МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И.Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н.Ульянова»)

Факультет информатики и вычислительной техники
Кафедра математического и аппаратного обеспечения информационных систем

УТВЕРЖДЕНЫ
на заседании кафедры
05 ноября 2024 г., протокол № 4
Заведующий кафедрой

Т.Н. Копышева

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине (модулю)
«Методы и системы защиты информации, информационная безопасность»

Научная специальность – 2.3.6. Методы и системы защиты информации, информационная безопасность
Форма обучения – очная
Год начала освоения – 2022

Чебоксары – 2024

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Заведующий кафедрой математического
и аппаратного обеспечения
информационных систем, к.ф.-м.н., доцент
Т.Н. Копышева

СОГЛАСОВАНО:
Декан факультета А.В. Щипцова

1. **Паспорт оценочных материалов по дисциплине (модулю).**

№ п/п	Контролируемые разделы (темы) дисциплины	Контролируемые результаты освоения дисциплины (модуля)	Наименование оценочного средства
Семестр 3			
Раздел 1. Принципы комплексного обеспечения ИБ. Архитектура защищенной сети. Контроль доступа.			
1.	Тема 1. Принципы комплексного обеспечения ИБ.	К7, К8, К9	Вопросы для проведения устного вопроса, вопросы к зачету, экзаменационные вопросы
2.	Тема 2. Архитектура защищенной сети	К7, К8, К9	Вопросы для проведения устного вопроса, вопросы к зачету, экзаменационные вопросы
3.	Тема 3. Контроль доступа	К7, К8, К9	Вопросы для проведения устного вопроса, вопросы к зачету, экзаменационные вопросы
Семестр 4			
Раздел 2. Управление угрозами ИБ. Управление инцидентами			
5.	Тема 4. Управление угрозами ИБ	К7, К8, К9	Вопросы для проведения устного вопроса, вопросы к зачету, экзаменационные вопросы
6.	Тема 5. Управление инцидентами	К7, К8, К9	Вопросы для проведения устного вопроса, вопросы к зачету, экзаменационные вопросы

В процессе освоения данной дисциплины, обучающиеся формируют следующие результаты освоения дисциплины:

К7 – способность к разработке научных основ, принципиально новых методов анализа и синтеза, научных подходов и технических принципов создания систем защиты информации и информационной безопасности;

К8 – способность самостоятельно исследовать свойства и создавать алгоритмы для методов и систем защиты информации;

К9 – способность использовать в профессиональной деятельности современные языки программирования, базы данных, операционные системы, электронные библиотеки и пакеты математических и специализированных программ, сетевые технологии, а также

умение применять новые поколения программного и аппаратного обеспечения в области математического моделирования процессов защиты информации.

2. Критерии оценки успеваемости обучающихся.

Критерии получения зачета по дисциплине (модулю):

- оценка «зачтено» ставится, если обучающийся выполнил не менее половины аудиторных контрольных работ, домашних заданий, докладов, ответил на половину вопросов к зачету;

- оценка «не зачтено» ставится, если обучающийся выполнил менее половины аудиторных контрольных работ, домашних заданий, докладов, не ответил на половину вопросов к зачету.

Критерии экзаменационной оценки:

- для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

- для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильные действия по применению знаний на практике, четкое изложение материала;

- для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

- для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

2. **Оценочные материалы текущего контроля успеваемости.**

Перечень вопросов для проведения устного вопроса.

1) Что такое эшелонированная защита
2) Что такое многоуровневая защита
3) Что такое управление рисками
4) Что такое контроль доступа
5) Что такое hardening
6) Что такое доверенные системы
7) Что такое фреймворки безопасности: Common Criteria, ISO 27000, NIST CSF, CIS Top 20, Cyber Essentials
8) Анализ сетевого траффика. Принцип работы снифферов
9) Программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других Wireshark
10) Утилита UNIX, позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа Tcpdump
11) Блокирование нежелательного трафика. Сетевые экраны
12) Блокирование нежелательного трафика. Брандмауэр Windows
13) Блокирование нежелательного трафика.
14) Гибкая утилита межсетевого экрана Iptables
15) Принцип работы систем обнаружения вторжений
16) Система обнаружения вторжений и система предотвращения вторжений на основе открытого исходного кода. Snort, Suricata
17) Платформа сетевого анализа программного обеспечения с открытым исходным

кодом Bro/Zeek
18) Принципы аутентификации
19) Принципы авторизации
20) Принципы контроля ресурсов
21) Модели управления доступом
22) Токены и биометрия
23) Парольная защита. Оценка стойкости пароля
24) Парольная защита. Хеширование
25) Парольная защита. Хранение паролей в ОС Windows, Linux
26) Утилиты подбора пароля. Атака перебором и подбором по словарю
27) Свободная программа, предназначенная для восстановления паролей по их хешам John the ripper
28) Программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов THC Hydra
29) Контроль целостности объектов файловой системы
30) Средства доверенной загрузки уровня базовой системы ввода-вывода
31) Средства доверенной загрузки уровня платы расширения
32) Средства доверенной загрузки уровня загрузочной записи
33) Технология «доверенной загрузки» Intel TXT (Trusted Execution Technology)
34) Протокол UEFI Secure Boot
35) Определения: угроза, уязвимость, инцидент
36) База данных общеизвестных уязвимостей информационной безопасности CVE, система категорий для слабых мест и уязвимостей программного обеспечения CWE, - открытый проект обеспечения безопасности веб-приложений OWASP Top 10
37) Открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы CVSS, коэффициент возврата инвестиций ROI, коэффициент возврата инвестиций ROSI
38) Банк данных угроз безопасности информации ФСТЭК
39) Анализ защищенности с применением сканеров безопасности. Видимые адреса (hping3)
40) Анализ защищенности с применением сканеров безопасности. Открытые порты (nmap)
41) Анализ защищенности с применением сканеров безопасности. Уязвимые сервисы (GVM/ScanOval/linys/Retina)
42) Инфраструктура безопасности Windows
43) Контроль доступа
44) Групповая политика безопасности
45) Управление ролями и службами
46) Архитектура безопасности Windows
47) Разграничение доступа в Linux
48) Утилиты Безопасности
49) Управление конфигурацией и службами
50) Принцип работы антивирусов
51) Правила представляют собой описание сигнатур целевых атак и вторжений в IT-инфраструктуру организации Yara rules
52) 6-шаговый процесс реагирования на инциденты
53) Матрица атак
54) Стратегии защиты
55) Мониторинг компьютерных сетей, серверов и сетевого оборудования
56) Стратегия мониторинга журналов

57) Принцип работы SIEM
58) Унифицированный формат описания правил детектирования, основанных на данных из логов Sigma Rules
59) Корпоративное решение для мониторинга безопасности с открытым исходным кодом для обнаружения угроз, мониторинга целостности, реагирования на инциденты и соответствия требованиям. Wazuh.
60) Принципы компьютерной форензики
61) Инверсия управления IOC
62) Extended Detection and Response (XDR)
63) Мониторинг артефактов Velociraptor
64) Виды и способы архивирования
65) Восстановление и уничтожение объектов файловой системы
66) Копирование дисков. Partclone, Partimage, ddrescue
67) Оперативные центры обеспечения кибербезопасности (Security Operations Center, SOC)
68) Incident Response Platform

Критерии оценки устного опроса

Развернутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях. Критериями оценивания являются:

1) полнота и правильность ответа;
2) степень осознанности, понимания изученного;
3) языковое оформление ответа.

Оценка «зачтено» ставится, если обучающийся полно излагает материал, дает правильное определение основных понятий, обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, излагает материал последовательно и правильно с точки зрения норм литературного языка.

Оценка «не зачтено» ставится, если обучающийся обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, неуверенно излагает материал. Оценка «не зачтено» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом.

4. Оценочные материалы промежуточной аттестации обучающихся.

4.1. Примерный перечень вопросов к зачету

1) Чем угроза ИБ отличается от уязвимости ИБ?
2) Дайте определение понятию риска.
3) Приведите примеры наиболее распространенных современных уязвимостей.
4) Чем отличается модель безопасности Белла-ЛаПадулы от модели дискреционного доступа (DAC)?
5) Что такое RBAC?
6) Что означает слово «криптология» и кем оно введено?
7) Какие недостатки имеют несимметричные методы шифрования перед симметричными?
8) В чем заключается проблема управления ключами?
9) Где используется стеганография?
10) В каких случаях применяется хеширование?
11) Какие существуют хеш-функции?
12) Опишите принцип работы цифровой подписи документа.

13) Опишите принципы контроля доступа.
14) Опишите принципы цифрового хранения информации.
15) Перечислите критерии оценки доверенных компьютерных систем?
16) Для чего используется БДУ ФСТЭК?
17) Опишите принципы построение системы защитных мер.
18) Опишите процедуру расследования инцидента.
19) Назовите основные угрозы физической безопасности.
20) Назовите программные средства для контроля периметра.
21) Опишите принципы работы антивируса?
22) Какие существуют виды сетевых экранов?

4.2. Перечень экзаменационных вопросов

1. Основные понятия информационной безопасности: информация, конфиденциальность, целостность, доступность, защита данных, информационная безопасность, обеспечение информационной безопасности
2. Подходы к обеспечению информационной безопасности и защиты информации.
3. Аппаратно-программные средства защиты информационных систем.
4. Организационные меры защиты информационных систем.
5. Способы выявления, идентификации, классификации угроз нарушения информационной безопасности.
6. Способы защиты от угроз информационной безопасности в открытых компьютерных сетях, включая Интернет.
7. Средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
8. Формирование комплекса средств противодействия угрозам информационной безопасности.
9. Риски нарушения информационной безопасности. Способы управления рисками.
10. Способы анализа и оценки рисков нарушения информационной безопасности.
11. Модели и методы оценки защищенности информации и информационной безопасности объекта.
12. Модели и методы оценки эффективности средств и мер обеспечения информационной безопасности.
13. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.
14. Модели и системы разграничения доступа. Политика безопасности по доступу к объектам.
15. Способы выявления и противодействия распространению ложной и вредоносной информации.
16. Политика обеспечения информационной безопасности.
17. Регламенты и правила информационной безопасности.
18. Принцип работы различных средств защиты информации и обеспечения информационной безопасности.
19. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта защиты.
20. Способы реагирования и расследования инцидентов информационной безопасности.
21. Жизненный цикл инцидентов информационной безопасности.
22. Средства мониторинга и управления инцидентами информационной безопасности.
23. Принципы разработки безопасного программного обеспечения.
24. Способы анализа дефектов безопасности (уязвимостей) программного обеспечения.

25. Понятие скрытого канала передачи и способы выявления и противодействия.
26. Выявление уязвимостей в компьютерных системах и сетях.
27. Управление обеспечением информационной безопасности, непрерывного функционирования и восстановления систем, противодействию отказу в обслуживании.
28. Криптографические алгоритмы. Криптографические протоколы.
29. Криптографические методы и средства защиты хранящихся данных.
30. Криптографические методы и средства защиты передаваемых данных по сети.
31. Нормативно-правовое обеспечение информационной безопасности.
32. Способы защиты от вредоносного кода.
33. Способы защиты от методов социальной инженерии и фишинга.

Каждому аспиранту на экзамене дополнительно задаются вопросы по теме диссертации на соискание ученой степени кандидата наук.