МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
«28» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Безопасность операционных систем Linux»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Преподаватель  /Г.Ф. Шипулин/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью преподавания дисциплины является формирование у студентов знаний в области безопасности операционных систем Linux.
Задачи преподавания дисциплины:

- изучение принципов организации информационных систем в соответствии с требованиями по защите информации;
- освоение методов, способов и средств развертывания, конфигурирования вычислительные сети, настраивания политики безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применения отечественных и зарубежных стандартов в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- изучение типовых криптографических алгоритмов.

В результате освоения дисциплины «Безопасность операционных систем Linux» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:
знать:
- принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах;
уметь:
- развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
владеть:
- навыками использования типовых криптографических алгоритмов.

Обучение по дисциплине «Безопасность операционных систем Linux» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях;	ИОПК-1.2.1. Знает принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах; ИОПК-1.2.2. Умеет развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки

	защищенности компьютерных систем; ИОПК-1.2.3. Владеет навыками использования типовых криптографических алгоритмов.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность операционных систем Linux» относится к числу учебных дисциплин обязательной части (Б1.1) основной образовательной программы (Б1.31).
Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Безопасность операционных систем Windows», «Безопасность сетей электронных вычислительных машин».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, т.е. 144 часов (лабораторные занятия – 72 часа, самостоятельная работа – 72 часа, форма контроля – экзамен, курсовой проект) в 4 семестре.
Структура и содержание дисциплины «Безопасность операционных систем Linux» по срокам и видам работы отражены в п. 3.2

3.1Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			4	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**72**	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		Экзамен	
	Курсовой проект		+	
	Итого	**144**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1.						
1.1	Тема 1. Устройство ОС Linux.	28			14		14
1.2	Тема 2. Работа с командной строкой, программирование на Bash.	28			14		14
1.3	Тема 3. Механизмы разграничения прав доступа в ОС Linux.	28			14		14
1.4	Тема 4. Сетевая подсистема ОС Linux.	28			14		14
1.5	Тема 5. Мониторинг событий, СОВ и аудит ОС Linux.	32			16		16
	Итого	**144**			**72**		**72**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3. Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1	
1.1	Устройство ОС Linux.	Работа с оборудованием, управление устройствами в Linux. Процесс загрузки Linux. Инициализация sysV, systemd, upstart. Подсистема инициализации и управления службами systemd. Загрузчики Linux. Управление библиотеками в Linux. Управление пакетами в Redhat-подобных и в Debian - подобных ОС. Работа с жесткими дисками: создание и форматирование разделов жесткого диска, управление квотами дисков. Структура файловой системы ОС Linux. Проверка файловой системы, монтирование и демонтирование. Мягкие и жесткие ссылки. Поиск и расположение команд и файлов в LINUX.
1.2	Работа с командной строкой, программирование на Bash.	Понятие командной оболочки, настройка, переменные среды, алиасы. Работа с процессами в Linux, приоритеты процессов. Работа в командной строке Linux: текстовые потоки, операции с файлами и директориями, использование потоков, конвейеров и перенаправлений. Программирование

		на Bash: переменные, условные операторы; массивы, циклы; входные параметры, функции. Регулярные выражения: общий принцип, обработка файлов формата csv.
1.3	Механизмы разграничения прав доступа в ОС Linux.	Процесс аутентификации пользователей в ОС Linux, PAM-аутентификация. Управление учетными записями пользователей и групп, их свойствами. Механизм проверки прав доступа у субъекта к объекту. Владельцы папок и файлов, права доступа к файлам и папкам, маска создания файлов и папок. SUID SGID STICKY биты. Структуры потоков и процессов. Механизм контейнеризации процессов cgroups. Система принудительного контроля доступа SELinux, AppArmor. Классификация уязвимостей ОС Linux.
1.4	Сетевая подсистема ОС Linux.	Сети: IPv4 адреса и маски подсетей, классовая и без классовая адресации, стек TCP/IP, сетевые порты и службы, протокол IPv6. Конфигурационные файлы сети, ручная настройка сети, утилиты настройки сети, управление сетевыми демонами. Сетевая маршрутизация в ОС Linux, инструменты диагностики сети, настройка клиента DNS. Настройка и использование межсетевых экранов в ОС Linux. Протокол FTP/SFTP: механизм работы, настройка безопасного FTP/SFTP-сервера. Протокол ssh: механизм работы, настройка безопасного ssh-сервера. VPN. Туннелирование сессий и портов, шифрование файлов. Протокол IPSec: туннельный и транспортный режимы. Построение защищенного канала связи. Введение в git, развертывание локального git-сервера.
1.5	Мониторинг событий, СОВ и аудит ОС Linux.	Планировщики задач cron, anacron: синтаксис и расположение файлов, пользовательские и системные задания, списки доступа. Журналирование событий: syslog, rsyslog, syslog-ng, journal, logrotate. Мониторинг сети с помощью ELK-стека: настройка и использование. Анализ защищенности ELK-стека. Системы обнаружения вторжений (СОВ), настройка и использование СОВ Snort. Аудит системы с помощью auditd: настройка и применение. Использование и настройка средства контейнеризации Docker на основе ОС Linux.

3.4Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение лабораторной работы №1 по теме 1	8
2	Выполнение лабораторной работы №2 по теме 1	6
3	Выполнение лабораторной работы №3 по теме 2	6
4	Выполнение лабораторной работы №4 по теме 2	8
5	Выполнение лабораторной работы №5 по теме 3	8
6	Выполнение лабораторной работы №6 по теме 3	6
7	Выполнение лабораторной работы №7 по теме 4	4
8	Выполнение лабораторной работы №8 по теме 4	6
9	Выполнение лабораторной работы №9 по теме 4	4
10	Выполнение лабораторной работы №10 по теме 5	16
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом запланировано, темы курсовых работ:

1. Анализ операционных систем беспроводных точек доступа.
2. Развертывание централизованной системы сбора логов на базе решения ELK-стека.
3. Методы обхода аутентификации в ОС Linux.
4. Включение в корпоративную сеть под управлением Microsoft Active Directory серверов на базе ОС Linux.
5. Выделение памяти и ее использование в ОС Linux.
6. Разработка программного обеспечения в области аудита ОС Linux.
7. Построение защищенного канала связи на базе IPSec.
8. Методы сокрытия следов несанкционированного доступа в ОС Linux.
9. Развертывание и настройка системы обнаружения вторжений Snort.
10. Настройка и использование средства контейнеризации Docker на основе ОС Linux.
11. Устройство виртуальной памяти ОС Linux.
12. Средства отладки ядра ОС Linux.
13. Анализ безопасности ОС Linux.
14. Развертывание централизованного сервера сбора системных логов.
15. Настройка и безопасная конфигурация сервера Apache.
16. Настройка и безопасная конфигурация сервера NGINX.
17. Межсетевой экран в ОС Linux: средства фильтрации сетевого трафика.
18. Программирование на bash: автоматизация мониторинга диска.
19. Программирование на bash: настройка фильтрации папок и файлов в сети на основе регулярных выражений.
20. Настройка безопасного SMTP-сервера в ОС Linux.
21. Антивирусы Linux.
22. Артефакты, оставляемые в результате НСД в ОС Ubuntu.
23. Артефакты, оставляемые в результате НСД в ОС Cesntos.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность».

4.2 Основная литература

1. «Bash и кибербезопасность. Атака, защита и анализ из командной строки», авторы: Олбинг Карл, Тронкон Пол, url: https://www.ozon.ru/product/bash-i-kiberbezopasnost-ataka-zashchita-i-analiz-iz-komandnoy-stroki-linux-olbing-karl-tronkon-pol-211432367
2. «Ядро Linux», автор: Д. Бовет, url: https://www.livelib.ru/book/1000289082-yadro-linux-d-bovet
3. «Безопасность Linux. Руководство администратора по системам защиты с открытым исходным кодом», автор: Скотт Манн, url: https://www.ozon.ru/product/bezopasnost-linux-rukovodstvo-administratora-po-sistemam-zashchity-s-otkrytym-ishodnym-kodom-1472334

4.3 Дополнительная литература

1. «Linux глазами хакера. 6-е изд.», автор: Фленов Михаил Евгеньевич, url: https://www.ozon.ru/product/linux-glazami-hakera-6-e-izd-flenov-mihail-evgenevich-242310026

4.4 Электронные образовательные ресурсы

1. ЭОР «Безопасность операционных систем Linux» [Электронный ресурс] — URL: https://online.mospolytech.ru/course/view.php?id=9267 (дата обращения: 18.02.2023).

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Дистрибутив ОС Centos7, Ubuntu 20.04
3. Дистрибутив ОС Kali Linux

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Документация CentOS [Электронный ресурс] — URL: https://docs.centos.org/en-US/docs/ (дата обращения: 18.02.2023).
2. Документация Ubuntu [Электронный ресурс] — URL: https://help.ubuntu.com/ (дата обращения: 18.02.2023).

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.
Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.
В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопрос для проведения экзамена по дисциплине:
1. Работа с оборудованием, управление устройствами в Linux.
2. Процесс загрузки Linux. Инициализация sysV, systemd, upstart.
3. Подсистема инициализации и управления службами systemd.
4. Загрузчики Linux. Управление библиотеками в Linux. Управление пакетами в Redhat-подобных и в Debian - подобных ОС.
5. Работа с жесткими дисками: создание и форматирование разделов жесткого диска, управление квотами дисков.

6. Структура файловой системы ОС Linux. Проверка файловой системы, монтирование и демонтирование. Мягкие и жесткие ссылки. Поиск и расположение команд и файлов в LINUX.
7. Понятие командной оболочки, настройка, переменные среды, алиасы.
8. Работа с процессами в Linux, приоритеты процессов.
9. Работа в командной строке Linux: текстовые потоки, операции с файлами и директориями, использование потоков, конвейеров и перенаправлений.
10. Программирование на Bash: переменные, условные операторы; массивы, циклы; входные параметры, функции.
11. Регулярные выражения: общий принцип, обработка файлов формата csv.
12. Процесс аутентификации пользователей в ОС Linux, PAM-аутентификация.
13. Управление учетными записями пользователей и групп, их свойствами.
14. Механизм проверки прав доступа у субъекта к объекту. Владельцы папок и файлов, права доступа к файлам и папкам, маска создания файлов и папок. SUID SGID STICKY биты.
15. Структуры потоков и процессов.
16. Механизм контейнеризации процессов cgroups.
17. Система принудительного контроля доступа SELinux, AppArmor.
18. Классификация уязвимостей ОС Linux.
19. Сети: IPv4 адреса и маски подсетей, классовая и без классовая адресации, стек TCP/IP, сетевые порты и службы, протокол IPv6.
20. Конфигурационные файлы сети, ручная настройка сети, утилиты настройки сети, управление сетевыми демонами.
21. Сетевая маршрутизация в ОС Linux, инструменты диагностики сети, настройка клиента DNS.
22. Настройка и использование межсетевых экранов в ОС Linux.
23. Протокол FTP/SFTP: механизм работы, настройка безопасного FTP/SFTP-сервера.
24. Протокол ssh: механизм работы, настройка безопасного ssh-сервера.
25. VPN. Туннелирование сессий и портов, шифрование файлов.
26. VPN. Протокол IPSec: туннельный и транспортный режимы. Построение защищенного канала связи.
27. Введение в git, развертывание локального git-сервера.
28. Планировщики задач cron, anacron: синтаксис и расположение файлов, пользовательские и системные задания, списки доступа.
29. Журналирование событий: syslog, rsyslog, syslog-ng, journal, logrotate.
30. Мониторинг сети с помощью ELK-стека: настройка и использование.
31. Системы обнаружения вторжений (СОВ), настройка и использование СОВ Snort.
32. Аудит системы с помощью auditd: настройка и применение.
33. Использование и настройка средства контейнеризации Docker на основе ОС Linux.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Безопасность операционных систем Linux
Бакалавры. Курс 2, семестр 2

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Система принудительного контроля доступа SELinux, AppArmor.
2. Понятие командной оболочки, настройка, переменные среды, алиасы.

Преподаватель _____ / Шипулин Г.Ф. /