МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Программно-аппаратные средства защиты информации»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ Е.Ю. Чапурин

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целями освоения дисциплины «Программно-аппаратные средства защиты информации» являются изучение системы сертификации средств защиты информации и овладение практическими навыками по эксплуатации программно-аппаратных средств защиты информации.

1.2. Задачи освоения дисциплины

- изучение порядка проведения сертификации средств защиты информации;
- изучение программно-аппаратных средств защиты информации, применяемых в автоматизированных системах;
- приобретение знаний о методах обеспечения защиты информации, реализуемых программно-аппаратными средствами защиты информации;
- приобретение знаний и навыков по установке, настройке и эксплуатации программно-аппаратных средств защиты информации, применяемых в автоматизированных системах;
- приобретение знаний и навыков по установке, настройке и эксплуатации средств анализа защищенности информации в автоматизированных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Программно-аппаратные средства защиты информации» направлен на формирование следующих компетенций:

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

ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-2	Знать: – общие принципы построения современных персональных компьютеров; – состав, назначение аппаратных средств и программного обеспечения персонального компьютера;
	Уметь: – применять типовые программные средства сервисного

	назначения, информационного поиска и обмена данными; – составлять документы, используя прикладные программы офисного назначения;
	Владеть: – навыками администрирования и использования средств пользовательских интерфейсов операционных систем
ОПК-15	Знать: – порядок сертификации средств защиты информации; – реестры сертифицированных средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в автоматизированных системах, средств защиты информации
	Уметь: – устанавливать, настраивать, эксплуатировать программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программных и программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при эксплуатации программных и программно-аппаратных средств защиты информации; – использовать типовые программные и программно-аппаратные средства криптографической защиты информации
	Владеть: – навыками установки, настройки, эксплуатации программных и программно-аппаратных средств защиты информации; – навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами защиты

	информации; – навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – навыками установки, настройки и эксплуатации средств анализа защищенности информации в автоматизированных системах; – навыками выявления событий и инцидентов безопасности в автоматизированных системах

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Программно-аппаратные средства защиты информации» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8
Аудиторные занятия (всего)	108	108
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	36	36
Часы на контроль	36	36
Виды промежуточной аттестации - экзамен	+	+
Общая трудоемкость: академические часы зач.ед.	 180 5	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Операционные системы семейства Windows и Linux. Прикладное программное обеспечение, в том числе отечественного производства, предназначенное для решения задач профессиональной деятельности. Специализированное программное обеспечение для подготовки отчетных материалов по результатам аттестационных испытаний на соответствие требованиям по безопасности информации	4	4	4	4	12

2	Система сертификации средств защиты информации	Участники системы сертификации средств защиты информации. Схемы сертификации средств защиты информации. Порядок проведения сертификации средств защиты информации. Реестр сертифицированных средств защиты информации	6	6	6	6	24
3	Средства антивирусной защиты информации	Назначение средства антивирусной защиты информации. Разграничение доступа к управлению средством антивирусной защиты информации. Управление работой средства антивирусной защиты информации. Управление параметрами средства антивирусной защиты информации. Управление установкой обновлений (актуализации) баз данных признаков компьютерных вирусов средства антивирусной защиты информации. Аудит безопасности средства антивирусной защиты информации. Выполнение проверок объектов воздействия. Обработка объектов воздействия. Сигнализация средства антивирусной защиты информации. Ограничения программной среды.	2	2	2	2	8
4	Средства защиты информации от несанкционированного доступа	Назначение средств защиты информации от несанкционированного доступа. Основные функции средств защиты информации от несанкционированного доступа. Состав устанавливаемых компонентов средств защиты информации от несанкционированного доступа. Механизм защиты входа в систему. Идентификация и аутентификация пользователей. Блокировка компьютера. Дискреционное управление доступом. Мандатное управление доступом. Контроль целостности. Разграничение доступа к устройствам. Контроль подключения и изменения устройств компьютера. Контроль печати. Регистрация событий. Работа с журналами регистрации событий. Построение отчетов по журналу регистрации событий.	8	8	8	8	32
5	Средства доверенной загрузки	Назначение программно-аппаратного комплекса доверенной загрузки. Варианты исполнения и принципы функционирования программно-аппаратного комплекса доверенной загрузки. Механизм идентификации и аутентификации. Управление пользователями программно-аппаратного комплекса. Механизм блокировки загрузки операционных систем со съемных носителей. Механизм контроля целостности. Подготовка к инициализации. Выполнение инициализации программно-аппаратного комплекса доверенной загрузки. Настройка и эксплуатация программно-аппаратного комплекса доверенной загрузки.	4	4	4	4	16
6	Средства криптографической защиты информации и межсетевые экраны	Назначение аппаратно-программного комплекса шифрования. Состав аппаратно-программного комплекса шифрования. Принципы функционирования	6	6	6	6	24

		аппаратно-программного комплекса шифрования. Аутентификация пользователей аппаратно-программного комплекса шифрования. Обеспечение отказоустойчивости аппаратно-программного комплекса шифрования. Журналы регистрации событий аппаратно-программного комплекса шифрования. Управление криптографическими ключами аппаратно-программного комплекса шифрования. Процедуры генерации, распределения и смены ключей. Принципы функционирования межсетевых экранов. Программные и программно-аппаратные межсетевые экраны.					
7	Средства анализа защищенности	Назначение средства анализа защищенности. Область применения средства анализа защищенности. Выявление и анализ уязвимостей. Контроль установки обновлений операционных систем. Контроль параметров настройки комплекса средств защиты операционных систем специального назначения. Контроль состава технических средств, программного обеспечения и средств защиты информации. Обеспечение контроля реализации правил разграничения доступа. Контроль целостности программного обеспечения. Контроль уничтожения информации и обеспечение поиска остаточной информации на машинных носителях. Идентификация и аутентификация. Сбор, запись и хранение информации о событиях безопасности	6	6	6	6	24
		Итого	**36**	**36**	**36**	**36**	**144**

5.2 Перечень лабораторных работ

– установка операционной системы семейства «Windows» в среде виртуализации с последующей установкой прикладного и специализированного программного обеспечения необходимого для решения задач профессиональной деятельности;

– установка операционной системы семейства «Linux» в среде виртуализации с последующей установкой прикладного и специализированного программного обеспечения необходимого для решения задач профессиональной деятельности;

– подготовка пакета документов для проведения сертификации средств защиты информации;

– установка и настройка средства антивирусной защиты информации;

– установка и настройка дискреционного и мандатного управления доступом к информации средства защиты информации от несанкционированного доступа;

– установка и настройка средства защиты информации от несанкционированного доступа в соответствии с установленным классом защищенности;

– установка, настройка и эксплуатация программно-аппаратного комплекса доверенной загрузки;

– развертывание и эксплуатация аппаратно-программного комплекса шифрования и межсетевого экранирования;

– установка, настройка и эксплуатация средств анализа защищенности.

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-2	Знать: – общие принципы построения современных персональных компьютеров; – состав, назначение аппаратных средств и программного обеспечения персонального компьютера;	Знает общие принципы построения современных персональных компьютеров; состав, назначение аппаратных средств и программного обеспечения персонального компьютера	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: – применять типовые программные средства сервисного назначения, информационного поиска и обмена данными; – составлять документы, используя прикладные программы офисного назначения;	Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными; составлять документы, используя прикладные программы офисного назначения	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: – навыками администрирования и использования средств пользовательских интерфейсов операционных систем	Владеет навыками администрирования и использования средств пользовательских интерфейсов операционных систем	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-15	Знать: – порядок сертификации средств защиты информации; – реестры сертифицированных средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств защиты информации в	Знает порядок сертификации средств защиты информации; реестры сертифицированных средств защиты информации; особенности и способы применения программных и	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	автоматизированных системах; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в автоматизированных системах, средств защиты информации	программно-аппаратных средств защиты информации в автоматизированных системах; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; типовые средства и методы ведения аудита, средств и способов защиты информации в автоматизированных системах, средств защиты информации		
	Уметь: – устанавливать, настраивать, эксплуатировать программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программных и программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при эксплуатации программных и программно-аппаратных средств защиты информации; – использовать типовые программные и программно-аппаратные средства криптографической защиты информации	Умеет устанавливать, настраивать, эксплуатировать программные и программно-аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программных и программно-аппаратных средств защиты информации; проверять выполнение требований по защите информации от несанкционированного доступа при эксплуатации программных и программно-аппаратных средств защиты информации; использовать типовые программные и программно-аппаратные средства криптографической защиты информации	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть: – навыками установки, настройки, эксплуатации программных и программно-аппаратных средств защиты информации; – навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами защиты информации; – навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных	Владеет навыками установки, настройки, эксплуатации программных и программно-аппаратных средств защиты информации; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами защиты информации; навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных	Выполнение работ в срок, предусмотренных в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	средств защиты информации; – навыками установки, настройки и эксплуатации средств анализа защищенности информации в автоматизированных системах; – навыками выявления событий и инцидентов безопасности в автоматизированных системах	средств защиты информации; навыками установки, настройки и эксплуатации средств анализа защищенности информации в автоматизированных системах; навыками выявления событий и инцидентов безопасности в автоматизированных системах		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-2	Знать: – общие принципы построения современных персональных компьютеров; – состав, назначение аппаратных средств и программного обеспечения персонального компьютера;	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: – применять типовые программные средства сервисного назначения, информационного поиска и обмена данными; – составлять документы, используя прикладные программы офисного назначения;	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: – навыками администрирования и использования средств пользовательских интерфейсов операционных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

ОПК-15	Знать: – порядок сертификации средств защиты информации; – реестры сертифицированных средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в автоматизированных системах, средств защиты информации	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь: – устанавливать, настраивать, эксплуатировать программные и программно-аппаратные средства защиты информации; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программных и программно-аппаратных средств защиты информации; – проверять выполнение требований по защите информации от несанкционированного доступа при эксплуатации программных и программно-аппаратных средств защиты информации; – использовать типовые программные и программно-аппаратные средства криптографической защиты информации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть: – навыками установки, настройки, эксплуатации программных и	Решение прикладных задач в	Задачи решены в полном	Продемонстрирован верный ход	Продемонстрирован верный ход решения в	Задачи не решены

	программно-аппаратных средств защиты информации; – навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами защиты информации; – навыками тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – навыками установки, настройки и эксплуатации средств анализа защищенности информации в автоматизированных системах; – навыками выявления событий и инцидентов безопасности в автоматизированных системах	конкретной предметной области	объеме и получены верные ответы	решения всех, но не получен верный ответ во всех задачах	большинстве задач	

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Подлежат ли сертификации в системе сертификации ФСТЭК России средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации?

- Да;
- Нет.

2. Кто относится к участникам системы сертификации ФСТЭК России?

- федеральный орган по сертификации;
- организации, аккредитованные ФСТЭК России в качестве органа по сертификации;
- организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории;
- все вышеперечисленные.

3. Срок действия сертификата соответствия не может превышать…?

- 3 года;
- 4 года;
- 5 лет;
- 6 лет.

4. Что из перечисленного не входит в процедуры сертификации средств защиты информации?

- подача заявки на сертификацию;
- принятие решения о проведении сертификации средства защиты информации;
- аттестационные испытания средства защиты информации;
- выдача (отказ в выдаче) сертификата соответствия.

5. Что не указывается в заявке на сертификацию средства защиты информации?

- наименование средства защиты информации;
- назначение средства защиты информации;
- графические изображения функционирования средства защиты информации;
- заявляемый срок действия сертификата соответствия.

6. Допускается ли проводить сертификацию (сертификационные испытания) средства защиты информации до принятия решения о проведении сертификации средства защиты информации?

- нет;
- да.

7. В течение какого времени орган по сертификации рассматривает программу и методику сертификационных испытаний средства защиты информации и при отсутствии недостатков утверждает их?

- 30 рабочих дней;
- 30 календарных дней;
- 10 рабочих дней;
- 10 календарных дней.

8. На основании какого документа заявитель организует маркирование средств защиты информации знаками соответствия?

- аттестата соответствия;
- сертификата соответствия;
- заключения по результатам сертификации средства защиты информации;
- протокола по результатам сертификации средства защиты информации.

9. Сертификат соответствия средства защиты информации подлежит переоформлению в случае:

- реорганизации заявителя в форме преобразования;
- изменения наименования заявителя;
- изменения местонахождения заявителя;
- внесения изменений в сертифицированное средство защиты

информации, требующих внесения изменений в сертификат соответствия.

10. На какой срок может быть приостановлено действие сертификата соответствия средства защиты информации?

- не более 90 календарных дней;
- не более 90 рабочих дней;
- не более 10 календарных дней;
- не более 45 рабочих дней.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Основными этапами классификации автоматизированной системы являются:

- разработка и анализ исходных данных;
- выявление основных признаков автоматизированной системы, необходимых для классификации;
- сравнение выявленных признаков автоматизированной системы с классифицируемыми;
- присвоение автоматизированной системы соответствующего класса защиты информации от несанкционированного доступа.

2. Необходимыми исходными данными для проведения классификации конкретной автоматизированной системы являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам автоматизированной системы, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам автоматизированной системы;
- режим обработки данных в автоматизированной системе.

3. Сколько устанавливается классов защищенности автоматизированной системы от несанкционированного доступа к информации?

- 9;
- 5;
- 4;
- 3.

4. Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств – это...?

-автоматизированная система;
-информационная система;
-информационно-телекоммуникационная сеть.

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя - это...?

-целостность информации;

-конфиденциальность информации;

-доступность информации.

6. Совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица – это…?

- авторизация;
- аутентификация;
- идентификация.

7. Совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным – это…?

- авторизация;
- аутентификация;
- идентификация.

8. Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации – это…?

-средство защиты информации;

-средство антивирусной защиты;

-средство защиты информации от несанкционированного доступа.

9. Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации – это...?

- вредоносное программное обеспечение;
- уязвимость;
- порт.

10. Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации,

организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации – это…?

- средство защиты информации;
- система защиты информации;
- объект защиты.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Какие функциональные модули включает в себя система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C»?

- систему защиты информации от несанкционированного доступа;
- средство контроля съемных машинных носителей информации;
- персональный межсетевой экран;
- систему обнаружения вторжений.

2. До какого класса защищенности автоматизированных систем, в соответствии с Руководящим документом. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации (Гостехкомиссия России, 1992), может применяться система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C»?

- 2А включительно;
- 1А включительно;
- 1Б включительно.

3. Возможно ли эксплуатировать систему защиты информации от несанкционированного доступа «Dallas Lock 8.0-C» и программно-аппаратный комплекс «Соболь» одновременно на персональном компьютере?

- Нет;
- Да.

4. Какие основные функции выполняет средство защиты информации «Secret Net Studio – C»?

- защиту от несанкционированного доступа к информационным ресурсам компьютера;
- поиск и ликвидация компьютерных вирусов;
- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений.

5. Какие компоненты входят в состав средства защиты информации «Secret Net Studio – C»?

- «Secret Net Studio – Сервер безопасности»;
- «Secret Net Studio – Центр управления»;
- «Secret Net Studio – Клиент»;
- «Secret Net Studio – Антивирус».

6. Какие виды разграничения доступа к файловым ресурсам реализованы в средстве защиты информации «Secret Net Studio – C»;

- Дискреционное разграничение доступа;
- Мандатное разграничение доступа;
- Ролевое разграничение доступа.

7. Программный комплекс «Средство анализа защищенности «Сканер-ВС» предназначен для…?

- автоматизированного анализа (контроля) защищенности информации;
- автоматизированного анализа (контроля) защищенности информации и защиты информации от несанкционированного доступа;
- автоматизированного анализа (контроля) защищенности информации и доверенной загрузке операционных систем.

8. Какие функции безопасности реализует программный комплекс «Средство анализа защищенности «Сканер-ВС»?

- выявление и анализ уязвимостей информационной системы;
- контроль состава технических средств, программного обеспечения и средств защиты информации;
- обеспечение контроля использования беспроводных сетей в информационной системе;
- разграничение доступа на базе ролевой модели доступа.

9. Выполняет ли программный комплекс «Средство анализа защищенности «Сканер-ВС» такую функцию безопасности как контроль параметров настройки комплекса средств защиты операционной системы специального назначения?

- Да;
- Нет.

10. Какое средство защиты информации относится к средствам криптографической защиты информации?

- программно-аппаратный комплекс «Соболь»;
- средство защиты информации «ViPNet Client»;
- система защиты информации от несанкционированного доступа «Dallas Lock 8.0-C»;
- программное изделие «Kaspersky Endpoint Security для Windows».

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Термины, относящиеся к средствам обеспечения информационной безопасности организации.
2. Ответственность, предусмотренная за неправомерный доступ к

компьютерной информации.

3. Ответственность, предусмотренная за создание, использование и распространение вредоносных компьютерных.

4. Ответственность, предусмотренная за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

5. Ответственность, предусмотренная за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

6. Перечень сведений конфиденциального характера.

7. Участники сертификации средств защиты информации.

8. Участники системы, а также схемы сертификации средств защиты информации.

9. Процедуры сертификации средств защиты информации.

10. Порядок подачи заявки на сертификацию средства защиты информации.

11. Порядок принятия решения о проведении сертификации средства защиты информации.

12. Порядок сертификационных испытаний средства защиты информации.

13. Порядок оформления экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия.

14. Порядок выдачи (отказ в выдаче) сертификата соответствия средства защиты информации.

15. Порядок предоставления дубликата сертификата соответствия средства защиты информации.

16. Порядок маркирования средств защиты информации.

17. Порядок внесения изменений в сертифицированное средство защиты информации.

18. Порядок переоформления сертификата соответствия средства защиты информации.

19. Порядок продления срока действия сертификата соответствия средства защиты информации.

20. Порядок приостановления действия сертификата соответствия средства защиты информации.

21. Порядок прекращения действия сертификата соответствия средства защиты информации.

22. Функциональные модули, реализованные в системе защиты информации от несанкционированного доступа, и их характеристики.

23. Ограничения по эксплуатации системы защиты информации от несанкционированного доступа.

24. Возможность применения средства анализа защищенности в информационных (автоматизированных) системах.

25. Функции безопасности, реализуемые средством анализа

защищенности. Их характеристики мер защиты.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 2 письменных вопроса и 5 тест-вопроса. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, письменный вопрос оценивается в 5 баллов. Максимальное количество набранных баллов – 15.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 7 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 7 до 9 баллов.

3. Оценка «Хорошо» ставится в случае, если студент набрал от 10 до 12 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 13 до 15 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
2	Система сертификации средств защиты информации	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
3	Средства антивирусной защиты информации	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
4	Средства защиты информации от несанкционированного доступа	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
5	Средства доверенной загрузки	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
6	Средства криптографической защиты информации и межсетевые экраны	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата
7	Средства анализа защищенности	ОПК-2, ОПК-15	Тест, контрольная работа, защита лабораторных работ, защита реферата

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методике выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Толстых Н.Н. Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс] : Учеб.пособие / Н.Н. Толстых. - Электрон.текстовые, граф. дан. (1,75 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2. Толстых Н.Н. Введение в теорию конфликтного функционирования информационных и информационно-управляющих систем: учеб.пособие / Н.Н. Толстых, В.А. Павлов, Е. И. Воробьева. - Воронеж: ВГТУ, 2003. - 169 с. - 30-00.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

1. Электронная информационно-образовательная среда ВГТУ. – Электрон. дан. – Режим доступа : https://old.education.cchgeu.ru/.

2. Электронный каталог Научной библиотеки ВГТУ. – Электрон. дан. – Режим доступа : http://bibl.cchgeu.ru/MarcWeb2/Found.asp.

3. Научная электронная библиотека «eLIBRARY.RU». – Электрон. дан. – Режим доступа : https://elibrary.ru/defaultx.asp.

4. Электронно-библиотечная система «IPRbooks». – Электрон. дан. – Режим доступа : https://www.iprbookshop.ru/.

5. Национальная Электронная Библиотека. – Электрон. дан. – Режим доступа : https://rusneb.ru/.

6. Электронно-библиотечная система «Университетская библиотека онлайн». – Электрон. дан. – Режим доступа : https://biblioclub.ru/.

7. Электронно-библиотечная система «ЭБС-ЮРАЙТ». – Электрон. дан. – Режим доступа : https://urait.ru/.

8. Электронная справочно-правовая система «КонсультантПлюс». – Электрон. дан. – Режим доступа : http://www.consultant.ru/.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Лекционная аудитория с возможностью воспроизведения подготовленных презентационных материалов на мультимедийном оборудовании.

Аудитория для проведения лабораторных и практических занятий, оборудованная средствами вычислительной техники, с предустановленным программным обеспечением.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Программно-аппаратные средства защиты информации» читаются лекции, проводятся практические занятия и лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков расчета. Занятия проводятся путем решения конкретных задач в аудитории.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое	Конспектирование рекомендуемых источников. Работа с

занятие	конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.