МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Программно-аппаратные средства защиты информации

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Программно-аппаратные средства защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-7.1. - Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Применяет программные средства системного и прикладного назначений для решения задач профессиональной деятельности

Использует программные и программно-аппаратные средства испытания систем защиты информационных систем

Результаты обучения по дисциплине:

Знать программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

Знать программные и программно-аппаратные средства испытания систем защиты информационных систем.

Уметь применять типовые программные средства защиты информации.

Уметь использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем.

Владеть навыками применения программных средства системного и прикладного назначений для решения задач профессиональной деятельности.

Владеть навыками анализа состояния информационной безопасности на конкретном объекте защиты.

2 Место дисциплины "Программно-аппаратные средства защиты информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность операционных систем, Безопасность систем баз данных, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Сети и системы передачи информации, Нормативные требования по защите информации, Информационные угрозы, Классификация защищаемой информации и информационных систем, Методы и средства защиты информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Программно-аппаратные средства защиты информации" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Программно-аппаратные средства защиты информации" составляет 5 зачетных единиц, 180 часов.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 4/Семестр 7			
Всего часов	180		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		
Самостоятельная работа	64		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Программно-аппаратные средства защиты информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Введение	1
2. Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки	1
3. Правовые, нормативно-технические и организационные требования к средствам защиты информации	4
4. Подсистема контроля доступа пользователей к ресурсам	4
5. Подсистема регистрации и учета	2
6. Подсистема контроля целостности	4
7. Подсистема криптографической защиты	4
8. Межсетевое экранирование	2
9. Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации	4
10. Виртуальные частные сети	4
11. Контроль защищенности информации	2
Итого	**32**

4.2 Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах
	ОФ

1. (4) Аппаратные и программные средства санкционированной загрузки.	2
2. (4) Авторизация. Аппаратные ключи пользователей.	2
3. (4) Реализация разграничения доступа к внешним устройствам.	2
4. (4) Управление потоками информации.	2
5. (5) Регистрация событий входа-выхода, запуска задач.	2
6. (5) Регистрация событий администрирования, доступа к объектам.	2
7. (5) Реализация маркировки и учета документов.	2
8. (5) Гарантированное удаление информации.	2
9. (6) Контроль целостности файлов и папок.	2
10. (6) Контроль нарушения аппаратной конфигурации. Санкционированное использование внешних носителей.	2
11. (7) Хранение информации в шифрованном виде. Монопольный и коллективный доступ к контейнерам. Особенности реализации в различных СЗИ.	2
12. (8) Фильтрация пакетов.	2
13. (10) Центр управления сетью. Адресация.	2
14. (10) Ключевой удостоверяющий центр.	2
15. (11) Средства контроля защищенности информации для подсистемы контроля доступа.	2
16. (11) Средства контроля защищенности информации для подсистемы контроля целостности.	2
Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	30
Оформление отчетов по практическим и(или) лабораторным работам	28
Подготовка к промежуточной аттестации	6
Итого	**64**
Самостоятельная работа под руководством преподавателя	16
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Программно-аппаратные средства защиты информации"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Применяет программные средства системного и прикладного назначений для решения задач профессиональной деятельности	**Знать** программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. **Уметь** применять типовые программные средства защиты информации. **Владеть** навыками применения программных средства системного и прикладного назначений для решения задач профессиональной деятельности.	Высокий или средний
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-7.1. - Способен использовать программные и программноаппаратные средства для моделирования и испытания систем защиты информационных систем	Использует программные и программно-аппаратные средства испытания систем защиты информационных систем	**Знать** программные и программно-аппаратные средства испытания систем защиты информационных систем. **Уметь** использовать программные и программноаппаратные средства для моделирования и испытания систем защиты информационных систем. **Владеть** навыками анализа состояния информационной безопасности на конкретном объекте защиты.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной

и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Например:

1. Ролевое управление доступом.
2. Протоколирование и аудит

Критерии оценивания при ответе на вопросы:
- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Введение

1. Основные понятия программно-аппаратной защиты информации
2. Знаний в каких предметных областях требует программно-аппаратная защиты информации?
3. Чем характерны задачи программно-аппаратной защиты информации?
4. По каким критериям можно классифицировать метод и средства программно-аппаратной защиты информации?
5. Кто является постановщиком задач, связанных с программно-аппаратной защитой информации на конкретном предприятии?

2. Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки информации

1. В чем состоят основные задачи программно-аппаратной защиты информации?
2. Что является предметом рассмотрения и внимания при создании программно-аппаратных методов и средств защиты информации?
3. Что является предметом исследования и изучения при проектировании средств программно-аппаратных средств защиты информации?
4. Выбор решений программно-аппаратной защиты информации для конкретной ИС и режимов обработки информации
5. В чем состоят основные цели программно-аппаратной защиты информации?

3. Правовые, нормативно-технические и организационные требования к средствам защиты информации

1. Основное федеральное ведомство - регулятор, регламентирующее требования к средствам защиты информации
2. В каких случаях выполнение рекомендаций регулятора обязательно?
3. Какой нормативный документ ФСТЭК России устанавливает требования к защите информации, находящейся в государственных информационных системах (ИС), если она не содержит государственную тайну?
4. Что в целом регламентируют нормы ФСТЭК ?
5. О чем гласит Указ Президента № 1085 относительно ФСТЭК в сфере защиты информации?

4. Подсистема контроля доступа пользователей к ресурсам

1. Какие требования предъявляются к созданию учётных записей пользователей в защищенных АИС?
2. Какие требования предъявляются к механизмам разграничения доступа в защищенных АИС?
3. Основные программно-аппаратные разновидности подсистем контроля доступа пользователей к ресурсам
4. Основные модели управления доступом на примере ОС типа Windows NT и Unix
5. Понятие Access Control List (ACL) и принцип его действия

5. Подсистема регистрации и учета

1. Назначение подсистемы регистрации и учета в контексте ЭВМ или ИС
2. Требования к подсистеме регистрации и учета
3. На основе чего может быть реализована подсистема регистрации и учета?
4. Объекты и субъекты для подсистемы регистрации и учета
5. Как проверить эффективность и корректность работы подсистемы регистрации и учета? Существуют ли для этой цели нормативные документы?

6. Подсистема контроля целостности

1. Назначение подсистемы целостности и доступности
2. Варианты реализации подсистемы целостности и доступности
3. Основные требования к подсистеме целостности и доступности
4. Основные методы контроля целостности данных
5. Особенности криптографического контроля целостности, его основные механизмы

7. Подсистема криптографической защиты

1. Назначение подсистемы криптографической защиты
2. Варианты реализации подсистемы криптографической защиты
3. Основные требования к подсистеме криптографической защиты
4. Объекты и субъекты для подсистем криптографической защиты
5. Оценка качества подсистем криптографической защиты

8. Межсетевое экранирование

1. Критерии эффективности межсетевых экранов
2. Назначение межсетевого экранирования
3. Разновидности и классификация межсетевых экранов
4. Типовые правила настроек межсетевого экранирования
5. От каких угроз не могут большинство межсетевых экранов?

9. Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации

1. Основные компоненты, входящие в состав нормативно-методического обеспечения КСЗИ
2. Какие федеральные документы послужили базой (поводом) для создания типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну.
3. Основные моменты (разделы) типовых требований по организации и обеспечению

функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну
4. Основные моменты нормативного документа № Р 1323565.1.012-2017 (ОКС 35.040) Рекомендации по стандартизации. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации.
5. Основные моменты Положения ПКЗ-2005

10. Виртуальные частные сети

1. Основное назначение и концепция виртуальных частных сетей
2. Основные методы защиты данных в виртуальных частных сетях
3. Как работают механизмы криптографии в виртуальных частных сетях
4. Разновидности реализаций виртуальных частных сетей
5. Наиболее современные и безопасные протоколы для построения виртуальных частных сетей.

11. Контроль защищенности информации

1. Основная цель контроля защищенности информации
2. В чем состоит контроль защищенности информации для государственных и федеральных учреждений?
3. Какими федеральными службами организуется периодический контроль защищенности информации для государственных и федеральных учреждений?
4. Какие процедуры подтверждают осуществление контроля защищенности информации и безопасность информационной системы?
5. Какие действия должны выполняться, если в ходе контроля защищенности информации были обнаружены уязвимости в защищаемой ИС?

Примерный перечень тестовых заданий:

1. ***Введение***

1. Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в... куда? выбрать все верные

системный блок
сетевые операционные системы
пакет Microsoft Office
операционную систему MS DOS

2. Что относится к аппаратным средствам защиты информации? выбрать все верные

электронные устройства
электронно-механические устройства
механические средства

3. К основным программным средствам защиты информации относятся: выбрать все верные

программы идентификации и аутентификации пользователей КС
программы разграничения доступа пользователей к ресурсам КС
программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.
программы шифрования информации
программы кодирования информации

2. Цели и задачи обеспечения безопасности информационных технологий в различных режимах обработки информации

1. Основные задачи обеспечения информационной безопасности ИТ состоят в обеспечении:

Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Защищенности всех звеньев системы

2. Обеспечение безопасности информационных технологий это обеспечение:

Независимости информации
Изменения информации
Копирования информации
Сохранности информации
Преобразования информации

3. Цели информационной безопасности ИТ – своевременное обнаружение, предупреждение:

несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

3. Правовые, нормативно-технические и организационные требования к средствам защиты информации

1. Согласно ГОСТ Р 50922-2006 (НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ для термина «Средство защиты информации подходит следующее определение:

Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2. Согласно организационным требованиям по защите данных в государственных ИС (Приказ № 17) и у операторов ПД (Приказ № 21) Объектом защиты признаются: выбрать все верные

данные, содержащиеся в ИС,
оборудование,
съемные носители,
средства связи,
средства расшифровки информации,
программное обеспечение всех типов,
операционные системы,
технологии сохранения безопасности сведений
технические средства их защиты.
персонал, работающий с ИС

3. Нормативные требования ФСТЭК в целом регламентируют: выбрать все верные

классификацию программных и технических средств защиты информации по разным критериям;
использование определенных защитных схем данных исходя из существенности угроз;
критерии оценки работы организаций и персонала;
условия получения лицензий на деятельность и сертификатов на ПО.
стоимость и производителя (разработчика) систем защиты информации

4. Подсистема контроля доступа пользователей к ресурсам

1. На базе чего может быть реализована подсистема контроля доступа пользователей к ресурсам? выбрать все верные

аппаратно
программно
на уровне автономной (клиентской) ОС
на уровне сетевой ОС

2. Модель управления доступом к ресурсам должна отдавать предпочтение _____ способам

Детективным
Восстанавливающим
Корректирующим
Превентивным

3. Какую роль играет биометрия в управлении доступом к ресурсам?

Авторизация
Аутентичность
Аутентификация
Подотчетность

5. Подсистема регистрации и учета

1. Подсистема регистрации и учета предназначена для реализации следующих функций: выбрать все верные

- идентификации и проверка подлинности субъектов доступа при входе в ИС;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

2. Подсистема регистрации и учета может быть реализована с помощью: выбрать все верные

штатных средств (операционных систем, приложений и СУБД).
специальных технических средств или их комплекса
биометрических устройств
внешних сетевых сервисов, например, соцсетей

3. Кто имеет право просматривать отчет (историю) подсистемы регистрации и учета? выбрать все верные

системный администратор
специалист службы безопасности
руководитель организации
контролирующие органы

6. Подсистема контроля целостности

1. Что включает в себя подсистема обеспечения целостности? выбрать все верные

целостность программных средств защиты информации от несанкционированного доступа
целостность обрабатываемой информации
целостность программной среды
целостность учетных записей
целостность истории переходов в веб-браузере и файлов cookie

2. Какие дополнительные действия / мероприятия необходимо проводить чтобы подсистема контроля целостности работала надежно? выбрать все верные

физическая охрана средств вычислительной техники
периодическое тестирование функций средств защиты информации от несанкционированного доступа
наличие резервных копий
ежедневный просмотр действий пользователей

3. Как могут быть реализованы средства контроля целостности, запрещающие загрузку при угрозе нарушения целостности? выбрать все верные

программно
в виде специальных плат, подключаемых к компьютеру
в виде специальных флэш-карт
в виде токенов
в виде смарт-карт

7. Подсистема криптографической защиты

1. Достоинствами аппаратной реализации криптографической защиты данных являются:

высокая производительность и простота
доступность и конфиденциальность
практичность и гибкость
целостность и безопасность

2. Из перечисленного подсистема управления криптографическими ключами структурно состоит из: 1) центра распределения ключей; 2) программно-аппаратных средств; 3) подсистемы генерации ключей; 4) подсистемы защиты ключей

1, 3
1, 2
2, 4
3, 4

3. Чем определяется стойкость криптосистемы RSA?

сложностью извлечения корня степени *e* из большого целого числа по заданному модулю *n*
сложностью разложения на простые сомножители большого целого числа
оба ответа верны

8. Межсетевое экранирование

1. Межсетевой экран, блокирующий все порты, за исключением 80 и 443:

обеспечивает полную защиту web-сервера
является только первой линией обороны web-сервера
не влияет на безопасность web-сервера

2. Выберите правильные утверждения:

Межсетевой экран может анализировать несколько уровней модели OSI
Межсетевой экран может анализировать только один уровень модели OSI
Межсетевой экран может анализировать только прикладной уровень модели OSI

3. Встроенный в ОС межсетевой экран обеспечивает:

лучшую производительность
лучшую масштабируемость
лучшую защиту

9. Правовые, нормативно-технические и организационные требования к криптографическим средствам защиты информации

1. На основании постановления Правительства РФ от 16.04.2012 N 313 к средствам криптографической защиты информации относятся: выбрать все верные

средства шифрования
средства имитозащиты
средства электронной цифровой подписи
средства кодирования
средства изготовления ключевых документов
ключевые документы
носители информации

2. В каких случаях необходимо руководствоваться Положением ПКЗ-2005? выбрать все верные

при организации криптографической защиты информации конфиденциального характера
при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации
при обрабатывании информации конфиденциального характера, обладателем которой являются любые организации

3. К какому типу документа относится приказ ФАПСИ при Президенте Российской Федерации от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности

хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»?

нормативно-правовому
нормативно-техническому
организационному

10. Виртуальные частные сети

2. На каком уровне строятся наиболее распространенные VPN-системы:

транспортном;
прикладном;
сетевом;
канальном

3. В виртуальной частной сети реализуется топология:

любая;
точка-точка;
шина;
в виртуальной частной сети невозможно реализовать топологии.

Аппаратные сети VPN на основе оборудования бывают (Выбрать все верные.):

сети на основе маршрутизаторов
сети на основе брандмауэров

11. Контроль защищенности информации

1. Укажите методы оценки эффективности средств защиты от несанкционированного доступа:

Метод экспертно-документального контроля
Метод тестирования функций, реализованных средствами защиты информации от несанкционированного доступа
Инструментальный метод
Инструментально-расчетный метод

2. Какие виды проверок включает в себя оценка эффективности функционирования средств защиты от несанкционированного доступа?

Проверка подсистемы управления доступом
Проведение инструментальных измерений
Оценка достаточности мер по защите информации на объекте информатизации
Анализ технологического процесса обработки информации на объекте информатизации

3. Проведение контроля эффективности принятых мер по защите информации на объекте информатизации проводится в рамках:

Экспертно-документальной оценки
Оценка эффективности функционирования средств защиты от несанкционированного доступа
Инструментальных измерений и оценки защищенности

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в

зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Основы законодательства об информации, информатизации и защите информации.
2. Основы законодательства об участии в международном информационном обмене.
3. Основы законодательства о правовой охране программ для ЭВМ и баз данных.
4. Общее понятие информационной безопасности. ИБ государства. ИБ предприятия.
5. Модели угроз ИБ.
6. Методы и средства обеспечения ИБ.
7. Класс программно-аппаратных средств обеспечения ИБ
8. Обеспечение требований ИБ на стадиях жизненного цикла создания информационной системы.
9. Криптография. Основные направления. Основные понятия.
10. Симметричный метод шифрования
11. Ассиметричный метод шифрования.
12. Классификация современных программно-аппаратных комплексов обеспечения ИБ.
13. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
14. Виды информации в КС. Информационные потоки в КС. Понятие исполняемого модуля.

15. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
16. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
17. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
18. Политика безопасности в компьютерных системах. Оценка защищенности.
19. Способы защиты конфиденциальности, целостности и доступности в КС.
20. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
21. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).
22. Основные подходы к защите данных от НСД. Шифрование. Контроль доступа. Разграничение доступа.
23. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
24. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
25. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
26. Способы фиксации факторов доступа. Журналы доступа и критерии их информативности.
27. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
28. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
29. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
30. Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения.
31. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.
32. Построение программно-аппаратных комплексов шифрования.
33. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
34. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
35. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.
36. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
37. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.
38. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.
39. Надежность средств защиты компонент. Понятие временной и гарантированной надежности.
40. Несанкционированное копирование программ. Юридические аспекты несанкционированного копирования программ. Несанкционированное копирование программ как тип НСД.
41. Защита программ от несанкционированного копирования (общее понятие защиты от копирования). Разновидности задач защиты от копирования.
42. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.
43. Привязка программ к гибким машинным дискам (ГМД). Структура данных на ГМД. Управление контроллером ГМД.
44. Способы создания некопируемых меток. Точное измерение характеристик форматирования дорожки. Технология «слабых битов».
45. Физические метки и технология работы с ними.
46. Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ.
47. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».
48. Хранение ключей информации.
49. Секретная информация, используемая для контроля доступа: ключи и пароли.
50. Классификация средств хранения ключей и идентифицирующей информации.

51. Организация хранения ключей (с примерами реализации).
52. Магнитные диски прямого доступа.
53. Магнитные и интеллектуальные карты.
54. Средство TouchMemory.
55. Открытое распределение ключей. Метод управляемых векторов.
56. Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО.
57. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды.
58. Временная надежность (невозможность обеспечения гарантированной надежности).
59. Задачи защиты от изучения и способы их решения.
60. Защита от отладки: итеративный программный замок.
61. Защита от отладки: принцип ловушек и избыточного кода.
62. Защита от дизассемблирования. Принцип внешней загрузки файлов.
63. Динамическая модификация программы. Защита от трассировки по прерываниям.
64. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки.
65. Программно-аппаратные средства реализации блочных шифров с секретным ключом в различных режимах функционирования: базовые режимы простой замены, электронной кодовой книги, режимы гаммирования, сцепления блоков.
66. Ключи на базе перепрограммируемой постоянной памяти.
67. Ключи на базе заказных чипов.
68. Примеры реализации ключей (Aktivator, HASP, Alladin и другие).
69. Ключи на базе микропроцессоров.
70. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности.
71. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

Примерный перечень тестовых заданий:

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….

1. информационная война
2. информационное оружие
3. информационное превосходство

1. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

1. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

1. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано

1. надежность

2. точность
3. контролируемость
4. устойчивость
5. доступность

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер

учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 17.04.2026). – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – Текст : электронный.

3. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180093 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

5. Жмуров, Д. Б. Программно-аппаратные средства защиты информации : учебное пособие / Д. Б. Жмуров, С. В. Жуков. — Самара : Самарский университет, 2022. — 80 с. — ISBN 978-5-7883-1799-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/336515 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Царев, Р. Ю. Программные и аппаратные средства информатики : учебник / Р. Ю. Царев, А. В. Прокопенко, А. Н. Князьков ; Сибирский федеральный университет. – Красноярск : Сибирский федеральный университет (СФУ), 2015. – 160 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=435670 (дата обращения: 16.04.2026). – Библиогр. в кн. – ISBN 978-5-7638-3187-0. – Текст : электронный.

2. Бутин, А. А. Программно-аппаратные средства защиты информации : учебное пособие / А. А. Бутин, Н. И. Глухов, С. И. Носков. — 2-е изд., перераб. и доп. — Иркутск : ИрГУПС, 2022. — 92 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342113 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Казарин, О. В. Программно-аппаратные средства защиты информации. защита программного

обеспечения.: учебник и практикум для вузов / Казарин О. В., Забабурин А. С.. – Москва : Юрайт, 2025. – 312 с. – ISBN 978-5-9916-9043-0. – URL: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-562070 (дата обращения: 23.03.2026). – Текст : электронный.

6.3 Методическая литература

1. Программно-аппаратные средства обеспечения информационной безопасности : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 51 с. – URL: http://library.kuzstu.ru/meto.php?n=9103 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286
2. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746
3. Информация и безопасность : научный журнал
4. Прикладная информатика : научно-практический журнал https://eivis.ru/browse/publication/66410
5. САПР и графика : журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Программно-аппаратные средства защиты информации"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Программно-аппаратные средства защиты информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Google Chrome
3. 7-zip
4. Microsoft Windows
5. ESET NOD32 Smart Security Business Edition
6. Kaspersky Endpoint Security
7. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Программно-аппаратные средства защиты информации"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.