Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:53
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании
Высшей школы интеллектуальных систем и кабертехнологий

Протокол от 06.09.2024 № 2

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств) для проведения промежуточной аттестации
по дисциплине

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриат**

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»
наименование образовательной программы

10.03.01 «Информационная безопасность»
шифр, наименование направления подготовки / специальности

Составитель Яницкая Т.С., доцент ВШИСиКТ, к.т.н., доцент
ФИО, должность, структурное подразделение,
учёная степень, учёное звание

Тольятти
2024

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности
ПК-6	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИПК-6.2. Работает с программным обеспечением с соблюдением действующих требований по защите информации

В результате изучения дисциплины обучающийся должен:

Владеть: методами выявления угроз, средствами контроля доступа, инструментами мониторинга, технологиями шифрования и практиками защиты сетевой инфраструктуры

Уметь: настраивать средства защиты сети, конфигурировать AAA, ACL, IPS, VPN и межсетевые экраны, анализировать угрозы и тестировать безопасность.

Знать: принципы сетевой безопасности, методы защиты устройств, механизмы аутентификации, авторизации и учёта, работу межсетевых экранов, IPS, VPN и криптографических систем.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Тема 1. Современные угрозы сетевой безопасности	ОПК-10 ПК-6
2.	Тема 2. Обеспечение безопасности сетевых устройств	
3.	Тема 3. Аутентификация, авторизация и учет	
4.	Тема 4. Внедрение технологий межсетевого экрана	
5.	Тема 5. Внедрение системы предотвращения вторжений	
6.	Тема 6. Обеспечение безопасности локальной сети (LAN)	
7.	Тема 7. Криптографические системы	
8.	Тема 8. Внедрение виртуальных частных сетей (VPN)	
9.	Тема 9. Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance	
10.	Тема 10. Многофункциональное устройство обеспечения безопасности Cisco ASA с расширенным функционалом	
11.	Тема 11. Управление безопасной сетью	

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине –зачёт.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
		70-85,9	«хорошо» / 4	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Вопросы для подготовки к зачёту

№	Содержание вопроса
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	
1.	Какие критерии используются для фильтрации трафика?
2.	Какой метод аутентификации используется для доступа к сетевым устройствам?
3.	Какую задачу выполняют административные роли?
4.	Какой протокол используется для мониторинга устройств?
5.	Какой протокол используют для централизованной аутентификации AAA?
6.	Какой тип межсетевого экрана отслеживает состояние соединений?
7.	Какой командой можно настроить SNMP на маршрутизаторе?
8.	Какой инструмент можно использовать для тестирования безопасности сети? a) Nmap) b) DHCP-сервер c) FTP-клиент d) SNMP
9.	Какой из перечисленных методов относится к пассивным атакам на сеть? a) Перехват трафика) b) SQL-инъекция c) DDoS-атака d) Внедрение вредоносного кода
10.	Что представляет собой двухфакторная аутентификация? a) Использование двух различных методов подтверждения личности) b) Использование двух паролей c) Аутентификация через VPN-соединение d) Применение сложных паролей
11.	Какой механизм безопасности относится к методам защиты оконечных устройств? a) Антивирусное ПО) b) NAT c) Межсетевой экран d) MAC-фильтрация
12.	Какую функцию выполняет протокол IPsec в VPN-сетях? a) Обеспечивает конфиденциальность и целостность данных) b) Назначает IP-адреса клиентам c) Управляет пропускной способностью сети d) Перенаправляет трафик через прокси-сервер
13.	Какое утверждение о межсетевых экранах верно? a) Они фильтруют трафик на основе заранее заданных правил) b) Они работают только на уровне приложения c) Они не могут анализировать состояние соединений d) Они заменяют антивирусные решения
14.	Какой инструмент можно использовать для тестирования безопасности сети? a) Nmap) b) DHCP-сервер c) FTP-клиент d) SNMP
ПК-6 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
15.	Какой командой можно отключить службу восстановления паролей?
16.	Какую команду используют для обновления списка доступа?
17.	Какой командой можно просмотреть таблицу маршрутизации?
18.	Какой командой можно установить ACL на интерфейс?
19.	Какой командой можно проверить состояние доступа к VTY-портам?

№	Содержание вопроса
20.	Какая команда позволяет настроить SSH на маршрутизаторе?
21.	Какую команду следует использовать для генерации RSA-ключей?
22.	Что будет отключено при выполнении команды no service password-recovery?
23.	Какой из следующих алгоритмов используется для симметричного шифрования? a) AES) b) RSA c) ECC d) SHA-256
24.	Что из перечисленного относится к серверному решению AAA? a) RADIUS) b) VPN c) DHCP d) NAT
25.	Какую роль выполняет Security Device Manager в ASA? a) Обеспечивает графический интерфейс для управления устройством) b) Увеличивает скорость передачи данных c) Фильтрует трафик на уровне 2 d) Управляет маршрутизацией трафика
26.	Какой из следующих протоколов обеспечивает шифрование данных в VPN-сетях? a) IPsec) b) HTTP c) FTP d) SMTP
27.	Что из перечисленного является основным компонентом технологии IPS? a) Сигнатуры) b) VPN-туннели c) NAT d) VLAN
28.	Какой алгоритм используется для генерации открытого и закрытого ключей? a) RSA) b) MD5 c) SHA-1 d) DES
29.	Какую функцию выполняет сервер TACACS+? a) Аутентификация, авторизация и учет пользователей) b) Управление межсетевым экраном c) Мониторинг сети d) Динамическое распределение IP-адресов
30.	Какой принцип лежит в основе зональных межсетевых экранов? a) Разделение сети на зоны с различными уровнями доверия) b) Анализ поведения пользователей c) Шифрование данных d) Использование NAT
31.	Какой механизм защиты используется для предотвращения атак с подделкой MAC-адресов? a) Port Security) b) ACL c) NAT d) VPN