определения класса защищенности информационных систем; навыками оценки	решение тематических задач по соответствующим разделам курса; выполнение лабораторных	объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям изложенным в	*ЛР* ПЗ

критериев эффективности системы обеспечения информационной безопасности; навыками подготовки аналитических отчетов по результатам проведенного анализа	экспериментов по тематике курса	задании к лабораторной работе и ПЗ	

О – опрос, Т – тест, ЛЗ – лабораторные работы, Э –вопросы для экзамена, ПЗ- практические задания.

1.2 Шкалы оценивания:

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

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

2 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 экзамена

1. Основные понятия информационной безопасности.
2. Основные составляющие. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Классификация защищаемой информации по степени важности и ценности.
5. Основные определения и критерии классификации угроз.
6. Законодательный уровень информационной безопасности.
7. Административный уровень информационной безопасности.
8. Содержание политики безопасности. Программа безопасности.
9. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
10. Управление рисками. Основные этапы управления рисками.
11. Методы и модели анализа угроз.
12. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
13. Основные программно-технические меры.
14. Архитектурная безопасность.
15. Идентификация и аутентификация, управление доступом.
16. Мониторинг и аудит.
17. Шифрование, контроль целостности.
18. Экранирование, анализ защищенности.
19. Классификация межсетевых экранов.
20. Основные причины возможности проведения атаки типа Инъекция.
21. Алгоритм поведения атаки типа Иньекиия на скрипт-коды.
22. Алгоритм проведения атаки типа SQL-инъекция
23. Классификация XSS атак.
24. Отличия между хранимой и временной XSS атаками.
25. Понятия и сущность Flood-атаки.
26. Различия между DoS и DDoS атаками.
27. Методы проведения DNS-атак.
28. Методы проведения атаки BruteForce.
29. Условия успешного проведения атак типа DoS/DDoS/Flood.
30 Причины актуальности сетевых удаленных атак.
31. Сущность активного сканирования атакуемого сетевого ресурса.

32. Сущность пассивного сканирования атакуемого сетевого ресурса.
33. Методы анализа атакуемого узла.

Критерии оценивания*:*

- 84-100 баллов (оценка «отлично») - 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;

- 67-83 баллов (оценка «хорошо») - 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; усвоена основная литература, рекомендованная в рабочей программе дисциплины;

- 50-66 баллов (оценка «удовлетворительно») - наличие основных знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, исправленными после дополнительных вопросов; выполняются в целом корректные действия по применению знаний на практике;

- 0-49 баллов (оценка «неудовлетворительно») - ответы не связаны с вопросами, наличие грубых ошибок в ответе, демонстрирующие непонимание сущности излагаемого вопроса и неумение применять знания на практике; отсутствие уверенности и неточность ответов на дополнительные и наводящие вопросы.

Тесты

1. Банк тестов по разделам и (или) темам

Раздел 1. Методы и средства защиты от удалённых сетевых атак

Тема 1. «Формирование модели нарушителя компьютерных сетей».

Задание 1:

Какой аспект информационной безопасности был нарушен, если в результате атаки на сайт авторизованные пользователи не могут получить доступ к необходимым данным?

(Отметьте один правильный вариант ответа.)

Вариант 1 конфиденциальность

Вариант 2 аутентичность

Вариант 3 доступность

Вариант 4 целостность

Задание 2:

Каким термином обозначается целостность информации, подлинность факта, что данные были созданы законными участниками информационного процесса, и невозможность отказа от авторства?

(Отметьте один правильный вариант ответа.)

Вариант 1 доступность

Вариант 2 аутентичность

Вариант 3 авторизованность

Вариант 4 конфиденциальность

Задание 3:

Какие из нижеперечисленных угроз относятся к внешним угрозам?

(Ответ считается верным, если отмечены все правильные варианты ответов.)

Вариант 1 использование сотрудниками слабых паролей для доступа к информационным системам

Вариант 2 передача сотрудниками конфиденциальной информации конкурентам

Вариант 3 атаки из Интернета

Вариант 4 распространение вредоносного программного обеспечения

Вариант 5 преднамеренное удаление конфиденциальной информации сотрудниками

Вариант 6 перехват информации с использованием радиоприемных устройств

Задание 4:

Чем червь отличается от компьютерного вируса?

(Отметьте один правильный вариант ответа.)

Вариант 1 распространение червей санкционировано пользователем

Вариант 2 червь – это код, который внедряется в существующие файлы, а компьютерный вирус – это файл

Вариант 3 черви не размножаются

Вариант 4 черви размножаются, не заражая другие файлы

Задание 5:

Как называется вредоносная программа-троян, предназначенная для сокрытия в системе определенных объектов либо активности?

(Отметьте один правильный вариант ответа.)

Вариант 1 Exploit

Вариант 2 Backdoor

Вариант 3 Rootkit

Вариант 4 Trojan-Mailfinder

Какую атаку осуществляет злоумышленник, если он ждет от потенциального объекта атаки передачи ARP-запроса?

(Отметьте один правильный вариант ответа.)

Вариант 1 атака по запросу от атакуемого объекта

Вариант 2 безусловная атака

Вариант 3 атака по наступлению ожидаемого события на атакуемом объекте

Задание 6:

Благодаря чему стало возможным реализация атак типа «ложный объект сети»?

(Отметьте один правильный вариант ответа.)

Вариант 1 на клиентских машинах сети не установлено антивирусное программное обеспечение

Вариант 2 уязвимости, присущие протоколам различных уровней стека TCP/IP

Вариант 3 слишком большое количество узлов в сети Интернет привело к нехватке места в таблицах маршрутизации

Вариант 4 ограниченные возможности системных ресурсов конечных узлов сети

Задание 7:

Как называется атака, при которой атакующий передает сообщения от имени легального объекта сети?

(Отметьте один правильный вариант ответа.)

Вариант 1 отказ в обслуживании

Вариант 2 анализ сетевого трафика

Вариант 3 подмена доверенного объекта сети

Задание 8:

На каком уровне модели OSI реализуется атака типа «анализ сетевого трафика»?

(Отметьте один правильный вариант ответа.)

Вариант 1 транспортный

Вариант 2 сетевой

Вариант 3 прикладной

Вариант 4 канальный

Задание 9:

Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

(Отметьте один правильный вариант ответа.)

Вариант 1 централизованность

Вариант 2 универсальность

Вариант 3 адекватность

Вариант 4 непрерывность

Задание 10:

Как называется атака, при которой злоумышленник генерирует большое количество сообщений с разных источников для почтового сервера, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу?

(Отметьте один правильный вариант ответа.)

Вариант 1 Mailbombing

Вариант 2 ICMP-flood

Вариант 3 SYN-flood

Вариант 4 UDP-flood

Тема 2 «Анализ средств противодействия компьютерным атакам.»

Задание 1:

Какие системы предназначены для обеспечения сетевого мониторинга, анализа и оповещения в случае обнаружения сетевой атаки?

Ответ:

(1) IDP
(2) AV
(3) WCF
(4) IPS

Задание 2:

Чем системы IPS отличаются от систем IDS?

Ответ:

(1) они способны обнаруживать атаки на сеть
(2) они способны создавать оповещения в случае обнаружения сетевой атаки

(3) они способны блокировать сетевую атаку

(4) они способны осуществлять преобразование IP-адресов

Задание 3:

Какие системы предназначены для обеспечения сетевого мониторинга, анализа, оповещения в случае обнаружения сетевой атаки, а также способны ее блокировать?

Ответ:

(1) IDP

(2) AV

(3) WCF

(4) IPS

Задание 4:

В чем заключается отличие вторжений от вирусных атак?

Ответ:

(1) вторжения обычно содержатся в отдельном загрузочном файле, который закачивается в систему пользователя

(2) вторжения по характеру воздействия на атакуемую сеть могут быть как негативные, так и нейтральные

(3) вторжения проявляются как образцы вируса, нацеленные на поиск путей преодоления механизмов обеспечения безопасности

(4) вторжения могут осуществляться посредством сети

Задание 5:

Система IDP предназначена для обнаружения…

Ответ:

(1) дефектов в программном обеспечении

(2) спама

(3) вторжений

(4) нарушения целостности передаваемых данных

Задание 6:

Как система IDP в NetDefend обнаруживает вторжения?

Ответ:

(1) по сигнатурам вирусов и атак

(2) по адресу отправителя трафика

(3) на основе статистического анализа

(4) с помощью поля ESP в составе передаваемых данных

Задание 7:

Как называется определенные образцы вирусов и атак, с использованием которых IDP обнаруживает вторжения?

Ответ:

(1) сертификаты

(2) профили

(3) сигнатуры

(4) аутентификаторы

Задание 8:

На каком принципе основано обнаружение неизвестных угроз в NetDefendOS IDP?

Ответ:

(1) она не способна обнаруживать неизвестные угрозы

(2) на основе статистического анализа

(3) на использовании сертификатов открытых ключей

(4) при создании вторжений за основу часто берется использовавшийся ранее код

Задание 9:

Какая настройка в NetDefendOS IDP определяет действие, которое следует предпринять при обнаружении вторжения во входящем трафике?

Ответ:

(1) Pipe Rules

(2) Threshold Rules

(3) IDP Rules

(4) IP Rules

Задание 9:

Какие сигнатуры обладают самой высокой точностью?

Ответ:

(1) сигнатуры предотвращения вторжений
(2) сигнатуры обнаружения вторжения
(3) политики сигнатур

Задание 10:

Какие сигнатуры обнаруживают различные типы приложений трафика и могут применяться для блокировки определенных приложений?

Ответ:

(1) сигнатуры предотвращения вторжений
(2) сигнатуры обнаружения вторжения
(3) политики сигнатур

Тема 3 «Механизмы защиты информации»

Задание 1

Какая составляющая WPA отвечает за замену одного статического ключа WEP-ключами, которые автоматически генерируются и рассылаются сервером аутентификации?

Варианты ответа:

(1) TKIP
(2) EAP
(3) MIC

Задание 2

Какой метод шифрования является наиболее стойким?

Варианты ответа:

(1) WEP
(2) TKIP
(3) CCMP

Задание 3

Что посылает устройство клиента во все радиоканалы в беспроводной локальной сети IEEE 802.11 в начале процесса открытой аутентификации?

Варианты ответа:

(1) Authentication Request
(2) Association Request
(3) Association Response
(4) Probe Request

Задание 4

Какой метод аутентификации стандарта IEEE 802.11 требует настройки статического ключа шифрования WEP, одинакового для точки доступа и клиентского устройства?

Варианты ответа:

(1) открытая аутентификация
(2) аутентификация с общим ключом
(3) назначение идентификатора беспроводной локальной сети
(4) аутентификация клиента по MAC-адресу

Задание 5

Какой протокол стал первым стандартом шифрования данных в беспроводных сетях?

Варианты ответа:

(1) SSL
(2) TLS
(3) WEP
(4) WPA

Задание 6

Что такое ICV в составе WEP-кадра?

Варианты ответа:

(1) заголовок 802.11

(2) вектор инициализации

(3) значение контроля целостности

(4) ключ шифрования

Задание 7

На каком алгоритме шифрования основан CCMP (Counter-Mode with CBCMAC Protocol)?

Варианты ответа:

(1) RC4

(2) DES

(3) 3DES

(4) AES

Задание 8

На каком алгоритме шифрования основан WEP?

Варианты ответа:

(1) RC4

(2) DES

(3) 3DES

(4) AES

Задание 9

Обязательной частью какого стандарта беспроводных сетей является метод шифрования CCMP (Counter-Mode with CBCMAC Protocol)?

Варианты ответа:

(1) WEP

(2) WEP2

(3) WPA

(4) WPA2

Задание 10

Какой механизм в составе WPA позволяет предотвратить перехват пакетов, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети?

Варианты ответа:

(1) TKIP

(2) EAP

(3) MIC

Раздел 2. Аппаратные и программные технологии защиты от сетевых атак

Тема 4. Фильтрация трафика и виртуальные сети. Технология преобразования сетевых адресов, механизмы

Задание 1:

Как называется логическая группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам?

Ответ:

(1) виртуальная частная сеть

(2) виртуальная локальная сеть

(3) защищенная магистральная сеть

(4) виртуальная канальная сеть

Задание 2:

Выберите верное утверждение в отношении VLAN.

Ответ:

(1) трафик устройств, находящихся в разных VLAN'ах, полностью изолирован от других узлов сети на канальном уровне, только если они подключены к разным коммутаторам

(2) трафик устройств, находящихся в разных VLAN'ах, полностью изолирован от других узлов сети на канальном уровне, даже если они подключены к одному коммутатору

(3) трафик устройств, находящихся в разных VLAN'ах, полностью изолирован от других узлов сети на канальном уровне, только если они подключены в разным маршрутизаторам

(4) трафик устройств, находящихся в разных VLAN'ах, не изолирован от других устройств сети

Задание 3

Выберите верное утверждение в отношении VLAN.

Ответ:

(1) передача кадров между разными VLAN осуществляется на основе MAC-адреса

(2) передача кадров между разными VLAN невозможна

(3) передача кадров между разными VLAN возможна только на основании индивидуального MAC-адреса

(4) передача кадров между разными VLAN на основании MAC-адреса невозможна

Задание 4:

Как называется стандарт для виртуальных локальных сетей?

Ответ:

(1) IEEE 802.11

(2) IEEE 802.11i

(3) IEEE 802.1Q

(4) 802.1ad

Задание 4:

Как называется стандарт, который позволяет пробрасывать VLAN внутри другого VLAN'а?

Ответ:

(1) IEEE 802.11

(2) IEEE 802.11i

(3) IEEE 802.1Q

(4) 802.1ad

Задание 5:

Выберите верные утверждения в отношении VLAN и NetDefendOS.

Ответ:

(1) VLAN ID может назначаться только одному порту

(2) VLAN ID может назначаться разным портам

(3) если на одном коммутаторе разным портам присвоены разные значения VLAN ID, трафик подключенных VLAN не будет изолирован

(4) если на одном коммутаторе разным портам присвоены разные значения VLAN ID, трафик подключенных VLAN будет изолирован

Задание 6:

Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?

Ответ:

(1) виртуальная частная сеть

(2) виртуальная локальная сеть

(3) защищенная магистральная сеть

(4) виртуальная канальная сеть

Задание 7:

Как называется канал типа «точка-точка» в VPN-соединении?

Ответ:

(1) шлюз

(2) транк

(3) туннель

(4) мост

Задание 8:

Для какой цели применяются виртуальные частные сети?

Ответ:
(1) для снижения нагрузки на сеть
(2) для обеспечения информационной безопасности
(3) для обеспечения отказоустойчивости
(4) для уменьшения количества передаваемого служебного трафика

Задание 9:

На каком уровне модели OSI создают туннели протоколы L2TP и PPTP?

Ответ:
(1) канальный
(2) транспортный
(3) сетевой
(4) прикладной

Задание 10:

На каком уровне модели OSI создается управляющее VPN-туннелем соединение при работе с протоколом PPTP?

Ответ:
(1) канальный
(2) транспортный
(3) сетевой
(4) прикладной

Тема 5. Управление межсетевыми экранами

Задание 1:

Какой IP-адрес интерфейса управления при использовании протокола HTTP назначается по умолчанию интернет-маршрутизатору D-Link?

Ответ:
(1) 192.168.0.0
(2) 192.168.0.1
(3) 192.168.0.3
(4) 192.168.1.0

Задание 2:

Какой браузер необходимо использовать для просмотра web-интерфейса маршрутизатора D-Link?

Ответ:
(1) Internet Explorer
(2) Opera
(3) Google Chrome
(4) любой браузер

Задание 3:

Какое имя пользователя используется по умолчанию в интернет-маршрутизаторах D-Link серии DSR-xxx?

Ответ:
(1) user
(2) admin или Admin
(3) admin
(4) пустое поле

Задание 4:

Как называется функция DIR-100, которая позволяет фильтровать нежелательные URL-адреса Web-сайтов, блокировать домены и управлять расписанием по использованию выхода в Интернет?

Ответ:
(1) полный контроль
(2) родительский контроль
(3) прозрачный контроль
(4) пограничный контроль

Задание 5:

Что необходимо сделать для того, чтобы маршрутизатор DIR-100 превратился из широкополосного маршрутизатора в маршрутизатор Triple Play?

Ответ:

(1) зарегистрировать его на официальном сайте D-Link

(2) загрузить с FTP-сервера D-Link необходимое программное обеспечение

(3) купить в магазине дополнительное устройство DIR-100/F и настроить его

(4) данная модель не может быть маршрутизатором Triple Play

Задание 6:

Что такое Triple Play?

Ответ:

(1) способность маршрутизатора одновременно работать в прозрачном режиме и режиме некоммутируемых маршрутов

(2) способность маршрутизатора обрабатывать трафик IP-телефонии

(3) поддержка трех протоколов шифрования WEP/WPA/WPA2

(4) возможность одновременной передачи голосового, видео- и интернет-трафика с помощью одного WAN-соединения

Задание 7:

Какая модель маршрутизаторов D-Link разработана для применения в сетях ETTH (Ethernet To The Home)?

Ответ:

(1) DIR-100/F

(2) DIR-100

(3) DIR-300/NRU

(4) DIR-620

Задание 8:

В какую серию маршрутизаторов D-Link входят маршрутизаторы, поддерживающие 3G-сети?

Ответ:

(1) DIR-1xx

(2) DIR-2xx

(3) DIR-3xx

(4) DIR-3xx

Задание 9:

Как называется операционная система для управления межсетевыми экранами D-Link?

Ответ:

(1) Cisco IOS

(2) NetDefendOS

(3) Microsoft Windows

(4) Unix

Задание 10:

Какая функция межсетевых экранов D-Link обеспечивает ограничение и распределение полосы пропускания?

Ответ:

(1) Traffic Shaping

(2) Threshold Rules

(3) Server Load Balancing

(4) ZoneDefense

Ознакомиться с содержанием вопроса. Выбрать ответ, из предложенных, который вы считаете правильным, отметить его. Если в инструкции к вопросу предлагается выбрать несколько вариантов, то нужно отметить все верные по вашему мнению.

Критерии оценивания: студенту рондомно выпадает 15 вопросов.

правильный и полный ответ на 1 вопрос – 1 балл;

неправильный ответ на 1 вопрос – 0 баллов.

Количество баллов за семестр – 15 баллов.

Вопросы для опросов

1. Понятие перехвата функций ОС, как алгоритма работы вирусов

2. Классификация троянских программ.
3. Среда распространения компьютерных червей.
4. Особенности функционирования эксплоитов.
5. Методы обнаружения вирусной инвазии.
6. Признаки заражения информационной системы.
7. Достоинства сигнатурных методов обнаружения вирусов.
8. Недостатки сигнатурных методов обнаружения вирусов.
9. Достоинства не сигнатурных методов обнаружения вирусов
10. Недостатки не сигнатурных методов обнаружения вирусов
11. Определение статического метода анализа исполняемого кода
12. Определение динамического метода анализа исполняемого кода
13. Параметры воздействия сетевой атаки на внешний периметр информационной системы
14. Параметры воздействия сетевой атаки на внутренний периметр информационной системы
15. Этапы проведения сетевой атаки.
16. Определение самого сложного по реализации этапа сетевой атаки
17. Цели сетевой удаленной атаки.
18. Методы анализа атакуемого узла.
19. Классификация удаленных атак по уровню воздействия на атакуемые объекты
20. Сущность атаки типа Sniffing.
21. Сущность атаки типа Spoofing.
22. Сущность атаки типа Hijacking
23. Классификация атак типа Инъекция.
24. Основные причины возможности проведения атаки типа Инъекция.
25. Алгоритм поведения атаки типа Иньекиия на скрипт-коды.
26. Алгоритм проведения атаки типа SQL-инъекция
27. Классификация XSS атак.
28. Отличия между хранимой и временной XSS атаками.
29. Понятия и сущность Flood-атаки.
30. Различия между DoS и DDoS атаками.
31. Методы проведения DNS-атак.
32. Методы проведения атаки BruteForce.
33. Условия успешного проведения атак типа DoS/DDoS/Flood.
34. Причины актуальности сетевых удаленных атак.
35. Сущность активного сканирования атакуемого сетевого ресурса.
36. Сущность пассивного сканирования атакуемого сетевого ресурса.

Критерии оценивания:

правильный и полный ответ на 1 вопрос – 1 балл;

неправильный ответ на 1 вопрос – 0 баллов.

Количество баллов за семестр – 30 баллов.

Лабораторные задания

1.Тематика лабораторных работ по разделам и темам

Раздел 1. Методы и средства защиты от удалённых сетевых атак

Тема. «Механизмы защиты информации».

Лабораторная работа 1. Подключение и основные настройки межсетевого экрана, управление через консоль.

Раздел 2. Аппаратные и программные технологии защиты от сетевых атак

Тема. «Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизатов»

Лабораторная работа 2. Настройка Syslog-сервера. SNMP Trap.

Тема. «Фильтрация трафика и виртуальные сети. Технология преобразования сетевых адресов, механизмы»

Лабораторная работа 3. DHCP-клиент, DHCP-сервер, DHCP Relay, IP Pool..

Тема. «Особенности применения межсетевых экранов и маршрутизаторов D-Link»

Лабораторная работа 4. Ограничение размера пакетов транспортных и диагностических протоколов, запрет и разрешение ICMP. Поддержка IPv6.

Лабораторная работа 5. Настройка NAT, NAT Pool, SAT, PAT, DNS Relay.

Критерии оценки:

5 баллов. – задание выполнено верно;
3-4 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
1-2 баллов. – при выполнении задания были допущены ошибки;
0 баллов. – задание не выполнено.
Максимальное количество баллов, которые могут быть получены обучающимся — 25

Практические задания

1. Формирование модели нарушителя компьютерных сетей на базе модели ФСТЭК
2. Атаки типа "отказ в обслужинании": практические занятия по теме лекции.
3. Логические объекты – адресная книга (Address Book), сервисы (Services), интерфейсы (Interfaces). Правила (Rules). Шлюз уровня приложений (Application Layer Gateway).LibreOffice
4. " Механизмы защиты информации"
5. Подключение и основные настройки межсетевого экрана посредством Web-интерфейса. Конфигурирование межсетевого экрана посредством Webинтерфейса
6. Настройка DHCP-сервера, DHCP-клиента, PPPoE-клиента Маршрутизация
7. Резервирование маршрутов (Route Failover). Настройка маршрутизации на основе правил (Policy-Based Routing)
8. Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах, выполнение тестов
9. Технология преобразования сетевых адресов
10. Управление межсетевыми экранами D-Link NetDefend, выполнение тестов
11. Широковещательные рассылки. Multicast Routing. IGMP. Multicast GRE over IPSec. Управление широковещательным трафиком в современных сетях – необходимая составляющая обеспечения информационной безопасности. Межсетевые экраны D-Link предоставляют механизмы управления широковещательным трафиком.
12. Фильтрация трафика и виртуальные сети. Виртуальные локальные сети VLAN. Виртуальные частные сети (VPN)

Критерии оценки:

5 баллов. – задание выполнено верно;
3-4 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;

1-2 баллов. – при выполнении задания были допущены ошибки;
0 баллов. – задание не выполнено.
Максимальное количество баллов, которые могут быть получены обучающимся — 30.

3 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. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Экзамен проводится по расписанию промежуточной аттестации. Количество вопросов в задании – 3. Объявление результатов производится в день экзамена. Результаты аттестации заносятся в электронную ведомость и книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания адресованы студентам очной форм обучения.

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия и методы обнаружения и организации противодействия атак на информационные сети, даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов. При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к занятиям студенты могут воспользоваться консультациями преподавателя.

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на контрольные вопросы по изучаемой теме.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. 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, студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.