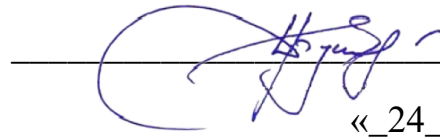


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной  
образовательной программы

 Буинцев Д.Н.  
«\_24\_» сентября 2024 г

**РАБОЧАЯ ПРОГРАММА**

Дисциплины

*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***

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск  
2024

Рабочая программа дисциплины Программно-аппаратные средства защиты информации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

Г.В. Филиппова, старший преподаватель кафедры информатики



Рабочая программа дисциплины Программно-аппаратные средства защиты информации утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности  
заведующего кафедрой

Г.С. Осипов



## 1. Цель и задачи дисциплины

### Цель дисциплины

Целями освоения дисциплины *«Программно-аппаратные средства защиты информации»* являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по основам защиты информации в компьютерных системах при помощи программно-аппаратных средств достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

### Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. Формирование представления и получение навыков работы с программно-аппаратными средствами защиты информации, реализующим отдельные функциональные требования по защите.
2. Формирование базовых знаний и умений разработки компонентов программно-аппаратных средств защиты информации.
3. Формирование базовых знаний по методам и средствам хранения ключевой информации, методам и средствам ограничения доступа к компонентам вычислительных систем, задачам и технологии сертификации программно-аппаратных средств защиты информации на соответствие требованиям информационной безопасности.
4. Формирование базовых знаний и умений по методам защиты от вредоносных программ, защите программ от изменения и контролю целостности.

### Место дисциплины в структуре образовательной программы

Дисциплина *«Программно-аппаратные средства защиты информации»* относится к обязательной части Блока 1 Дисциплины (модули) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность

### Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знаниях, полученных в результате изучения таких дисциплин как «Основы информационной безопасности», Разработка и эксплуатация защищенных автоматизированных систем, Методы и средства криптографической защиты информации, Основы управления информационной безопасностью

Изучение данной дисциплины проходит параллельно с изучением такой дисциплины, как «Защита информации от утечки по техническим каналам» и базируется на знаниях, полученных в результате изучения этой дисциплины.

### Постреквизиты дисциплины:

Знания и умения, полученные студентами при изучении дисциплины, применяются ими во время учебной и преддипломной практик и в их профессиональной деятельности.

## 2. Формируемые компетенции и индикаторы их достижения по дисциплине

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

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

### 3. Структура и содержание дисциплины

#### 3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, акад. часов	
	8 семестр	всего
<b>Общая трудоемкость</b>	<b>108</b>	<b>108</b>
<b>Контактная работа:</b>	<b>50</b>	<b>50</b>
Лекции	22	22
Лабораторные работы (Лаб)	24	24
Контактная работа в период теоретического обучения (КонтТО) ( <i>Проведение текущих</i>	4	4

консультаций и индивидуальная работа со студентами)		
<b>Промежуточная аттестация (зачет)</b>		
<b>Самостоятельная работа:</b> - самоподготовка (проработка и повторение материала занятий, учебников и учебных пособий); - подготовка к лабораторным занятиям;	<b>58</b>  29 29	<b>58</b>  29 29

#### 4. Распределение видов работы и их трудоемкости по разделам дисциплины

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
		контактная			Самостоятельная работа	
		Лекции	Практические занятия	Лабораторные занятия		
8 семестр						
1.	Тема 1. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности	6			10	Устный опрос по теме лекции Выполнение практического задания Тестирование
2.	Тема 2. Программно-аппаратные средства обеспечения информационной безопасности.	14		24	38	Устный опрос по теме лекции Выполнение практического задания Тестирование
3.	Тема 3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	2			10	Устный опрос по теме лекции Выполнение практического задания Тестирование
	итоги:	22		24	58	

##### 4.1. Содержание разделов дисциплины

###### Раздел 1 Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.

Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. Обеспечение гарантий выполнения политики безопасности. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды

###### Раздел 2 Программно-аппаратные средства обеспечения информационной безопасности.

Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Средства обеспечения информационной безопасности в операционной системе GNU/Linux. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в

операционной системе GNU/Linux. Замкнутая программная среда и контроль целостности в операционной системе GNU/Linux. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности.

### **Раздел 3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.**

Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем. Требования к процессу сертификации продукта информационных технологий

#### **Темы и планы лабораторных занятий**

##### **Лабораторное занятие №1 (2 ч.)**

Тема. Дискреционный и мандатный механизмы разграничения доступа к файловым объектам в операционной системе.

Вопросы для обсуждения:

1. Дискреционный механизм разграничения доступа к файловым объектам
2. Мандатный механизм разграничения доступа к файловым объектам
3. Достоинства и недостатки дискреционного и мандатного механизмов разграничения доступа к файловым объектам.

##### **Лабораторное занятие №2 (2 ч.)**

Тема. Замкнутая программная среда и контроль целостности в операционной системе

Вопросы для обсуждения:

1. Замкнутая программная среда в операционной системе
2. Контроль целостности в операционной системе.
3. Организация контроля целостности в операционной системе.

##### **Лабораторное занятие №3-4 (4 ч)**

Тема. Разработка защищенного ПО с применением аппаратных ключей eToken

Знакомство с eToken API.

Вопросы для обсуждения:

1. Базовые функции, связанные с определением наличия eToken в системе
2. Получение информации о подключенном eToken.

##### **Лабораторное занятие №5-6 (4 ч)**

Тема. Разработка защищенного ПО с применением аппаратных ключей eToken

Работа с сертификатами X.509 на eToken

Вопросы для обсуждения:

1. знакомство с сертификатами X.509,
2. изучение функции eToken API, связанных с импортом сертификатов на eToken,
3. выполнение операции входа пользователя на eToken.

##### **4. 1. Лабораторное занятие №7-8 (4 ч)**

Тема. Разработка защищенного ПО с применением аппаратных ключей eToken.

Объекты eToken.

Вопросы для обсуждения:

1. Типы объектов, которые позволяет хранить и использовать eToken,
2. операции, связанные с чтением, записью, удалением и поиском объектов на eToken

**Лабораторное занятие №9-10 (4 ч)**

Тема. Разработка защищенного ПО с применением аппаратных ключей eToken.

Шифрование данных с помощью eToken.

Вопросы для обсуждения:

1. типы шифрования и механизмы, обеспечивающими генерацию ключей eToken,
2. шифрование данных с помощью eToken.
3. расшифровывание данных с помощью eToken

**Лабораторное занятие №11-12 (4 ч)**

Тема. «Защита автоматизированных систем от вредоносного программного обеспечения»

Вопросы для обсуждения:

1. принципы работы вредоносных программ.

**5. Темы дисциплины (модуля) для самостоятельного изучения**

Не предусмотрены

**6. Образовательные технологии**

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Тема 1. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности	Лекция 1 Лекция 2 Лекция 3	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
2.	Тема 2. Программно-аппаратные средства обеспечения информационной безопасности.	Лекция 1 Лекция 2 Лекция 3 Лекция 4 Лекция 5 Лекция 6 Лекция 7	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторная работа 1 Лабораторная работа 2 Лабораторная работа 3 Лабораторная работа 4 Лабораторная работа 5 Лабораторная работа 6 Лабораторная работа 7 Лабораторная работа 8 Лабораторная работа 9 Лабораторная работа 10 Лабораторная работа 11 Лабораторная работа 12	
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
3.	Тема 3 Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.
		Лабораторное занятие	Лабораторное занятие в компьютерном классе
		Самостоятельная работа	Повторение материала, подготовка домашнего задания.

		Лабораторное занятие	Лабораторное занятие в компьютерном классе
--	--	----------------------	--

## 7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.

Форма контроля для очной формы обучения – *зачет*,

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

### 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 МКTrusT не относится:
  - a) Позволяет работать в одном из двух режимов – защищенном (например, работа с ДБО или иными критичными к защищенности сервисами) и незащищенном, без ограничений возможностей
  - b) Защищенная ОС – Linux собственной сборки, незащищенная ОС – Android
  - c) В стандартной комплектации МКTrusT присутствует IP-телефон, построенный на «гарвардской» архитектуре
  - d) МКTrusT 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 МКTrusT:
  - a) Используется выбор режима в процессе загрузки компьютера
  - b) Используется дополнительное устройство, содержащее операционную систему для соответствующего режима работы МКTrusT
  - 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

с) Настройка параметров подключения к сети

д) Настройка контроля целостности

14. К переводу программно-аппаратного комплекса «Соболь» в режим эксплуатации не относится действие:

а) Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI

б) Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI

с) Вытащите кабель из порта «Настройка» и переключите его в порт «Эксплуатация»

д) 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

а) 2, 1, 3, 4, 5

б) 1, 2, 3, 5, 4

с) 2, 1, 3, 5, 4

д) 1, 2, 5, 4, 3

16. Какое из перечисленных программно-аппаратных средств не используют для хранения криптографических ключей?

а) eToken

б) Смарт-карты

с) iButton

д) Аппаратный модуль безопасности (HSM)

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

а) Запас чисел не ограничен

б) Низкие вычислительные затраты

с) Используется специальное устройство

д) Не занимает место в памяти

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

а) Задание списка разрешенных процессов (системных и прикладных) с возможностью запуска только тех процессов, которые отнесены к разрешенным

б) Задание папок, откуда разрешается запускать программы (с запретом записи и модификации в них файлов)

с) Задание специального общего пользователя, от чьего лица совершается установка и запуск программ

д) Дополнительный анализ содержимого файлов (поиск признаков исполняемого файла)

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

а) Отладка

б) Дизассемблирование

с) Диверсификация

д) Дамп оперативной памяти

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

а) Контроллер

б) Съемник информации с контактным устройством

с) Секретный логин и пароль, необходимый для первоначального запуска АМДЗ

д) 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».
16. Персональные идентификаторы. Виды, назначение, функции.
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 недеklarированных возможностей
31. Сертификация автоматизированных систем и средств вычислительной техники: требования по уровням доверия (Приказ ФСТЭК № 76).

## **8. 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

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
<b>Итого за семестр</b>			53	100

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1. Основная литература

#### а) основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. [Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/513300>.
2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/237770>.
3. Защита информации с использованием смарт-карт и электронных брелоков / Л. К.Бабенко, С. С. Ищуков, О. Б. Макаревич. - М. : "Гелиос АРВ", 2003. - 351[1] с. : ил., табл., портр. - Библиогр.: с. 348-349. (наличие в библиотеке ТУСУР - 29 экз.).

### 9.2.Дополнительная литература

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В- Спектр, 2007 - . Раздел 1. - 2-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 143[1] с. : ил. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.).
2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие: В 2 разделах / А. П. Зайцев ; Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - Томск : В- Спектр, 2007 - . Раздел 2. - 2-е изд., перераб. и доп. - Томск : 118[2] с. : ил. -Библиогр.: с. 37. - Б. ц. (наличие в библиотеке ТУСУР - 66 экз.).

### **9.3. Программное обеспечение**

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security & Acceleration Server Standard Edition 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYY FineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit OEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. Дистрибутивы Ubuntu GNU/Linux, Debian GNU/Linux
13. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;
14. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
15. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

### **9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий**

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии ([http://window.edu.ru/catalog/?p\\_rubr=2.2.75.6](http://window.edu.ru/catalog/?p_rubr=2.2.75.6))
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий ([www.intuit.ru](http://www.intuit.ru))
9. Онлайн среда разработки приложений ([ideone.com](http://ideone.com))
10. Журнал «КомпьютерПресс» ([www.compress.ru](http://www.compress.ru))
11. Издательство «Открытые системы» ([www.osp.ru](http://www.osp.ru))
12. Издание о высоких технологиях ([www.cnews.ru](http://www.cnews.ru))
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
15. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
16. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
17. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

## **10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

### ***Для слепых и слабовидящих:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

### ***Для глухих и слабослышащих:***

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

### ***Для лиц с нарушениями опорно-двигательного аппарата:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

### ***Для слепых и слабовидящих:***

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

### ***Для глухих и слабослышащих:***

- в печатной форме;
- в форме электронного документа.

### ***Для обучающихся с нарушениями опорно-двигательного аппарата:***

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

**для слепых и слабовидящих:**

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

**для глухих и слабослышащих:**

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

**для обучающихся с нарушениями опорно-двигательного аппарата:**

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

## **11. Материально-техническое обеспечение дисциплины (модуля)**

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

**К рабочей программе прилагаются:**

**Приложение 1** – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

**Приложение 2** – Методические указания для обучающихся по освоению дисциплины (модуля).