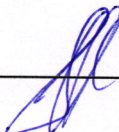


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г, протокол № 8
Исполняющий обязанности
заведующего кафедрой

 Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.В.ДВ.01.01 Защита конфиденциальной информации в организации

Направление подготовки

10.03.01 Информационная безопасность

профиль

Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования

БАКАЛАВРИАТ

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС–2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	<p>ПКС-2.1 Знать способы решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.</p> <p>ПКС-2.2 Уметь решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации</p> <p>ПКС-2.3 Иметь навыки решения задач профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации</p>
ПКС–3	Способен осуществлять управление средствами защиты информации, в том числе осуществляющими непрерывный мониторинг защищенности автоматизированных систем	<p>ПКС-3.1 Знать программно-аппаратные средства защиты информации, современные подходы к разработке и эксплуатации автоматизированных систем, средства управления и защиты автоматизированных систем.</p> <p>ПКС-3.2 Уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска), в том числе средства, осуществляющие непрерывный мониторинг защищенности автоматизированных систем.</p> <p>ПКС-3.3 Владеть навыками выбора программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</p>

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Тема 1. Введение в организацию конфиденциального	ПКС-2 ПКС-3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к

	делопроизводства и защиты коммерческой тайны		зачету
2	Тема 2 Жизненный цикл конфиденциального документа	ПКС-2 ПКС-3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
3	Тема 3 Программные средства защиты конфиденциальной информации	ПКС-2 ПКС-3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
4	Тема 4 Технические средства защиты конфиденциальной информации	ПКС-2 ПКС-3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету

Лабораторный практикум

Лабораторная работа «Изучение функциональных возможностей межсетевого экрана Netfilter»

Цель работы: Научиться пользоваться основными функциональными возможностями программы Netfilter.

Межсетевой экран — это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой firewall. Межсетевой экран позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Самым популярным межсетевым экраном для OS Linux на текущий момент является Netfilter. Русскоязычное руководство по администрированию межсетевого экрана Netfilter с помощью утилиты iptables доступно по адресу.

Выполнение:

1. Запустите виртуальную машину Ubuntu. Определить настройки протокола TCP/IP Вашего компьютера с помощью команды ifconfig. Сделайте экранный снимок сетевых настроек.
2. Для использования утилиты iptables требуются привилегии суперпользователя (root). В консоли введите команду su root и далее пароль суперпользователя.
3. Установите политику по умолчанию ACCEPT для цепочек INPUT, FORWARD и OUTPUT. В отчет вставьте введенные правила.
4. Закройте порт 80 цепочки INPUT для всех IP адресов. Остальные порты цепочки INPUT должны быть открыты. В отчет вставьте введенные правила. Перейдите в браузере по адресу <http://localhost/>. Проанализируйте в Wireshark какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки INPUT.
5. Закройте порт 80 цепочки INPUT только для одного выбранного IP адреса. Для всех остальных IP адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.
6. Закройте порт 80 цепочки OUTPUT для всех IP адресов. Остальные порты цепочки OUTPUT должны быть открыты. В отчет вставьте введенные правила. Перейдите в браузере по адресу <http://localhost/>. Проанализируйте в Wireshark какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки OUTPUT.
7. Закройте порт 80 цепочки OUTPUT только для одного выбранного IP адреса. Для всех остальных IP-адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.

8. Откройте возможность работы с локальным Web-сервером только Вашему компьютеру. Все остальные IP адреса не должны иметь доступ к Web-серверу компьютера. В отчет вставьте введенные правила.
9. Заблокируйте с помощью межсетевого экрана выбранные Вами Web-сайты. В отчет вставьте введенные правила.
10. Ограничьте количество возможных подключений к 22 порту openssh сервера (не более 3-х подключений в минуту). Проверку осуществляйте путем 4-х подключений подряд, вбивая в консоль команду `ssh localhost`. В отчет вставьте введенные правила.
11. Ограничьте количество запросов на 80 порт в секунду/минуту от одного пользователя. Проверку правильности правила осуществляйте с помощью команды `"ab -n 10000 -c 100 http://localhost/"`. В отчет вставьте введенные правила.
12. Выполните шаги 4-11, установив политику по умолчанию DROP для цепочек INPUT, FORWARD и OUTPUT (подсказка: правила придется переписать и использовать состояние соединения NEW и ESTABLISHED).
13. Заблокируйте доступ к локальному Web-серверу пользователю с заданным MAC-адресом. В отчет вставьте введенное правило.
14. Удалите любое выбранное правило из цепочки INPUT. В отчет вставьте введенное правило.
15. Продемонстрируйте возможности межсетевого экрана Netfilter по логированию сетевых пакетов. В отчет вставьте полученный лог и введенные правила.

Тестовые задания

- 1) К правовым методам, обеспечивающим информационную безопасность, относятся:
 - а) Разработка аппаратных средств обеспечения правовых данных
 - б) Разработка и установка во всех компьютерных правовых сетях журналов учета
 - в) действий
 - г) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
- 2) Основными источниками угроз информационной безопасности являются:
 - а) Хищение жестких дисков, подключение к сети, инсайдерство
 - б) Перехват данных, хищение данных, изменение архитектуры системы
 - в) Хищение данных, подкуп системных администраторов, нарушение регламента работы
- 3) Виды информационной безопасности:
 - а) Персональная, корпоративная, государственная
 - б) Клиентская, серверная, сетевая
 - в) Локальная, глобальная, смешанная
- 4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
 - а) Несанкционированного доступа, воздействия в сети
 - б) Инсайдерства в организации
 - в) Чрезвычайных ситуаций
- 5) Основные объекты информационной безопасности:
 - а) Компьютерные сети, базы данных
 - б) Информационные системы, психологическое состояние пользователей
 - в) Бизнес-ориентированные, коммерческие системы
- 6) Основными рисками информационной безопасности являются:
 - а) Искажение, уменьшение объема, перекодировка информации
 - б) Техническое вмешательство, выведение из строя оборудования сети
 - в) Потеря, искажение, утечка информации
- 7) К основным принципам обеспечения информационной безопасности относится:
 - а) Экономической эффективности системы безопасности

- б) Многоплатформенной реализации системы
 - в) Усиления защищенности всех звеньев системы
- 8) Основными субъектами информационной безопасности являются:
- а) руководители, менеджеры, администраторы компаний
 - б) органы права, государства, бизнеса
 - в) сетевые базы данных, брандмауэр
- 9) К основным функциям системы безопасности относят:
- а) Установление регламента, аудит системы, выявление рисков
 - б) Установка новых офисных приложений, смена хостинг-компаний
 - в) Внедрение аутентификации, проверки контактных данных пользователей
- 10) Принципом информационной безопасности является принцип недопущения:
- а) Неоправданных ограничений при работе в сети (системе)
 - б) Рисков безопасности сети, системы
 - в) Презумпции секретности
- 11) Принципом политики информационной безопасности является принцип:
- а) Невозможности миновать защитные средства сети (системы)
 - б) Усиления основного звена сети, системы
 - в) Полного блокирования доступа при риск-ситуациях
- 12) Принципом политики информационной безопасности является принцип:
- а) Усиления защищенности самого незащищенного звена сети (системы)
 - б) Перехода в безопасное состояние работы сети, системы
 - в) Полного доступа пользователей ко всем ресурсам сети, системы
- 13) Принципом политики информационной безопасности является принцип:
- а) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
 - б) Одноуровневой защиты сети, системы
 - в) Совместимых, однотипных программно-технических средств сети, системы
- 14) К основным типам средств воздействия на компьютерную сеть относится:
- а) Компьютерный сбой
 - б) Логические закладки («мины»)
 - в) Аварийное отключение питания
- 15) Когда получен спам по e-mail с приложенным файлом, следует:
- а) Прочитать приложение, если оно не содержит ничего ценного – удалить
 - б) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
 - в) Удалить письмо с приложением, не раскрывая (не читая) его
- 16) Принцип Кирхгофа:
- а) Секретность ключа определена секретностью открытого сообщения
 - б) Секретность информации определена скоростью передачи данных
 - в) Секретность закрытого сообщения определяется секретностью ключа
- 17) ЭЦП – это:
- а) Электронно-цифровой преобразователь
 - б) Электронно-цифровая подпись
 - в) Электронно-цифровой процессор
- 18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- а) Покупка нелегального ПО
 - б) Ошибки эксплуатации и неумышленного изменения режима работы системы
 - в) Сознательного внедрения сетевых вирусов
- 19) Наиболее распространены угрозы информационной безопасности сети:
- а) Распределенный доступ клиент, отказ оборудования
 - б) Моральный износ сети, инсайдерство
 - в) Сбой (отказ) оборудования, нелегальное копирование данных
- 20) Наиболее распространены средства воздействия на сеть офиса:

- а) Слабый трафик, информационный обман, вирусы в интернет
 - б) Вирусы в сети, логические мины (закладки), информационный перехват
 - в) Компьютерные сбои, изменение администрирования, топологии
- 21) Утечкой информации в системе называется ситуация, характеризующаяся:
- а) Потерей данных в системе
 - б) Изменением формы информации
 - в) Изменением содержания информации
- 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- а) Целостность
 - б) Доступность
 - в) Актуальность
- 23) Угроза информационной системе (компьютерной сети) – это:
- а) Вероятное событие
 - б) Детерминированное (всегда определенное) событие
 - в) Событие, происходящее периодически
- 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- а) Регламентированной
 - б) Правовой
 - в) Защищаемой
- 25) Разновидностями угроз безопасности (сети, системы) являются:
- а) Программные, технические, организационные, технологические
 - б) Серверные, клиентские, спутниковые, наземные
 - в) Личные, корпоративные, социальные, национальные
- 26) Полную ответственность за защищенность компьютерной сети несет:
- а) Владелец сети
 - б) Администратор сети
 - в) Пользователь сети
- 27) Политика безопасности в системе (сети) – это комплекс:
- а) Руководств, требований обеспечения необходимого уровня безопасности
 - б) Инструкций, алгоритмов поведения пользователя в сети
 - в) Нормы информационного права, соблюдаемые в сети
- 28) Наиболее важным при реализации защитных мер политики безопасности является:
- а) Аудит, анализ затрат на проведение защитных мер
 - б) Аудит, анализ безопасности
 - в) Аудит, анализ уязвимостей, риск-ситуаций

Примерный перечень вопросов к зачету (6 семестр)

1. Законодательная сторона защиты конфиденциальной информации в организации.
2. Иерархия законодательных органов, порядок создания законов и подзаконных актов, область действия по времени и месту.
3. Охраняемые сведения, понятия тайны и ее виды применительно к различным организациям.
4. Основные законы, связанные с конфиденциальным делопроизводством.
5. Организация конфиденциального делопроизводства.
6. Особенности организации конфиденциального делопроизводства с использованием электронного документооборота.
7. ФСБ, ФСТЭК, Роскомнадзор, Роспатент и другие организации, являющиеся регуляторами по отношению к вопросам конфиденциального делопроизводства.

8. Путь конфиденциального делопроизводства от создания до уничтожения.
9. Составление номенклатур, формирование и оформление конфиденциальных дел.
10. Подготовка конфиденциальных документов для архивного хранения и уничтожения.
11. ГОСТ Р 51275-2006 защиты информации.
12. Защита конфиденциальной информации при ее передаче по сети.
13. Система защищенного электронного документооборота.
14. Основные задачи, решаемые системами электронного документооборота.
15. Электронно-цифровая подпись.
16. Антивирусная защита.
17. Межсетевые экраны как средство защиты от несанкционированного доступа.
18. Криптографические средства.
19. Сканеры уязвимостей.
20. Системы обнаружения атак.
21. Парольная защита.
22. Идентификация и аутентификация.
23. Модели разграничения доступа к информационным системам и ресурсам.
24. Виды электронной подписи и принципы использования.
25. Удостоверяющие центры и сертификат ключа.
26. Квалифицированный сертификат.
27. Общетехнические средства контроля физического доступа к конфиденциальной информации.
28. Разрешительная система доступа к конфиденциальной информации.
29. Санкционированный и несанкционированный доступ.
30. Электронные ключи и замки.
31. Биометрические системы аутентификации.
32. Система видеонаблюдения.
33. Система охраны периметра.

Составитель
«12» марта 2024 г.



к.п.н., доцент Корнева О.С.