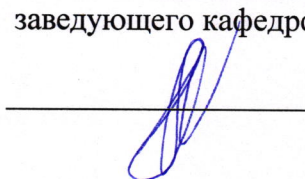


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сахалинский государственный университет»

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. О.31 Безопасность компьютерных сетей

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

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

Квалификация

бакалавр

Форма обучения

очная

Южно-Сахалинск
2024 г.

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

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы
ОПК-4.4	ОПК-4.4. Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации; ОПК-4.4.2 - Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, а также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы; ОПК-4.4.3 - Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств.

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. Основы безопасности компьютерных сетей. Основные понятия и терминология, угрозы, уязвимости, атаки	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции
2.	Тема 2. Основы безопасности компьютерных сетей. Нормативно-правовое обеспечение информационной безопасности КС	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции .
3.	Тема 3 Основы безопасности компьютерных сетей. Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции
4.	Тема 4 Основы безопасности компьютерных сетей. Сетевые атаки, модель Cyber-Kill Chain	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции
5.	Тема 5 Средства обеспечения безопасности компьютерных сетей. Фильтрация сетевого трафика, межсетевые экраны, NGFW	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
6.	Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
7.	Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
8.	Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
9.	Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
10.	Тема 10 Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания
11.	Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы	ОПК-4.3, ОПК-4.4	Устный опрос по теме лекции Выполнение практического задания

3. Оценочные средства

Форма контроля для очной формы обучения – **зачет**

Примеры заданий для текущего контроля и промежуточных заданий по различным темам:

Примерный перечень заданий

Задание 1

1. Изучить теоретический материал по межсетевым экранам
2. Изучить возможности межсетевого экрана, встроенного в операционную систему Windows.
3. Включить межсетевой экран на рабочей станции
4. Заблокировать Общий доступ к файлам и принтера на рабочей станции средствами Межсетевого экрана Windows
5. Разблокировать Общий доступ к файлам и принтерам, разрешить сетевой доступ только для рабочих станций локальной сети
6. Отключить межсетевой экран на одном из интерфейсов. Проверить результат

7. Задать параметры журнала безопасности. Просмотреть журнал безопасности, найти в журнале безопасности записи о попытках подключения к рабочей станции
8. Заблокировать возможность работы программы FAR Manager с ресурсами сети
9. Разблокировать возможность работы с сетью ранее заблокированной программы

Задание 2

Необходимо создать несколько политик безопасности IP для решения следующих задач:

1. Политика для клиента сети, разрешающая только защищенное (шифрование и поддержка целостности) обращение к любому http серверу.
2. Политика для клиента сети, разрешающая защищенное (шифрование) обращение к локальному http серверу с адресом 192.168.24.1 и не защищенные обращения к другим http и ftp серверам.
3. Политика для сервера сети, разрешающая только защищенные (поддержка целостности) обращения из локальной сети и незащищенные обращения от остальных станций по любому протоколу.
4. Политика для сервера сети, разрешающая только защищенные (шифрование и поддержка целостности) обращения по протоколам POP3 и SMTP с любой станции.
5. Политика безопасного (шифрование и поддержка целостности) соединения двух серверов. Остальные соединения не защищенные.

Задание 3

1. Изучить принципы разграничения доступа пользователей к файлам в операционной системе Linux
2. Зарегистрировать двух пользователей в операционной системе. Зарегистрировать новую группу пользователей. Включить новых пользователей в созданную группу.
3. Изменить права доступа, назначенные на рабочие папки пользователей по умолчанию, так чтобы один из пользователей мог входить в рабочую папку другого пользователя и выполнять некоторые действия с файлами, а второй пользователь не мог входить в рабочую папку первого пользователя
4. Изучить принципы настройки межсетевого экрана ipfw, встроенного в операционную систему Linux
5. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться только из локальной сети
6. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться по протоколам HTTP, SMTP и POP3 из любой точки Интернета
7. Настроить межсетевой экран таким образом, чтобы запросы, пришедшие на определенный сетевой интерфейс передавались другому компьютеру в локальной сети
8. Настроить параметры межсетевого экрана таким образом, чтобы с данного компьютера можно было подключаться только по протоколам HTTP и SSH к другим компьютерам сети Интернет

Задание 4

1. Изучить принципы защиты сетевых взаимодействий на прикладном уровне
2. Установить и настроить Центр сертификации Microsoft Windows
3. Изготовить ключи и выпустить сертификат открытого ключа для двух пользователей
4. Настроить программу Outlook Express (или другую почтовую программу) на использование ключей защиты
5. Осуществить обмен электронными письмами, защищенными с помощью электронно-цифровой подписи и шифрования. Проверить правильность подписи у каждого пользователя
6. Изготовить ключи и выдать сертификаты, необходимые для защищенного взаимодействия с веб-сервером сети

7. В программе Диспетчер IIS на сервере настроить веб-сервер, который поддерживает защищенное взаимодействие с клиентами Интернета
8. На рабочей станции настроить программу Internet Explorer для защищенного взаимодействия с веб-сервером. Осуществить подключение к защищенному веб-серверу и просмотреть доступные на нем страницы.

Примерный перечень тестовых заданий

1. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?
 - а) использовать систему обнаружения вторжений
 - б) переименовать учетную запись администратора
 - в) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации
 - г) использовать мультифакторную аутентификацию
2. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?
 - а) система обнаружения вторжений
 - б) персональный межсетевой экран
 - в) трансляция сетевых адресов
 - г) антивирусное программное обеспечение
3. Какое из средств защиты используется для мониторинга сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности?
 - а) межсетевой экран
 - б) система анализа защищенности
 - в) система предотвращения вторжений
 - г) средство антивирусной защиты
4. Как называется процесс защиты ресурсов сети от несанкционированного использования?
 - а) охрана оборудования сети
 - б) защита ядра безопасности
 - в) контроль доступа
 - г) защита периметра безопасности
5. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?
 - а) создать диапазон IP адресов
 - б) создать параметр DHCP
 - в) создать исключение для IP адреса г) создать область DHCP

6. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?
- а) сетевой доступ
 - б) папка
 - в) каталог
 - г) домен
7. Какой протокол используется для доступа к службе каталогов Active Directory?
- а) ShareDiscovery б) ADSL
 - б) LDAP
 - в) ICMP
8. Как называется компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам?
- а) хаб
 - б) рабочая станция
 - в) сервер
 - г) хост
9. В каком методе передачи данные пересылаются в двух направлениях одновременно?
- а) симплексный
 - б) синхронный
 - в) дуплексный
 - г) полудуплексный
10. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?
- а) синхронном
 - б) асинхронном
 - в) туннельном
 - г) транспортном

Примерные вопросы к зачету

1. Перехват информации в сети. Инструменты. Способы противодействия перехвату.
2. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.
3. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.
4. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.
5. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.
6. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.
7. Демилитаризованная зоны. Назначение. Способы выделения.
8. Классификация межсетевых экранов согласно нормативных документов ФСТЭК России. Применение межсетевых экранов различных классов.

9. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки. Понятие сети. Требования, предъявляемые к сети.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,5	1	8	16
Подготовка к занятию, выполнение домашнего задания	0,5	1	8	16
выполнение практических заданий по темам	3	5	27	45
Промежуточная аттестация (зачет)	10	23	10	23
Итого за семестр			53	100

Система оценивания планируемых результатов обучения

Оценка «зачтено» выставляется,

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту твердо знающему программный материал, грамотно и по существу излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания

Составитель


(подпись)

Филиппова
преподаватель
информатики

Г.В., старший
кафедры

«12 » марта 2024 г