

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.26 Программно-аппаратные средства защиты информации

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.	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1 - Знает основные физические законы, физическую сущность явлений и процессов; ОПК-4.2 - Умеет использовать математические модели физических явлений и процессов; ОПК-4.3 - Владеет практическими навыками решения типовых прикладных физических задач.
ОПК-6.	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации ограниченного доступа.
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

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. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности	ОПК-4, ОПК-6, ОПК-4.3	Устный опрос по теме лекции
2.	Тема 2. Программно-аппаратные средства обеспечения информационной безопасности.	ОПК-4, ОПК-6, ОПК-4.3	Устный опрос по теме лекции .
3.	Тема 3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации		Устный опрос по теме лекции

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

Необходимо написать программу, которая будет производить инициализацию библиотеки PKCS#11 для eToken, выводить информацию о данной библиотеке, в отдельном потоке получать информацию о событиях подключения/отключения eToken. В случае возникновения события подключения eToken должен производиться вывод информации о подключенном eToken.

Задание 2

Необходимо создать сертификат студента, подписанный с помощью сертификата преподавателя. Требуется написать программу, которая импортирует сертификат x.509 в DER кодировке на eToken. В данной программе необходимо: произвести инициализацию библиотеки PKCS#11 для eToken, запросить путь к сертификату на жестком диске, ПИН для подключения к eToken, произвести операцию Login к eToken, считать сертификат с жесткого диска, скопировать сертификат на eToken. Проверить наличие сертификата с помощью eToken PKI Client.

Задание 3

Требуется написать программу, которая:

- позволяет считывать закрытый ключ в формате PEM, записывать его на eToken;
 - позволяет записывать произвольные файлы на eToken;
 - позволяет искать данные на eToken и сохранять выбранные данные на жесткий диск;
 - позволяет удалять данные с eToken.
2. Необходимо извлечь закрытый ключ из хранилища Windows, записать его на eToken.
 3. Создать несколько файлов с секретными сведениями и записать их на eToken.
 4. Произвести поиск данных на eToken, сохранить выбранные данные на жесткий диск.
 5. Удалить один из файлов с eToken.

Задание 4

Требуется написать программу, которая:

- генерирует сессионный ключ шифрования;
 - считывает данные из файла и производит их шифрование, выводит зашифрованные данные в консоль;
 - расшифровывает данные и выводит их на консоль.
2. Для проверки используйте текстовый файл с содержимым, включающим номер группы и ФИО студента.
 3. Необходимо, чтобы программа выводила исходный текст после расшифровывания.

4. Учитывайте, что необходимо использовать буфер длиной 128 байт и производить шифрование данных кусками по 128 байт. Убедитесь, что программа работает с файлами больше 128 байт.

Задание 5

1. С помощью инструмента Process Monitor. создайте и примените три фильтра к различным программам.
2. Разархивируйте две вредоносные программы согласно варианту.
3. Запустите разархивированные вредоносные программы, создайте и примените фильтры для данных программ.
4. Проанализируйте детальную информацию, выведенную при помощи фильтров, и сделайте выводы о особенностях вредоносных программ.
5. Проведите лечение системы после ее заражения.

Примерный перечень тестовых заданий

1. Уберите лишнее. Применение аппаратных модулей безопасности (HSM) возможно в таких областях, как:
 - a) PKI, центр сертификации
 - b) Банковские операции
 - c) Экспорт криптографических ключей
 - d) Установление SSL соединений
2. Какая из функций не относится к аппаратным модулям безопасности (HSM):
 - a) Безопасная генерация ключей шифрования
 - b) Безопасное хранение и управление ключами
 - c) Работа с эллиптическими кривыми
 - d) Шифрование и расшифровывание конфиденциальной информации
3. Выберите верный вариант ответа. Ключи шифрования ключей (КК), используемые для пересылки ключей между двумя узлами сети, называются:
 - a) Ключами для шифрования МК (мастер-ключа)
 - b) Рабочие или сеансовые КК
 - c) Ключами обмена между узлами сети (cross-domain keys)
 - d) Ключами аутентификации сообщений
4. К особенностям программно-аппаратного комплекса MKTrusT не относится:
 - a) Позволяет работать в одном из двух режимов – защищенном (например, работа с ДБО или иными критичными к защищенности сервисами) и незащищенном, без ограничения возможностей
 - b) Защищенная ОС – Linux собственной сборки, незащищенная ОС – Android
 - c) В стандартной комплектации MKTrusT присутствует IP-телефон, построенный на «гарвардской» архитектуре
 - d) MKTrusT требует для работы только телевизор (монитор или проектор) через HDMI порт, питание от USB порта (не менее 1 Ампер), сеть – WiFi
5. Выберите верный вариант ответа. Как осуществляется выбор одного из двух режимов на выбор – защищенного или обычного – в программно-аппаратном комплексе MKTrusT:
 - a) Используется выбор режима в процессе загрузки компьютера
 - b) Используется дополнительное устройство, содержащее операционную систему для соответствующего режима работы MKTrusT

- c) Используется физический переключатель
 - d) Используется специальное ПО, реализующее подобие «виртуальной машины»
6. Вставьте пропущенное выражение. ... – период работы компьютера, в рамках которого обеспечивается доверенная загрузка ОС, организуется защищённое сетевое соединение и поддерживаются достаточные условия для работы СКЗИ:
- a) Информационно-поисковая система (ИПС)
 - b) Безопасный режим (БР)
 - c) Доверенный сеанс связи (ДСС)
 - d) Автоматизированный рабочий режим (АРР)
7. Что не относится к сложностям обеспечения безопасности удалённого доступа к информационным ресурсам?
- a) Сложность контроля выполнения требований политики ИБ на удалённых АРМ пользователей
 - b) Необходимость использования сертифицированных ОС, СЗИ НСД и СКЗИ для шифрованием и работы с ЭЦП
 - c) Необходимость проведения аттестационных, адаптационных и инспекционных действий для допуска пользователей к АРМ
 - d) Ограничение функционала сертифицированных ОС и прикладного ПО (в т.ч. сложность процедуры обновлений)
8. Какие из функций не относятся к возможностям КСЗИ «Панцирь-К»
- a) Идентификация и аутентификация: Console, flash, eToken USB, ...
 - b) Разграничение и аудит действий пользователей и приложений, контроль целостности
 - c) Временное гарантированное удаление информации с возможностью восстановления через встроенные механизмы
 - d) Шифрование: 3DES, AES, DES, ГОСТ 28147-89
9. Что не относится к основным принципам разграничения доступа к файловой системе в КСЗИ «Панцирь-К»?
- a) Существует две политики контроля доступа к ресурсам – разрешительная и запретительная
 - b) Права доступа назначаются субъектам, а не присваиваются объектам в качестве их атрибутов
 - c) Администратор имеет такие же права на назначение (изменение) права доступа субъекта к объекту, как и «Владелец»
 - d) Для любого субъекта доступа может быть реализована собственная разграничительная политика
10. Выберите верный вариант ответа. К механизмам контроля целостности КСЗИ «Панцирь-К» относится:
- a) Контроль целостности каталогов и файлов данных (синхронный и асинхронный)
 - b) Контроль целостности исполняемых файлов (программ перед запуском)
 - c) Все перечисленное
 - d) Контроль целостности файлов КСЗИ

11. Какое утверждение не относится к одному из вариантов обхода системы защиты ПО с помощью ключей защиты злоумышленником:
- a) Перехват, протоколирование и анализ обращений к ключу защиты с последующей эмуляцией ответов
 - b) Внесение изменений в программный модуль (взлом)
 - c) Создание вредоносной программы, временно блокирующей запросы к ключу защиты
 - d) Эмулирование наличия ключа путем перехвата вызовов библиотеки API для обмена с ключом
12. Какие утверждения не относятся к защите ПО с помощью API функций ключей защиты?
- a) Самостоятельная разработка защиты ПО
 - b) Интегрирование самостоятельно разработанной системы защиты в приложение на уровне исходного кода
 - c) Отсутствие необходимости изучения и модификации исполняемого кода защищенного приложения для обхода защиты
 - d) Сложность в нейтрализации защиты вследствие её уникальности и «размытости» в теле программы
13. К этапу инициализации программно-аппаратного комплекса «Соболь» не относится:
- a) Установка платы комплекса
 - b) Настройка общих параметров
 - c) Настройка параметров подключения к сети
 - d) Настройка контроля целостности
14. К переводу программно-аппаратного комплекса «Соболь» в режим эксплуатации не относится действие:
- a) Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI
 - b) Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI
 - c) Вытащите кабель из порта «Настройка» и переключите его в порт «Эксплуатация»
 - d) Подключите к плате считыватель iButton
15. Выберите верный вариант ответа. Выставьте в правильном порядке действия при установке программно-аппаратного комплекса «Аккорд».
1. Подсоединение контактного устройства (съемника информации).
 2. Установка платы контроллера в свободный слот ПЭВМ.
 3. Регистрация администратора БИ, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ.
 4. Назначение списка дисков, файлов, разделов реестра, контролируемых на целостность.
 5. Регистрация пользователей, назначение пользователям персональных идентификаторов, паролей и времени доступа
- a) 2, 1, 3, 4, 5
 - b) 1, 2, 3, 5, 4
 - c) 2, 1, 3, 5, 4
 - d) 1, 2, 5, 4, 3
16. Какое из перечисленных программно-аппаратных средств не используют для хранения криптографических ключей?
- a) eToken
 - b) Смарт-карты
 - c) iButton

d) Аппаратный модуль безопасности (HSM)

17. Какое из высказываний не относится к преимуществам аппаратного генератора случайных чисел:

- a) Запас чисел не ограничен
- b) Низкие вычислительные затраты
- c) Используется специальное устройство
- d) Не занимает место в памяти

18. Какое из действий не относится к организации замкнутой программной среды в КСЗИ «Панцирь-К»:

- a) Задание списка разрешенных процессов (системных и прикладных) с возможностью запуска только тех процессов, которые отнесены к разрешенным
- b) Задание папок, откуда разрешается запускать программы (с запретом записи и модификации в них файлов)
- c) Задание специального общего пользователя, от чьего лица совершается установка и запуск программ
- d) Дополнительный анализ содержимого файлов (поиск признаков исполняемого файла)

19. При взломе программ, защищенных с помощью аппаратных ключей защиты не используется следующий метод:

- a) Отладка
- b) Дизассемблирование
- c) Диверсификация
- d) Дамп оперативной памяти

20. Что не входит в комплектацию программно-аппаратного комплекса «Аккорд-АМДЗ»?

- a) Контроллер
- b) Съёмник информации с контактным устройством
- c) Секретный логин и пароль, необходимый для первоначального запуска АМДЗ
- d) Персональный идентификатор пользователя

Примерные вопросы к зачету

1. Методы обеспечения информационной безопасности автоматизированных систем (основные понятия, угрозы).
2. Методы обеспечения информационной безопасности автоматизированных систем (методы взлома, защита от взлома).
3. Методы обеспечения информационной безопасности автоматизированных систем (защита от программных закладок).
4. Политика безопасности. Модель автоматизированной системы.
5. Замкнутая программная среда. Ядро безопасности с учетом контроля порождения субъектов
6. Формирование и поддержка изолированной программной среды. Условия невозможности НСД
7. Реализация ИПС с использованием механизма расширения BIOS
8. UEFI. Принципы работы
9. Безопасное взаимодействие в КС. Процедуры идентификации и аутентификации
10. Аутентификация до загрузки ОС
11. Контроль и управление доступом
12. Персональное средство аутентификации eToken
13. eToken API
14. Назначение, функции, принцип работы ПАК «Аккорд».
15. Назначение, функции, принцип работы ПАК «Соболь».

17. Назначение, функции, принцип работы ключей защиты. Известные модели.
18. Виды защиты ПО с помощью электронных ключей. Методы взлома.
19. Защитные механизмы Astra Linux Special Edition: дискреционное и мандатное разграничение доступа.
20. Защитные механизмы Astra Linux Special Edition: замкнутая программная среда и контроль целостности
21. Управление криптографическими ключами
22. Концепция иерархии ключей, генерация ключей
23. Аппаратные модули безопасности (HSM)
24. Концепция доверенных сеансов связи. Комплекс «МАРШ!», «М!&М».
25. Защищенные микрокомпьютеры «МКТ». Назначение, функции.
26. Защищенные носители «СЕКРЕТ». Виды, назначение, функции.
27. Средства защиты виртуальной инфраструктуры. vGate.
28. Сертификация автоматизированных систем и средств вычислительной техники: виды нормативных документов, определяющих требования по сертификации СЗИ.
29. Сертификация автоматизированных систем и средств вычислительной техники: требования к средствам вычислительной техники
30. Сертификация автоматизированных систем и средств вычислительной техники: требования по контролю отсутствия недекларированных возможностей
31. Сертификация автоматизированных систем и средств вычислительной техники: требования по уровням доверия (Приказ ФСТЭК № 76).

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