Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ИС*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
19.05.2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Администрирование информационных систем

Направление подготовки *09.03.02 Информационные системы и технологии*

Профиль подготовки *Информационные системы и технологии*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
6	**108 / 3**	**28**		**16**	**2,8**	**0,25**	**47,05**	**60,95**	**Зач. с оц.**
Итого	**108 / 3**	**28**		**16**	**2,8**	**0,25**	**47,05**	**60,95**	

Муром, 2026 г.

1. Цель освоения дисциплины

Целью освоения дисциплины «Администрирование информационных систем» является обучение студентов основам администрирования вычислительных систем и операционных систем классов Windows и Linux.

Задачи дисциплины:

В результате освоения курса «Администрирование информационных систем» студенты должны иметь представление:

- о необходимости процедур администрирования в ИС;
- об объектах и методах администрирования;
- об инсталляции информационных систем;
- об управлении и обслуживании технических средств в информационных системах;
- о методах организации и настройки сетевой инфраструктуры.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Администрирование информационных систем» обеспечивает понимание основ администрирование операционных систем и компьютерных сетей. Курс базируется на знаниях, полученных студентами в процессе изучения дисциплин «Информатика», «Инфокоммуникационные системы и сети», «Управление данными».

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем;	ОПК-7.1 Демонстрирует зания платформ, технологий и инструментальных программно-аппаратных средств для реализации информационных систем	Знать основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем (ОПК-7.1)	Вопросы к устному опросу, вопросы по лабораторной работе
	ОПК-7.2 Уметь осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии реализации информационных систем	Уметь осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии реализации информационных систем (ОПК-7.2)	
	ОПК-7.3 Применяет технологии и инструментальные программно-аппаратныме средства для реализации информационных систем	Иметь навыки владения технологиями и инструментальными программно-аппаратными средствами для реализации информационных систем (ОПК-7.3)	
ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных	ОПК-5.1 Демонстрирует знание основ системного администрирования, администрирования СУБД, современных стандартов информационного взаимодействия систем	Знать основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем (ОПК-5.1)	Вопросы к устному опросу, вопросы по лабораторной работе

систем;	ОПК-5.2 Производит инсталляцию и настройку инструментального программного обеспечения для решения задач профессиональной деятельности	Уметь выполнять параметрическую настройку информационных и автоматизированных систем (ОПК-5.2) Иметь навыки инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем (ОПК-5.2)	
ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;	ОПК-4.2 Разрабатывает элементы и разделы технической документации, относящиеся к различным этапам жизненного цикла информационной системы	Разрабатывать элементы и разделы технической документации, относящиеся к различным этапам жизненного цикла информационной системы (ОПК-4.2)	Вопросы к устному опросу, вопросы по лабораторной работе

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Администрирование операционных систем	6	18		12					60	Устный опрос, лабораторная работа
2	Администрирование элементов разработки и развертывания программного обеспечения	6	10		4					0,95	Устный опрос, лабораторная работа
Всего за семестр		108	28		16			2,8	0,25	60,95	Зач. с оц.
Итого		108	28		16			2,8	0,25	60,95	

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 6

Раздел 1. Администрирование операционных систем

Лекция 1.

Назначение и функции административной системы: функции, процедуры и службы администрирования (2 часа).

Лекция 2.

Разметка дисков, файловые системы, терминальные команды (2 часа).

Лекция 3.

Права доступа к файлам и каталогам (2 часа).

Лекция 4.

Работа в ОС через терминал (2 часа).

Лекция 5.

Загрузка операционной системы Linux, процессы (2 часа).

Лекция 6.

Сетевая архитектура Linux (2 часа).

Лекция 7.

Обеспечение комплексной информационной безопасности (2 часа).

Лекция 8.

Настройка поддержки сети на стороне сервера (2 часа).

Лекция 9.

Прокси-сервер (2 часа).

Раздел 2. Администрирование элементов разработки и развертывания программного обеспечения

Лекция 10.

Контроль версий (2 часа).

Лекция 11.

Основы Kubernetes (2 часа).

Лекция 12.

Наблюдаемость систем (2 часа).

Лекция 13.

Конфигурационное управление IT инфраструктурой (2 часа).

Лекция 14.

Основы DevOps (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 6

Раздел 1. Администрирование операционных систем

Лабораторная 1.

Написание Bash скриптов (4 часа).

Лабораторная 2.

Управление пользователями и правами доступа к файлам и каталогам (4 часа).

Лабораторная 3.

Управление сетевой безопасностью ПК с использованием IPtables (4 часа).

Раздел 2. Администрирование элементов разработки и развертывания программного обеспечения

Лабораторная 4.

Развертывание репозитория на базе системы Gitea (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Основные показатели качества функционирования сетей.
2. Структура ФС ext2, ext3, ext4.
3. Сегментация памяти в UNIX.
4. Виды сигналов в UNIX-системах.
5. Средства настройки маршрутизации.
6. Репозитории ПО в Linux-системах.
7. Использование цепочек правил в iptables.
8. Настройка DNS-сервера bind.
9. Удаленная работа по протоколу SSH.
10. Протокол LDAP и организация на его основе сервера каталогов.
11. Утилиты графического удаленного рабочего стола в Linux.
12. Система инициализации systemd.
13. Работа с сертификатами, ключами и цифровыми подписями в OpenSSL.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

4.2 Форма обучения: заочная

Уровень базового образования: среднее профессиональное.
Срок обучения 3г 6м.

Семестр	Трудоемкость, час./ зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль,час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
5	**108 / 3**	**4**		**4**	**2**	**0,5**	**10,5**	**93,75**	**Зач. с оц.(3,75)**
Итого	**108 / 3**	**4**		**4**	**2**	**0,5**	**10,5**	**93,75**	**3,75**

4.2.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Администрирование операционных систем	5	2		4					93	Устный опрос, лабораторная работа
2	Администрирование элементов разработки и развертывания программного обеспечения	5	2							0,75	Устный опрос, лабораторная работа
Всего за семестр		108	4		4	+		2	0,5	93,75	Зач. с оц.(3,75)
Итого		108	4		4			2	0,5	93,75	3,75

4.2.2. Содержание дисциплины

4.2.2.1. Перечень лекций

Семестр 5

Раздел 1. Администрирование операционных систем

Лекция 1.

Разметка дисков, файловые системы, терминальные команды. Права доступа к файлам и каталогам. Загрузка операционной системы Linux, процессы. Сетевая архитектура Linux (2 часа).

Раздел 2. Администрирование элементов разработки и развертывания программного обеспечения

Лекция 2.

Контроль версий. Наблюдаемость систем. Конфигурационное управление IT инфраструктурой (2 часа).

4.2.2.2. Перечень практических занятий

Не планируется.

4.2.2.3. Перечень лабораторных работ

Семестр 5

Раздел 1. Администрирование операционных систем

Лабораторная 1.

Написание Bash скриптов (4 часа).

4.2.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Основные показатели качества функционирования сетей.
2. Структура ФС ext2, ext3, ext4.
3. Сегментация памяти в UNIX.
4. Виды сигналов в UNIX-системах.
5. Средства настройки маршрутизации.
6. Репозитории ПО в Linux-системах.
7. Использование цепочек правил в iptables.
8. Настройка DNS-сервера bind.
9. Удаленная работа по протоколу SSH.
10. Протокол LDAP и организация на его основе сервера каталогов.
11. Утилиты графического удаленного рабочего стола в Linux.
12. Система инициализации systemd.
13. Виды сетевых атак.
14. Web-сервер Apache.
15. Разграничение прав доступа в Windows и Linux.
16. Основные компоненты и функции ядра Linux.
17. Прокси-серверы и пакетные фильтры.
18. Настройка прокси-сервера Squid.
19. Работа с сертификатами, ключами и цифровыми подписями в OpenSSL.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.2.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

1. Технология VPN.
2. Защита от вирусов в ОС Windows и Linux.
3. Администрирование пользователей.
4. Администрирование серверов WWW.

5. Фильтрация пакетов. Создание и администрирование пакетных фильтров.
6. Proxy-серверы. Создание и администрирование proxy-сервера.
7. Network Address Translation (NAT). Создание и использование.
8. Межсетевые экраны. Создание и администрирование.
9. Основные виды Internet-атак.
10. Протокол SOCKS.
11. Использование SQUID в ОС Linux и Windows для создания proxy-сервера.
12. Использование iptables для фильтрации пакетов в ОС Linux.
13. Аппаратные брандмауэры.
14. Аудит и log-файлы.
15. Защита информации в современных файловых системах (управление доступом, шифрование и т.п.).
16. Протокол SAMBA.
17. Фильтрация пакетов в операционной системе Windows.
18. Proxy-серверы в операционной системе Windows.
19. Фильтрация пакетов в операционной системе Linux.
20. Proxy-серверы в операционной системе Linux.
21. Маршрутизация пакетов в ОС Linux. Создание маршрутизатора на базе Linux.
22. Маршрутизация пакетов в ОС Windows. Создание маршрутизатора на базе Windows.
23. Протокол LDAP.
24. FTP-серверы в Unix-системах. Особенности использования.
25. Протокол DHCP и его реализации.
26. Настройка домена на основе Linux.
27. Пакетный фильтр Shorewall.
28. Инструменты удаленного администрирования Windows- и Unix-систем.
29. Протокол IPv6.
30. Протокол PPTP и его реализации.

4.2.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины «Администрирование информационных систем» применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении лабораторных работ применяется имитационный или симуляционный подход, когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Курячий, Г. В. Операционная система UNIX : учебное пособие / Г. В. Курячий. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 258 c. — ISBN 978-5-4497-0670-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/97557.html

2. Администрирование ОС Unix : учебное пособие / . — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 303 c. — ISBN 978-5-4497-0855-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/101988.html

3. Мошков, М. Е. Введение в системное администрирование Unix : учебное пособие / М. Е. Мошков. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 207 c. — ISBN 978-5-4497-0906-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/102003.html

4. Гончарук, С. В. Администрирование ОС Linux : учебное пособие / С. В. Гончарук. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 163 c. — ISBN 978-5-4497-0299-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/89414.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учебное пособие / Ю. В. Власов, Т. И. Рицкова. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 622 c. — ISBN 978-5-4497-0649-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/27280.html

2. Айвенс, К. Администрирование Microsoft Windows Server 2003 : учебное пособие / К. Айвенс. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 486 c. — ISBN 978-5-4497-0853-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - http://www.iprbookshop.ru/101986.html

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

- Документация по РЕД ОС (https://redos.red-soft.ru/documentation/)
- Документация по Fedora (https://docs.fedoraproject.org/ru/docs/)
- Документация по Windows (https://docs.microsoft.com/ru-ru/windows/)

Программное обеспечение:

Wireshark (GNU GPL 2+)

РЕД ОС (Соглашение №140/05-21У от 18.05.2021 года о сотрудничестве в области науки, развития инновационной деятельности)

iptables (GNU GPL)

SQUID (GNU GPL 2+)

SAMBA (GNU GPL)

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория информатики и программирования

12 персональных компьютеров; проектор Sanyo PDG-DSU20; экран настенный Drapper Apex Star.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторные работы проводятся в компьютерном классе. Обучающиеся выполняют индивидуальную задачу в соответствии с заданием на лабораторную работу. Полученные результаты сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требования к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – зачет с оценкой. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *09.03.02 Информационные системы и технологии* и профилю подготовки *Информационные системы и технологии*
Рабочую программу составил *ст. преподаватель Булаев А.В.*_____

Программа рассмотрена и одобрена на заседании кафедры *ИС*

протокол № 21 от 05.05.2026 года.
Заведующий кафедрой *ИС* _____*Андрианов Д.Е.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 9 от 12.05.2026 года.
Председатель комиссии ФИТР _____ *Кутарова Е.И.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине
Администрирование информационных систем

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Вопросы для устного опроса
1. Основные функции административной системы.
2. Какие типы адресов имеет узел в сети TCP/IP?
3. Что собой представляет IP-адрес?
4. Что такое сетевая маска?
5. Какие данные хранятся в таблице маршрутизации?
6. Отличия протоколов IPv4 и IPv6.
7. Назначение протокола DHCP.
8. Принцип формирования DNS-имени.
9. Как DNS-адрес преобразуется в IP-адрес?
10. Зачем нужны группы пользователей?
11. Управление правами пользователей в Windows.
12. Управление правами пользователей в Linux.
13. Назначение и способ работы пакетного фильтра.
14. Перечислить основные виды атак в глобальной сети.
15. Способы построения межсетевых экранов.
16. Как можно добавить правила фильтрации в iptables?
17. Что такое таблица в терминах iptables? Назовите основные таблицы.
18. Назначение и способ работы proxy-сервера.
19. Что такое acl? Пример использования.
20. Просмотр журнала событий в Windows.
21. Основные log-файлы Linux.
22. Назначение технологии VPN.
23. Основные принципы PKI.

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	Устный опрос (5 вопросов)	20 баллов
Рейтинг-контроль 2	Устный опрос (5 вопросов)	20 баллов
Рейтинг-контроль 3	Устный опрос (5 вопросов)	20 баллов
Посещение занятий студентом		20 баллов
Дополнительные баллы (бонусы)		
Выполнение семестрового плана самостоятельной работы	Устный опрос (5 вопросов)	20 баллов

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

ОПК-4, ОПК-5, ОПК-7
Блок "Знать"
1. Что из перечисленного является пакетным фильтром

– samba
+ iptables
– squid
– apache

2. Что делает правило следующего вида

INPUT -p tcp --dport 21 -j DROP

+ отбрасывает входящие пакеты на порт 21 по протоколу tcp
– принимает входящие пакеты с порта 21 по протоколу tcp
– отбрасывает входящие пакеты с порта 21 по протоколу tcp
– принимает входящие пакеты на порт 21 по протоколу tcp

3. Как будет выглядеть правило, запрещающее пользователю student (идентификатор 1000) пользоваться протоколом ssh (порт 22)

– OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j ACCEPT
– OUTPUT -p tcp --dport 22 -m owner 1000 -j DROP
– OUTPUT -p tcp 22 -m owner --uid-owner 1000 -j DROP
– OUTPUT -p tcp --dport 22 -m owner --uid-owner ! 1000 -j DROP
+ OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j DROP

4. Правило, разрешающее входящие пакеты с узла 10.0.0.1 только на порт 1194 протокола udp

– INPUT --dport 1194 -p udp -d 10.0.0.1 -j ACCEPT
– INPUT -p udp --dport 1194 -s 10.0.0.1 -j ACCEPT
– INPUT -p udp 1194 -s 10.0.0.1 -j ACCEPT
– INPUT -p udp --dport ! 1194 -s 10.0.0.1 -j ACCEPT
+ INPUT -s 10.0.0.1 -p udp --dport ! 1194 -j DROP
– INPUT -s ! 10.0.0.1 -p udp --dport 1194 -j DROP

5. Для запрета доступа пользователей из подсети 192.168.10.0 к прокси-серверу squid нужно использовать следующий набор правил:

– acl src 192.168.10.1-192.168.11.1
http_access deny
+ acl bad src 192.168.10.0/24
http_access deny bad
– http_access deny src 192.168.10.1-192.168.11.1
– acl deny 192.168.10.0/24

6. Как запретить всем компьютерам кроме 10.5.4.1 доступ только к сайтам с подстрокой game (используя squid)

– acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access deny the_one
http_access deny gamestr
http_access allow all
– acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access allow the_one gamestr
http_access deny the_one
+ acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access allow the_one gamestr
http_access deny gamestr
– acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access allow all
http_access deny gamestr
– acl rule src 10.5.4.1 game
http_access allow rule

http_access deny game

– acl rule src 10.5.4.1, url_regex game

http_access allow rule

http_access deny all

7. Адрес, используемый на сетевом уровне, назначаемый администратором во время конфигурирования компьютеров и маршрутизаторов:

– локальное имя компьютера

– DNS-имя

+ IP-адрес

– MAC-адрес

8. Протокол определения IP-адреса по известному MAC-адресу называется:

– Address Resolution Protocol, ARP

+ Reverse Address Resolution Protocol, RARP

– Internet Storage Name Service, iSNS

– Dynamic Host Configuration Protocol, DHCP

9. Для определения по IP-адресу физического местоположения компьютера в сети служит:

+ маршрутизация

– сети туннелей VPN

– навигация

– трансляция адресов

– система доменных имен (DNS)

10. В таблице маршрутизации хранится:

+ Адрес сети

– Имя пользователя

+ Адрес шлюза

– Название сетевого протокола

+ Сетевое подключение (интерфейс)

+ Маска сети

11. Протокол DHCP используется для:

– Маршрутизации входящего и исходящего трафика

+ Автоматизации процесса назначения сетевых настроек узлам сети

– Преобразования символьного (DNS) имени в IP адрес

– Обеспечения безопасности информации, передаваемой по протоколу TCP

12. Что представляет собой адрес узла на сетевом уровне в стеке протоколов TCP/IP v4?

– Строка

– 64 битное число

+ 4 байтное число

– 4 десятичных числа, разделённых точками

13. Распределённая система разрешения доменных имён в IP-адреса

+ DNS

– DHCP

– WINS

– ARP

14. Какие типы групп пользователей существуют в операционных системах класса Windows NT

+ локальная группа компьютера

– глобальная группа компьютера

+ локальная группа домена

+ глобальная группа домена

15. Стандартными разрешениями для файлов и каталогов в UNIX-системах являются:

+ Чтение

+ Выполнение
– Создание
– Удаление
+ Изменение

16. Транспортный протокол, который содержит механизмы установки соединения и подтверждения доставки

– IP
+ TCP
– UDP
– ICMP

17. Транспортный протокол для передачи данных в сетях IP без установки соединения

– ICMP
– TCP
– RIP
+ UDP

18. Атака, основанная на протоколе ICMP, выводящая ОС компьютера из строя

+ Ping of death
– Ping flood
– ICMP flood
– Echo redirect

19. От каких атак защищает установка обновлений, выпускаемых разработчиками ОС

+ Недостатки сетевых протоколов
+ Ping of death
+ Фрагментация пакетов
– Спам
– DOS-атаки
– SYN flood

20. Какими способами можно бороться с фальсификацией электронной почты

+ Использовать цифровые подписи
– Использовать уникальные почтовые ящики
– Использовать протокол IMAP
+ Использовать VPN

21. Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

– HTTP
– Все перечисленные
– FTP
+ Ни один из перечисленных
– SSH
– DNS

22. Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

– ICMP
+ Все перечисленные
– TCP
– Ни один из перечисленных
– UDP

23. Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

– HTTP
– Все перечисленные
+ ICMP

– Ни один из перечисленных
– IP
– DNS

24. Протокол, используемый для диагностики и настройки сетей
+ ICMP
– VPN
– DHCP
– RIP

25. Переполнение буфера используется в атаках вида
+ Недостатки приложений
– DDOS-атаки
– DOS-атаки
– SYN flood

26. Сведения, используемые для фильтрации трафика из заголовка IP
+ Адрес отправителя
– Порт отправителя
+ Адрес получателя
– Порт получателя
– Флаг установки соединения
+ Протокол
– Все перечисленные

27. Выберите соответствие адресов компьютера их типам
10.0.2.5 - IP-адрес
6F:D4:32:0A:46:1B - MAC-адрес
ftp.mandriva.com - DNS-имя
mycomp - Netbios-имя

28. Какие из перечисленных протоколов используют флаги SYN, ACK
+ TCP
– UDP
– ICMP
– IP
– ARP

29. Совокупность адреса компьютера и номера порта, определяющая конечные точки соединения, называется ...
– Сеанс
+ Сокет
– Соединение
– URL

30. Что такое бит SYN?
+ бит синхронизации устанавливается при передаче начального запроса на установку соединения
– бит подтверждения доставки пакета
– бит отклонения, означающий повреждение пакета
– бит завершения соединения

31. Что такое бит ACK?
– бит синхронизации устанавливается при передаче начального запроса на установку соединения
+ бит подтверждения доставки пакета
– бит отклонения, означающий повреждение пакета
– бит завершения соединения

32. Укажите достоинства пакетных фильтров
+ "бесплатная" фильтрация пакетов
– простота настройки
– возможность фильтрации по содержимому пакетов

+ прозрачность для пользователей

Блок "Уметь"

33. Каким образом хранятся пароли пользователей в большинстве современных Linux-систем
- – в открытом виде в файле /etc/passwd
- – в открытом виде в файле /etc/shadow
- – в зашифрованном виде в файле /etc/passwd
- – в зашифрованном виде в файле /etc/shadow
- – в виде хэша в файле /etc/passwd
- + в виде хэша в файле /etc/shadow

34. Неправильным URL-адресом является:
- – http://ru.wikipedia.org/wiki/URL
- – http://en.wikipedia.org:80/wiki/Special:Search?search=train&go=Go
- – ftp://myname:mypass@myhost.com:21/etc/motd
- + myhost.dom://ftp/pros/somename

35. Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах
- – HTTP
- – Все перечисленные
- – FTP
- + Ни один из перечисленных
- – SSH
- – DNS

36. Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах
- – ICMP
- + Все перечисленные
- – TCP
- – Ни один из перечисленных
- – UDP

37. Какими способами можно бороться с фальсификацией электронной почты
- + Использовать цифровые подписи
- – Использовать уникальные почтовые ящики
- – Использовать протокол IMAP
- + Использовать VPN

38. Укажите достоинства пакетных фильтров
- + "бесплатная" фильтрация пакетов
- – простота настройки
- – возможность фильтрации по содержимому пакетов
- + прозрачность для пользователей

39. Сведения, используемые для фильтрации трафика из заголовка IP
- + Адрес отправителя
- – Порт отправителя
- + Адрес получателя
- – Порт получателя
- – Флаг установки соединения
- + Протокол
- – Все перечисленные

40. Планировщик в UNIX-системах
- – timed
- – shed
- + cron
- – daemon

41. Какие типы групп пользователей существуют в операционных системах класса Windows NT

+ локальная группа компьютера
– глобальная группа компьютера
+ локальная группа домена
+ глобальная группа домена

42. Стандартными разрешениями для файлов и каталогов в UNIX-системах являются:

+ Чтение
+ Выполнение
– Создание
– Удаление
+ Запись

43. Вид прав в UNIX-системах, позволяющий пользователю заходить в каталог

– r
– w
+ x
– e

44. Какой из IP-адресов является адресом широковещательной рассылки

– 127.0.0.1
– 192.168.8.0
+ 10.2.255.255
– 0.0.0.0

45. Шлюз по умолчанию имеет адрес

– 127.0.0.1
– 255.255.255.255
– 8.8.8.8
+ 0.0.0.0

46. Какая информация передаётся по протоколу DHCP

– IP-адрес
– DNS-сервер
– Маска сети
+ Всё перечисленное

47. Что представляет собой адрес узла на сетевом уровне в стеке протоколов TCP/IP v4?

– Строка
– 64 битное число
+ 4 байтное число
– 4 десятичных числа, разделённых точками

48. Выберите соответствие адресов компьютера их типам

10.0.2.5 IP-адрес
6F:D4:32:0A:46:1B MAC-адрес
ftp.mandriva.com DNS-имя
mycomp Netbios-имя

49. Какие из перечисленных протоколов используют флаги SYN, ACK

+ 100%TCP
– UDP
– ICMP
– IP
– ARP

Блок "Владеть"

50. Укажите назначение различных протоколов

Протокол передачи файлов FTP

Протокол диагностики и настройки сети ICMP
Транспортный протокол с установкой соединения TCP
Транспортный протокол без установки соединения UDP

51. Укажите назначение различных протоколов

Передача пакетов между различными сетями IP
Автоматическая настройка узлов сети DHCP
Передача гипертекстовой информации HTTP
Разрешения IP-адресов в MAC-адреса ARP

52. Что делает правило следующего вида

INPUT -p tcp --dport 21 -j DROP

\+ отбрасывает входящие пакеты на порт 21 по протоколу tcp
– принимает входящие пакеты с порта 21 по протоколу tcp
– отбрасывает входящие пакеты с порта 21 по протоколу tcp
– принимает входящие пакеты на порт 21 по протоколу tcp

53. Как будет выглядеть правило, запрещающее пользователю student (идентификатор 1000) пользоваться протоколом ssh (порт 22)

– OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j ACCEPT
– OUTPUT -p tcp --dport 22 -m owner 1000 -j DROP
– OUTPUT -p tcp 22 -m owner --uid-owner 1000 -j DROP
– OUTPUT -p tcp --dport 22 -m owner --uid-owner ! 1000 -j DROP
\+ OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j DROP

54. Укажите корректные сетевые маски

\+ 255.255.0.0
\+ 255.255.255.0
– 255.0.255.0
– 255.255.250.0
\+ 255.255.252.0
\+ 255.255.255.192

55. Правило, разрешающее входящие пакеты с узла 10.0.0.1 только на порт 1194 протокола udp

– INPUT --dport 1194 -p udp -d 10.0.0.1 -j ACCEPT
– INPUT -p udp --dport 1194 -s 10.0.0.1 -j ACCEPT
– INPUT -p udp 1194 -s 10.0.0.1 -j ACCEPT
– INPUT -p udp --dport ! 1194 -s 10.0.0.1 -j ACCEPT
\+ INPUT -s 10.0.0.1 -p udp --dport ! 1194 -j DROP
– INPUT -s ! 10.0.0.1 -p udp --dport 1194 -j DROP

56. Для запрета доступа пользователей из подсети 192.168.10.0 к прокси-серверу squid нужно использовать следующий набор правил:

– acl src 192.168.10.1-192.168.11.1

http_access deny

\+ acl bad src 192.168.10.0/24

http_access deny bad

– http_access deny src 192.168.10.1-192.168.11.1
– acl deny 192.168.10.0/24

57. Как запретить всем компьютерам кроме 10.5.4.1 доступ только к сайтам с подстрокой game (используя squid)

– acl the_one src 10.5.4.1

acl gamestr url_regex game
http_access deny the_one
http_access deny gamestr
http_access allow all

– acl the_one src 10.5.4.1

acl gamestr url_regex game
http_access allow the_one gamestr

http_access deny the_one
+ acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access allow the_one gamestr
http_access deny gamestr
– acl the_one src 10.5.4.1
acl gamestr url_regex game
http_access allow all
http_access deny gamestr
– acl rule src 10.5.4.1 game
http_access allow rule
http_access deny game
– acl rule src 10.5.4.1, url_regex game
http_access allow rule
http_access deny all

58. Основные механизмы защиты в VPN
+ Идентификация пользователя
+ Шифрование данных
+ Подтверждение подлинности данных
– Фильтрация трафика
– Защита от вирусов
– Централизованное хранение учетных данных пользователей

59. От каких атак защищает установка обновлений, выпускаемых разработчиками ОС
+ Недостатки сетевых протоколов
+ Ping of death
+ Фрагментация пакетов
– Спам
– DOS-атаки
– SYN flood

60. В таблице маршрутизации хранится:
+ Адрес сети
– Имя пользователя
+ Адрес шлюза
– Название сетевого протокола
+ Сетевое подключение (интерфейс)
+ Маска сети

Методические материалы, характеризующие процедуры оценивания

На основе перечня вопросов к тестированию программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов: 8 вопросов из блока 1, 4 вопроса из блока 2 и 3 вопроса из блока 3. Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является балл, рассчитанный на основе количества правильных ответов. С учетом индивидуального семестрового рейтинга студента формируется итоговый балл по курсу.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

V1:top

V2:Администрирование информационных систем

V3:ОПК-7 Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем;

V4:ОПК-7.1 Демонстрирует знания платформ, технологий и инструментальных программно-аппаратных средств для реализации информационных систем

I:Команды Linux

S:Укажите команды Linux, соответствующие описанию
L1: Определение свободного места на диске
R1: df
L2: Управление разделами на диске
R2: fdisk
L3: Определение размера элемента файловой системы
R3: du
L4: Определение пути к текущему каталогу
R4: pwd
L5: Смена текущего каталога
R5: cd
R6: dd
I:Адрес, используемый на сетевом уровне, назначаемый администратором во время конфигурирования компьютеров ...
S:Адрес, используемый на сетевом уровне, назначаемый администратором во время конфигурирования компьютеров и маршрутизаторов:
-:локальное имя компьютера
-:DNS-имя
+:IP-адрес
-:MAC-адрес
I:Атака на БД
S:Как называется атака, заключающаяся во внедрении в HTTP-запрос непредусмотренного кода SQL
+:SQL-инъекция
-:SQL flooding
-:SQL gate
-:SQL bomb
I:Атака, основанная на протоколе ICMP, выводящая ОС компьютера из строя
S:Атака, основанная на протоколе ICMP, выводящая ОС компьютера из строя
+:Ping of death
-:Ping flood
-:ICMP flood
-:Echo redirect
I:В терминах администрирования UNIX-систем "демон" - это
S:В терминах администрирования UNIX-систем "демон" - это
+:Системная служба
-:Зависший пользовательский процесс
-:Злоумышленник, атакующий компьютер
-:Злобное мифическое существо с рогами и копытами
I:Главный конфигурационный файл веб-сервера Apache обычно называется:
S:Главный конфигурационный файл веб-сервера Apache обычно называется:
+:httpd.conf
-:webs.conf
-:samba.conf
-:host.conf
I:Для определения по IP-адресу физического местоположения компьютера в сети служит:
S:Для определения по IP-адресу физического местоположения компьютера в сети служит:
+:маршрутизация
-:сети туннелей VPN
-:навигация
-:трансляция адресов
-:система доменных имен (DNS)

I:Записи в конфигурационном файле syslog "kernel.alert" и "auth.warning" это примеры
S:Записи в конфигурационном файле syslog "kernel.alert" и "auth.warning" это примеры
+:селектора
-:действия
-:имени системного устройства
-:критичности события
I:Имя администратора в UNIX-системах
S:Имя администратора в UNIX-системах
+:root
-:superuser
-:admin
-:daemon
I:Интерфейс CGI предназначен для:
S:Интерфейс CGI предназначен для:
-:Доступа к статическим страницам на сервере
-:Защищённого обмена информацией между сервером и клиентом
+:Запуска на сервере программ или скриптов для получения динамических данных
-:Получения удалённого доступа к серверу
I:Каждая запись в конфигурационном файле утилиты syslog состоит из:
S:Каждая запись в конфигурационном файле утилиты syslog состоит из:
-:Устройство, действие
-:Критичность, действие
-:Селектор, устройство
+:Селектор, действие
-:Устройство, критичность
V4:ОПК-7.2 Уметь осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии реализации информационных систем
I:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах
S:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах
-:HTTP
-:Все перечисленные
+:ICMP
-:Ни один из перечисленных
-:IP
-:DNS
I:Какой параметр в конфигурации Apache определяет файл, возвращаемый сервером при обращении к каталогу
S:Какой параметр в конфигурации Apache определяет файл, возвращаемый сервером при обращении к каталогу
-:AccessFileName
+:DirectoryIndex
-:Alias
-:BaseFile
I:Команда Linux
S:Укажите команду Linux, позволяющую изменить права доступа к файлу
-:chright
-:chown
+:chmod
-:chkdsk
I:Методом передачи данных по протоколу HTTP не является:
S:Методом передачи данных по протоколу HTTP не является:

-:GET
-:POST
+:PUSH
-:PUT
I:Недостаток классических прокси-серверов
S:Недостаток классических прокси-серверов
-:сокрытие информации о клиентах внутренней сети
-:невозможность ведения log-файлов
+:необходимость перестройки или модификации клиентского ПО
-:невозможность фильтрации по содержимому трафика
I:Номер порта, обычно используемый веб-серверами
S:Номер порта, обычно используемый веб-серверами
-:20
+:80
-:1024
-:22
I:Одно из основных средств аудита в системах класса Unix?
S:Одно из основных средств аудита в системах класса Unix?
+:Утилита syslog
-:Утилита squid
-:Утилита wtmp
-:Утилита lastlog
I:Переполнение буфера используется в атаках вида
S:Переполнение буфера используется в атаках вида
+:Недостатки приложений
-:DDOS-атаки
-:DOS-атаки
-:SYN flood
I:Протокол DHCP используется для:
S:Протокол DHCP используется для:
-:Маршрутизации входящего и исходящего трафика
+:Автоматизации процесса назначения сетевых настроек узлам сети
-:Преобразования символьного (DNS) имени в IP адрес
-:Обеспечения безопасности информации, передаваемой по протоколу TCP
I:Протокол MIME служит для:
S:Протокол MIME служит для:
+:Определения типа содержимого в передаваемых данных
-:Указания метода обмена данными с веб-сервером
-:Установки шифрованного соединения с веб-сервером
-:Передачи произвольных файлов с веб-сервера
I:Протокол, используемый для диагностики и настройки сетей
S:Протокол, используемый для диагностики и настройки сетей
+:ICMP
-:VPN
-:DHCP
-:RIP
I:Протокол определения IP-адреса по известному MAC-адресу называется:
S:Протокол определения IP-адреса по известному MAC-адресу называется:
-:Address Resolution Protocol, ARP
+:Reverse Address Resolution Protocol, RARP
-:Internet Storage Name Service, iSNS
-:Dynamic Host Configuration Protocol, DHCP
I:Распределённая система разрешения доменных имён в IP-адреса
S:Распределённая система разрешения доменных имён в IP-адреса

+:DNS
-:DHCP
-:WINS
-:ARP
V4:ОПК-7.3 Применяет технологии и инструментальные программно-аппаратные средства для реализации информационных систем
I:Сертификат пользователя содержит его:
S:Сертификат пользователя содержит его:
-:Закрытый ключ
+:Открытый ключ
-:Цифровую подпись
-:IP-адрес
I:Сети VPN используются для
S:Сети VPN используются для
-:Маршрутизации информации
+:Шифрования информации
-:Высокоскоростной передачи информации
-:Объединения сетей с различной архитектурой
I:Сниффер - это
S:Сниффер - это
+:Программа или устройство, для перехвата всего трафика, проходящего через данный узел
-:Участник DDOS-атаки
-:Вид пакетного фильтра
-:Атакующий, использующий подмену IP-адреса для проникновения через брандмауэр
I:Совокупность адреса компьютера и номера порта, определяющая конечные точки соединения, называется ...
S:Совокупность адреса компьютера и номера порта, определяющая конечные точки соединения, называется ...
-:Сеанс
+:Сокет
-:Соединение
-:URL
I:Транспортный протокол для передачи данных в сетях IP без установки соединения
S:Транспортный протокол для передачи данных в сетях IP без установки соединения
-:ICMP
-:TCP
-:RIP
+:UDP
I:Транспортный протокол, который содержит механизмы установки соединения и подтверждения доставки
S:Транспортный протокол, который содержит механизмы установки соединения и подтверждения доставки
-:IP
+:TCP
-:UDP
-:ICMP
I:Функция прокси-сервера, при которой количество внешних IP-адресов определяет количество одновременно ...
S:Функция прокси-сервера, при которой количество внешних IP-адресов определяет количество одновременно работающих с внешней сетью клиентов?
+:Базовая трансляция адресов
-:Трансляция адресов портов
-:Векторизация адресов

-:Фильтрация контента

I:Что из перечисленного является пакетным фильтром

S:Что из перечисленного является пакетным фильтром

-:samba

+:iptables

-:squid

-:apache

I:Что из перечисленного является протоколом обмена данными с веб-сервером?

S:Что из перечисленного является протоколом обмена данными с веб-сервером?

+:http

-:dns

-:dhcp

-:html

I:Что такое бит ACK?

S:Что такое бит ACK?

-:бит синхронизации устанавливается при передаче начального запроса на установку соединения

+:бит подтверждения доставки пакета

-:бит отклонения, означающий повреждение пакета

-:бит завершения соединения

I:Что такое бит SYN?

S:Что такое бит SYN?

+:бит синхронизации устанавливается при передаче начального запроса на установку соединения

-:бит подтверждения доставки пакета

-:бит отклонения, означающий повреждение пакета

-:бит завершения соединения

V3:ОПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем;

V4:ОПК-5.1 Демонстрирует знание основ системного администрирования, администрирования СУБД, современных стандартов информационного взаимодействия систем

I:Выберите соответствие адресов компьютера их типам

S:Выберите соответствие адресов компьютера их типам

L1: 10.0.2.5

R1: IP-адрес

L2: 6F:D4:32:0A:46:1B

R2: MAC-адрес

L3: ftp.mandriva.com

R3: DNS-имя

L4: mycomp

R4: Netbios-имя

I:Атаки на приложения

S:Укажите основные методы атак на приложения в глобальной сети

+:Неправильная (небезопасная) конфигурация

+:Переполнение буфера

+:Учетные записи по умолчанию

-:Несоответствие типа приложения назначению

-:Подделка цифровой подписи

I:Вид прав в UNIX-системах, позволяющий пользователю заходить в каталог

S:Вид прав в UNIX-системах, позволяющий пользователю заходить в каталог

-:r

-:w

+:x

-:e

I:Какая информация передаётся по протоколу DHCP

S:Какая информация передаётся по протоколу DHCP

-:IP-адрес

-:DNS-сервер

-:Маска сети

+:Всё перечисленное

I:Какие из перечисленных протоколов используют флаги SYN, ACK

S:Какие из перечисленных протоколов используют флаги SYN, ACK

+:TCP

-:UDP

-:ICMP

-:IP

-:ARP

I:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

S:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

-:ICMP

+:Все перечисленные

-:TCP

-:Ни один из перечисленных

-:UDP

I:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

S:Какие протоколы можно указывать при создании правил фильтрации в пакетных фильтрах

-:HTTP

-:Все перечисленные

-:FTP

+:Ни один из перечисленных

-:SSH

-:DNS

I:Какие типы групп пользователей существуют в операционных системах класса Windows NT

S:Какие типы групп пользователей существуют в операционных системах класса Windows NT

+:локальная группа компьютера

-:глобальная группа компьютера

+:локальная группа домена

+:глобальная группа домена

I:Какими способами можно бороться с фальсификацией электронной почты

S:Какими способами можно бороться с фальсификацией электронной почты

+:Использовать цифровые подписи

-:Использовать уникальные почтовые ящики

-:Использовать протокол IMAP

+:Использовать VPN

I:Каким образом хранятся пароли пользователей в большинстве современных Linux-систем

S:Каким образом хранятся пароли пользователей в большинстве современных Linux-систем

-:в открытом виде в файле /etc/passwd

-:в открытом виде в файле /etc/shadow

-:в зашифрованном виде в файле /etc/passwd

-:в зашифрованном виде в файле /etc/shadow
-:в виде хэша в файле /etc/passwd
+:в виде хэша в файле /etc/shadow
I:Какой из IP-адресов является адресом широковещательной рассылки
S:Какой из IP-адресов является адресом широковещательной рассылки
-:127.0.0.1
-:192.168.8.0
+:10.2.255.255
-:0.0.0.0
V4:ОПК-5.2 Производит инсталляцию и настройку инструментального программного обеспечения для решения задач профессиональной деятельности
I:Неправильным URL-адресом является:
S:Неправильным URL-адресом является:
-:http://ru.wikipedia.org/wiki/URL
-:http://en.wikipedia.org:80/wiki/Special:Search?search=train&go=Go
-:ftp://myname:mypass@myhost.com:21/etc/motd
+:myhost.dom://ftp/pros/somename
I:Планировщик в UNIX-системах
S:Планировщик в UNIX-системах
-:timed
-:shed
+:cron
-:daemon
I:Сведения, используемые для фильтрации трафика из заголовка IP
S:Сведения, используемые для фильтрации трафика из заголовка IP
+:Адрес отправителя
-:Порт отправителя
+:Адрес получателя
-:Порт получателя
-:Флаг установки соединения
+:Протокол
-:Все перечисленные
I:Стандартными разрешениями для файлов и каталогов в UNIX-системах являются:
S:Стандартными разрешениями для файлов и каталогов в UNIX-системах являются:
+:Чтение
+:Выполнение
-:Создание
-:Удаление
+:Запись
I:Укажите достоинства пакетных фильтров
S:Укажите достоинства пакетных фильтров
+:"бесплатная" фильтрация пакетов
-:простота настройки
-:возможность фильтрации по содержимому пакетов
+:прозрачность для пользователей
I:Что представляет собой адрес узла на сетевом уровне в стеке протоколов TCP/IP v4?
S:Что представляет собой адрес узла на сетевом уровне в стеке протоколов TCP/IP v4?
-:Строка
-:64 битное число
+:4 байтное число
-:4 десятичных числа, разделённых точками
I:Шлюз по умолчанию имеет адрес
S:Шлюз по умолчанию имеет адрес
-:127.0.0.1

-:255.255.255.255
-:8.8.8.8
+:0.0.0.0
V3:ОПК-4 Способен участвовать в разработке технической документации, связанной с профессиональной деятельностью с использованием стандартов, норм и правил;
V4:ОПК-4.2 Разрабатывает элементы и разделы технической документации, относящиеся к различным этапам жизненного цикла информационной системы
I:Укажите назначение различных протоколов
S:Укажите назначение различных протоколов
L1: Протокол передачи файлов
R1: FTP
L2: Протокол диагностики и настройки сети
R2: ICMP
L3: Транспортный протокол с установкой соединения
R3: TCP
L4: Транспортный протокол без установки соединения
R4: UDP
I:Укажите назначение различных протоколов
S:Укажите назначение различных протоколов
L1: Передача пакетов между различными сетями
R1: IP
L2: Автоматическая настройка узлов сети
R2: DHCP
L3: Передача гипертекстовой информации
R3: HTTP
L4: Разрешение IP-адресов в MAC-адреса
R4: ARP
I:В таблице маршрутизации хранится:
S:В таблице маршрутизации хранится:
+:Адрес сети
-:Имя пользователя
+:Адрес шлюза
-:Название сетевого протокола
+:Сетевое подключение (интерфейс)
+:Маска сети
I:Для запрета доступа пользователей из подсети 192.168.10.0 к прокси-серверу squid нужно использовать следующий ...
S:Для запрета доступа пользователей из подсети 192.168.10.0 к прокси-серверу squid нужно использовать следующий набор правил:
-:acl src 192.168.10.1-192.168.11.1
http_access deny
+:acl bad src 192.168.10.0/24
http_access deny bad
-:http_access deny src 192.168.10.1-192.168.11.1
-:acl deny 192.168.10.0/24
I:Как будет выглядеть правило, запрещающее пользователю student (идентификатор 1000) пользоваться протоколом ssh ...
S:Как будет выглядеть правило, запрещающее пользователю student (идентификатор 1000) пользоваться протоколом ssh (порт 22)
-:OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j ACCEPT
-:OUTPUT -p tcp --dport 22 -m owner 1000 -j DROP
-:OUTPUT -p tcp 22 -m owner --uid-owner 1000 -j DROP
-:OUTPUT -p tcp --dport 22 -m owner --uid-owner ! 1000 -j DROP
+:OUTPUT -p tcp --dport 22 -m owner --uid-owner 1000 -j DROP

I:Как запретить всем компьютерам кроме 10.5.4.1 доступ только к сайтам с подстрокой game (используя squid)

S:Как запретить всем компьютерам кроме 10.5.4.1 доступ только к сайтам с подстрокой game (используя squid)

-:acl the_one src 10.5.4.1
 acl gamestr url_regex game
 http_access deny the_one
 http_access deny gamestr
 http_access allow all

-:acl the_one src 10.5.4.1
 acl gamestr url_regex game
 http_access allow the_one gamestr
 http_access deny the_one

+:acl the_one src 10.5.4.1
 acl gamestr url_regex game
 http_access allow the_one gamestr
 http_access deny gamestr

-:acl the_one src 10.5.4.1
 acl gamestr url_regex game
 http_access allow all
 http_access deny gamestr

-:acl rule src 10.5.4.1 game
 http_access allow rule
 http_access deny game

-:acl rule src 10.5.4.1, url_regex game
 http_access allow rule
 http_access deny all

I:Основные механизмы защиты в VPN

S:Основные механизмы защиты в VPN

+:Идентификация пользователя

+:Шифрование данных

+:Подтверждение подлинности данных

-:Фильтрация трафика

-:Защита от вирусов

-:Централизованное хранение учетных данных пользователей

I:От каких атак защищает установка обновлений, выпускаемых разработчиками ОС

S:От каких атак защищает установка обновлений, выпускаемых разработчиками ОС

+:Недостатки сетевых протоколов

+:Ping of death

+:Фрагментация пакетов

-:Спам

-:DOS-атаки

-:SYN flood

I:Правило, разрешающее входящие пакеты с узла 10.0.0.1 только на порт 1194 протокола udp

S:Правило, разрешающее входящие пакеты с узла 10.0.0.1 только на порт 1194 протокола udp

-:INPUT --dport 1194 -p udp -d 10.0.0.1 -j ACCEPT

-:INPUT -p udp --dport 1194 -s 10.0.0.1 -j ACCEPT

-:INPUT -p udp 1194 -s 10.0.0.1 -j ACCEPT

-:INPUT -p udp --dport ! 1194 -s 10.0.0.1 -j ACCEPT

+:INPUT -s 10.0.0.1 -p udp --dport ! 1194 -j DROP

-:INPUT -s ! 10.0.0.1 -p udp --dport 1194 -j DROP

I:Укажите корректные сетевые маски

S:Укажите корректные сетевые маски
+:255.255.0.0
+:255.255.255.0
-:255.0.255.0
-:255.255.250.0
+:255.255.252.0
+:255.255.255.192
I:Что делает правило следующего вида
INPUT -p tcp --dport 21 -j DROP
S:Что делает правило следующего вида
INPUT -p tcp --dport 21 -j DROP
+:отбрасывает входящие пакеты на порт 21 по протоколу tcp
-:принимает входящие пакеты с порта 21 по протоколу tcp
-:отбрасывает входящие пакеты с порта 21 по протоколу tcp
-:принимает входящие пакеты на порт 21 по протоколу tcp

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=472&cat=2635%2C16676&qpage=0&category=38615%2C16676&qbshowtext=0&recurse=0&recurse=1&showhidden=0

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.