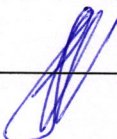


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

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.04 Прикладная криптография

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-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения 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 семестр			
1.	Тема 1. Введение в прикладные аспекты криптографической защиты информации	ПКС-1	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
2.	Тема 2. Инфраструктура открытых ключей	ПКС-1	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
3.	Тема 3. Механизмы управления ключами	ПКС-1	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
4.	Тема 4. Практические аспекты криптографической защиты информации	ПКС-1	Задания к лабораторным работам, контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену
5.	коллоквиумы	ПКС-1	контрольные вопросы, вопросы к коллоквиуму
6.	экзамен	ПКС-1	контрольные вопросы, вопросы к коллоквиуму, вопросы к экзамену

Лабораторное занятие №1 (10 ч.)

Тема Введение в прикладные аспекты криптографической защиты информации

Вопросы для обсуждения:

1. Криптографические файловые системы.
2. Шифрованная файловая система Windows.
3. Криптографические файловые системы.
4. Шифрование диска BitLocker
5. Шифрование дисков VeraCrypt

Задание на работу

1. Создайте учетные записи двух пользователей и файлы для каждого из них для выполнения лабораторной работы.
2. Зашифруйте по одному файлу каждому из пользователей.
3. Архивируйте сертификаты с закрытым ключом для каждого из пользователей.
4. Сделайте совместный доступ к одному зашифрованному файлу для обоих пользователей.
5. Создайте третьего пользователя и проверьте доступ к файлу от него.
6. Составить по проделанной работе отчет.

Контрольные вопросы

1. В каких выпусках операционных систем Windows присутствует шифрованная файловая система?
2. Для каких файловых систем применима шифрованная файловая система?
3. Для чего в шифрованной файловой системе используется симметричное шифрование?
4. Для чего в шифрованной файловой системе используется асимметричное шифрование?
5. Опишите алгоритм работы шифрованной файловой системы Windows.
6. Для чего нужно архивировать закрытый ключ и сертификат пользователя?
7. Что такое PKCS?
8. Для чего используется PKCS#12?
9. Каким образом можно предоставить доступ к зашифрованному файлу другому пользователю?
10. В каких форматах можно экспортировать сертификат из локального хранилища без экспорта закрытого ключа?

Задание на работу

1. Создайте второй локальный диск на виртуальной машине и зашифруйте его с помощью BitLocker.
2. Зашифруйте системный диск с применением usb-носителя для хранения ключа запуска.
3. Проверьте возможность запуска операционной системы с подключенным и отсутствующим носителем ключа запуска.
4. Составьте по проделанной работе отчет.

Контрольные вопросы

1. В каких выпусках операционных систем Windows присутствует технология шифрования дисков BitLocker?
2. Какие файловые системы могут использоваться на внешних устройствах, чтобы их можно было применить с технологией BitLocker?
3. В чем отличие BitLocker от шифрованной файловой системы?
4. Какой алгоритм шифрования применяется в BitLocker?
5. Для чего используется функция BitLocker To Go?
6. Какие режимы работы системы шифрования возможны для шифрования системных дисков?
7. Что такое TPM?
8. Какие носители можно использовать для сохранения ключа запуска?
9. Объясните отличие между ключом запуска и ключом восстановления.
10. Каким образом можно восстановить доступ к операционной системе, установленной на зашифрованном с помощью BitLocker локальном диске, в случае утери носителя с ключом запуска?

Задание на лабораторную работу

1. Создайте зашифрованный файловый контейнер с алгоритмом шифрования по своему варианту (табл. 1).
2. Проведите шифрование раздела жесткого диска в соответствии с вариантом из табл. 1.
3. Проведите шифрование системного диска.
4. Составьте по проделанной работе отчет.

Таблица 1

Варианты для индивидуального выполнения работы

№	Файловый контейнер	Шифрование диска
1	AES	AES(Twofish)

2	Serpent	AES(Twofish(Serpent))
3	Twofish	Camellia
4	Camellia	Kuznyechik
5	Kuznyechik	Serpent
6	AES(Twofish)	Twofish
7	AES(Twofish(Serpent))	AES
8	Serpent(AES)	Kuznyechik(Serpent(Camellia))
9	Twofish(Serpent)	Camellia(Serpent)
10	Camellia(Kuznyechik)	Kuznyechik(AES)

Контрольные вопросы

1. Какие алгоритмы шифрования применяются в VeraCrypt?
2. Что такое файловый контейнер?
3. Чем отличается скрытый том от обычного?
4. Что влияет на скорость тестируемых алгоритмов шифрования?
5. Для чего необходима очистка диска при шифровании системного диска?
6. Что такое PIM?
7. Какие достоинства и недостатки у использования ключевых файлов?
8. Что такое скрытая операционная система?
9. Как отразится на скрытом томе, если в обычный том будет записан большой объем информации?
10. Как отразится на открытом томе, если в скрытый том будет записан большой объем информации?

Лабораторное занятие №2 (10 ч.)

Тема Инфраструктура открытых ключей

Вопросы для обсуждения:

1. Установка и настройка служб удостоверяющего центра.
2. Функции удостоверяющего центра.
3. Кросс-сертификация удостоверяющих центров.
4. Построение иерархической архитектуры инфраструктуры открытых ключей

Задание на работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Настроить удостоверяющий центр на виртуальной машине в соответствии с методическими указаниями.
3. Составить по проделанной работе отчет.

Контрольные вопросы

6. Опишите протокол взаимодействия в симметричных криптосистемах.
7. Приведите пример симметричных криптосистем.
8. В чем заключается проблема распределения ключей в симметричных криптосистемах?
9. Какие криптографические алгоритмы относятся к бесключевым?
10. Опишите протокол взаимодействия в криптосистемах с открытым ключом.
11. Приведите пример криптосистем с открытым ключом.
12. В чем заключается атака типа «Человек посередине»?
13. Каким образом можно обеспечить защиту ключей от подмены?
14. Перечислите технологии, входящие в Active Directory?
15. Какая технология Active Directory позволяет организовать работу инфраструктуры открытых ключей?

Задание на работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Настроить удостоверяющий центр на виртуальной машине в соответствии с методическими указаниями.
3. Составить по проделанной работе отчет.

Контрольные вопросы

6. Опишите протокол взаимодействия в симметричных криптосистемах.
7. Приведите пример симметричных криптосистем.
8. В чем заключается проблема распределения ключей в симметричных криптосистемах?
9. Какие криптографические алгоритмы относятся к бесключевым?
10. Опишите протокол взаимодействия в криптосистемах с открытым ключом.
11. Приведите пример криптосистем с открытым ключом.
12. В чем заключается атака типа «Человек посередине»?
13. Каким образом можно обеспечить защиту ключей от подмены?
14. Перечислите технологии, входящие в Active Directory?
15. Какая технология Active Directory позволяет организовать работу инфраструктуры открытых ключей?

Задание на работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Создать шаблон сертификата для кросс-сертификации.
3. Провести взаимную кросс-сертификацию между настроенным Вами в предыдущих лабораторных работах удостоверяющим центром и готовым УЦ.
4. Составить по проделанной работе отчет.

Контрольные вопросы

1. Что такое инфраструктура открытых ключей?
2. Какие модели доверия Вам известны?
3. Что такое кросс-сертификация?
4. На какие два вида подразделяется кросс-сертификация? В чем отличие между ними?
5. Какие шаблоны сертификатов Вам известны?
6. Перечислите основные свойства сертификата.
7. Как импортировать и экспортировать сертификат?
8. Какие параметры можно установить при запросе сертификата?
9. Для чего используются списки отозванных сертификатов?
10. Опишите алгоритм получения нового списка отозванных сертификатов.

Задание на работу

1. Создайте самоподписанный сертификат.
2. Создайте электронную подпись на файле.
3. Проверьте статус электронной подписи и добавьте дополнительную подпись к подписанному файлу.
4. Зашифруйте файл с помощью сертификата.
5. Составить по проделанной работе отчет.

Контрольные вопросы

11. Какие криптографические операции можно выполнить в КриптоАРМ?
12. Что такое самоподписанный сертификат?
13. Какие варианты использования ключа доступны в КриптоАРМ?
14. Чем отличается квалифицированный сертификат от обычного?
15. В чем отличие CRL от CTL?

16. Для чего проставляется на документе штамп времени?
17. Для чего используется добавление подписи к подписанному файлу?
18. Что такое "заверяющая подпись"?
19. Какие режимы шифрования доступны в КристоАРМ?
20. Какой сертификат становится сертификатом расшифрования?

Лабораторное занятие №3 (8 ч.)

Тема Механизмы управления ключами

Вопросы для обсуждения:

1. Изучение стандарта ISO/IEC 11770.
2. Механизмы, использующие симметричные методы.
3. Механизмы, использующие асимметричные методы.
4. Механизмы, основанные на слабых секретах.
5. Управление групповыми ключами. Формирование ключей.

Задание на работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Установить и настроить криптопровайдер Signal-COM CSP.
3. Создать шаблон сертификата, использующий установленный криптопровайдер, и выдать на его основе сертификат.
4. Установить и настроить криптопровайдер КристоПро CSP.
5. Создать шаблон сертификата, использующий установленный криптопровайдер, и выдать на его основе сертификат.
6. Подписать файл с использованием созданного сертификата.
7. Отозвать сертификат и проверить подписанный с его помощью файл.
8. Составить по проделанной работе отчет.

Контрольные вопросы

1. Что такое криптопровайдер?
2. Что такое CryptoAPI?
3. Какие задачи выполняет CryptoAPI?
4. Какие функции обеспечивают криптопровайдеры?
5. В каком формате криптопровайдеры хранятся на компьютере?
6. Что такое ключевой контейнер?
7. Почему не рекомендуется устанавливать несколько криптопровайдеров на одном устройстве?
8. Какие виды носителей могут быть использованы для хранения ключевого контейнера в СКЗИ Signal-COM CSP?
9. Какие виды носителей могут быть использованы для хранения ключевого контейнера в СКЗИ КристоПро CSP?
10. Зачем необходим сбор энтропии при инициализации работы датчика случайных чисел?

Лабораторное занятие №4 (4 ч.)

Тема Практические аспекты криптографической защиты информации.

Вопросы для обсуждения:

1. Проблемы реализации криптографических алгоритмов.
2. Защита от утечки информации.
3. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.

Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Настроить удостоверяющий центр на виртуальной машине в соответствии с методическими указаниями.
3. Создать собственный шаблон сертификата с индивидуальным объектным идентификатором и выдать сертификат по данному шаблону.
4. Составить по проделанной работе отчет.

Контрольные вопросы

1. Какие функции выполняет удостоверяющий центр?
2. Что такое сертификат и какую функцию он выполняет?
3. Какие форматы сертификатов Вам известны?
4. Перечислите основные поля, содержащиеся в сертификате формата X.509?
5. Объясните разницу между централизованным и децентрализованным изданием сертификатов. Какой вид рассматривается в лабораторной работе?
6. Что такое объектный идентификатор (OID)?
7. Для чего нужен объектный идентификатор (OID)?
8. Для каких шаблонов рекомендуется использование опции «Архивировать закрытый ключ субъекта»?
9. Опишите жизненный цикл сертификата.
10. Приведите примеры ситуаций, при которых доверие к сертификату может быть подорвано до истечения срока его действия

Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Реализовать иерархическую архитектуру, состоящую из двух удостоверяющих центров и клиентской машины.
3. Подписать на клиентской машине документ с помощью, сертификата, полученного от подчиненного удостоверяющего центра.
4. Проверить состояние электронной подписи после отзыва сертификата корневым удостоверяющим центром.
5. Составить по проделанной работе отчет.

Контрольные вопросы

1. Объясните разницу между строгой и нестрогой иерархиями удостоверяющих центров.
2. Какие отличия между корневым и подчиненным удостоверяющими центрами?
3. Поясните понятие «путь сертификации».
4. Какие этапы включены в обработку пути?
5. Опишите алгоритм отзыва сертификата.
6. Какие причины можно указать при отзыве сертификата?
7. Опишите алгоритм восстановления отозванного сертификата.
8. Действие любого отозванного сертификата может быть возобновлено?
9. Для чего необходимо публиковать списки отозванных сертификатов после восстановления отозванного сертификата?
10. Какие существуют варианты проверки действия сертификата?

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3

коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр			60	100

Примерные вопросы к экзамену

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Основные атаки на криптографические протоколы.
4. Понятие электронной подписи.
5. Управление открытыми ключами.
6. Основные компоненты инфраструктуры открытых ключей.
7. Понятие сертификата открытого ключа.
8. Удостоверяющий центр.
9. Архитектура инфраструктуры открытого ключа.
10. Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ».
11. Понятие протоколов интерактивного доказательства и доказательства знания.
12. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
13. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.
14. Проблемы реализации криптографических алгоритмов.
15. Защита от утечки информации.

Критерии оценки:

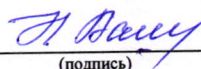
оценка «отлично» выставляется студенту, если студент свободно ориентируется в теоретическом материале; умеет изложить и корректно оценить различные подходы к излагаемому материалу, способен сформулировать и доказать собственную точку зрения; обнаруживает свободное владение понятийным аппаратом; демонстрирует готовность применять теоретические знания в практической деятельности и полное освоение показателей формируемых компетенций;

оценка «хорошо» выставляется студенту, если студент хорошо ориентируется в теоретическом материале; имеет представление об основных подходах к излагаемому материалу; знает определения основных теоретических понятий излагаемой темы, в основном демонстрирует готовность применять теоретические знания в практической деятельности и освоение большинства показателей формируемых компетенций;

оценка «удовлетворительно» выставляется студенту, если студент может ориентироваться в теоретическом материале; в целом имеет представление об основных понятиях излагаемой темы, частично демонстрирует готовность применять теоретические знания в практической деятельности и освоение некоторых показателей формируемых компетенций;

оценка «неудовлетворительно» выставляется студенту, если студент не ориентируется в теоретическом материале; не сформировано представление об основных понятиях излагаемой темы, не демонстрирует готовность применять теоретические знания в практической деятельности и освоение показателей формируемых компетенций.

Составитель


(подпись)

Вашакидзе Н.С

«7» марта 2024 г.