ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.1.31 Программно–аппаратные средства обеспечения информационной безопасности

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины:

- изучение программно-аппаратных средств защиты информации на объектах информатизации

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно–аппаратные средства обеспечения информационной безопасности» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Программно –аппаратные средства обеспечения информационной безопасности» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Курс полного школьного среднего образования. Информатика.
ПК-8	Курс полного школьного среднего образования. Информатика.
ПК-20	Курс полного школьного среднего образования. Информатика.
ПК-24	Курс полного школьного среднего образования. Информатика.
ПК-25	Курс полного школьного среднего образования. Информатика.

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-8	Технология защиты информации в различных отраслях деятельности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-20	Экономика и менеджмент в информационной безопасности критически важных объектов Основы менеджмента Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-24	Экономика и менеджмент в информационной безопасности критически важных объектов Основы менеджмента Преддипломная практика

	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-25	Экономика и менеджмент в информационной безопасности критически важных объектов Основы менеджмента Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению своей профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной деятельности	Этап1: основополагающие термины и понятия; предметную область, цели, состав и значение информационных ресурсов организации; характеристики основных классов информационных технологий; Этап 2: базовые концепции корпоративных информационных систем; современное состояние отечественного рынка программного обеспечения корпоративных информационных систем.	Этап1: самостоятельно изучать специальную литературу; Этап 2: проводить исследования в коммуникативном пространстве организации; оценивать эффективность коммуникаций в организации и анализировать причины их недостаточной эффективности; определять перспективные направления и пути совершенствования коммуникационной системы.	Этап 1: владеть навыками использования компьютерной техники и информационных технологий Этап 2: владеть основами информационно-аналитической деятельности и способностью их применить в профессиональной сфере
ПК-8 - способностью разрабатывать и анализировать проектные решения	Этап 1: основные этапы проектирования подсистемы	Этап 1: разрабатывать основные подсистемы	Этап 1: навыки разработки подсистем информационной безопасности

по обеспечению безопасности автоматизированных систем	информационной безопасности	безопасности информации	
ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 2: навыки технико - экономического обоснования проектных решений
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Этап 1: принципы разработки и внедрения информационных систем;	Этап 1: использовать методы разработки и внедрения информационных систем	Этап 1: методами разработки, внедрения, эксплуатации информационных систем
ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Этап 2: принципы эффективного применения автоматизированных информационных систем с учетом требований информационной безопасности	Этап 2: реализовать разработку автоматизированной информационной системы с учетом требований информационной безопасности	Этап 2: методами сопровождения информационных систем
ПК-24 - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	Этап 1: принципы эффективного применения информационно-технологических ресурсов;	Этап 1: использовать методы эффективного применения информационно-технологических ресурсов	Этап 1: методами разработки, внедрения, эксплуатации информационно-технологических ресурсов
ПК-24 - способностью	Этап 2: принципы	Этап 2:	Этап 2: методами

обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	информационной безопасности	реализовать политику информационной безопасности	сопровождения информационно-технологических ресурсов
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Этап 1: принципы эффективной реализации резервного копирования данных;	Этап 1: использовать методы резервного копирования данных	Этап 1: методами разработки, внедрения, эксплуатации резервного копирования данных
ПК-25 - способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	Этап 2: принципы информационной безопасности в процессах резервного копирования данных	Этап 2: реализовать политики информационной безопасности для процессов резервного копирования данных	Этап 2: методами сопровождения резервного копирования данных

4. Объем дисциплины

Объем дисциплины «Программно–аппаратные средства обеспечения информационной безопасности» составляет 6 зачетных единиц (216 академических часа), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 7		Семестр № 8	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	34		16		18	
2	Лабораторные работы (ЛР)	18				18	
3	Практические занятия (ПЗ)	50		32		18	
4	Семинары(С)						
5	Курсовое проектирование (КП)	2	20			2	20
6	Рефераты (Р)						
7	Эссе (Э)						
8	Индивидуальные домашние задания (ИДЗ)						
9	Самостоятельное изучение вопросов (СИВ)		36		18		18
10	Подготовка к занятиям (ПкЗ)		50		40		10
11	Промежуточная аттестация	6		2		4	
12	Наименование вида промежуточной аттестации	Х	х	зачет		экзамен	
13	Всего	110	106	50	58	60	48

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Программно-аппаратная защита информации**	**7**	**16**		**32**			**x**		**18**	**40**	**x**	**ОК-5, ПК-8, ПК-20, ПК-24, ПК-25**
1.1.	**Тема 1** Основные понятия программно-аппаратной защиты информации	7	8		16			x		8	20	x	**ОК-5**, ПК-8, ПК-25
1.2.	**Тема 2** Идентификация пользователей КС-субъектов доступа к данным	7	8		16			x		10	20	x	ПК-8, ПК-20, ПК-24, ПК-25
2.	**Контактная работа**	**7**	**16**		**32**			**x**				**2**	**x**
3.	**Самостоятельная работа**	**7**								**18**	**40**		**x**
4.	**Объем дисциплины в семестре**	**7**	**16**		**32**					**18**	**40**	**2**	**x**
5.	**Раздел 2 Средства ограниченного доступа**	**8**	**18**	**18**	**18**		**22**	**x**		**18**	**10**	**x**	**ПК-8, ПК-20, ПК-24, ПК-25**

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
5.1.	**Тема 3** Средства и методы ограничения доступа к файлам	8	4	4	4		8	х		4	4	х	**ОК-5** , ПК-24, ПК-25
5.2.	**Тема 4** Методы и средства ограничения доступа к компонентам ЭВМ	8	4	4	4		8	Х		4	2	х	ПК-8, ПК-20,
5.3.	**Тема 5** Защита программ и данных от несанкционированного копирования	8	4	4	4		4	Х		4	2	х	**ОК-5** ПК-8, ПК-20, ПК-25
5.4.	**Тема 6** Управление криптографическими ключами	8	6	6	6		2	х		6	2	х	ПК-8, ПК-20, ПК-24,
6.	**Контактная работа**	**8**	**18**	**18**	**18**		**2**	**х**				**4**	**х**
7.	**Самостоятельная работа**	**8**					**20**			**18**	**10**		**х**
8.	**Объем дисциплины в семестре**	**8**	**18**	**18**	**18**		**22**			**18**	**10**	**4**	**х**
9.	**Всего по дисциплине**	**Х**	**34**	**18**	**50**		**22**			**36**	**50**	**6**	**х**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Семестр №7		
Л-1	Предмет и задачи программно-аппаратной защиты информации	**2**
Л-2	Политика безопасности в компьютерных системах. Оценка защищенности	**2**
Л-3	Нормативно-методическое обеспечение создания АС	**2**
Л-4	Основные понятия и концепции	**2**
Л-5	Взаимная проверка подлинности пользователей	**2**
Л-6	Схема идентификации гиллоу-куискуотера	**2**
Л-7	Защита информации в кс от несанкционированного доступа	**2**
Л-8	Концепция построения систем разграничения доступа	**2**
Семестр №8		
Л-9	Защита информации, обрабатываемой пэвм и лвс, от утечки по сети электропитания	**2**
Л-10	Защита программ и данных от несанкционированного копировани	**2**
Л-11	Особенности проектирования на современном уровне и синтез	**2**
Л-12	Методы и методики проектирования КСИБ от НСД	**2**
Л-13	Методы и методики оценки КСИБ	**2**
Л-14	Генерация ключей	**2**
Л-15	Особенности эксплуатации КСИБ на объекте защиты	**2**
Л-16	Модели защиты информации	**2**
Л-17	Реализация системы управления доступом	**2**
Итого по дисциплине		**34**

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
ЛР-1	Защита информации в пэвм	**2**
ЛР-2	Виды мероприятий по защите информации	**2**
ЛР-3	Современные системы защиты пэвм от несанкционированного доступа к информации	**2**
ЛР-4	Методы, затрудняющие считывание скопированной информации	**2**
ЛР-5	Методы, препятствующие использованию скопированной информации	**2**
ЛР-6	«Основные функции средств защиты от копирования	**2**
ЛР-7	Хранение ключей	**2**
ЛР-8	Распределение ключей	**2**
ЛР-9	Определение открытых ключей	**2**
Итого по дисциплине		**18**

5.2.3 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
Семестр №7		
ПЗ-1	Основные понятия	**2**
ПЗ-2	Уязвимость компьютерных систем	**2**
ПЗ-3	Механизмы защиты	**2**
ПЗ-4	Идентификация и аутентификация пользователя	**2**
ПЗ-5	Протоколы идентификации с нулевой передачей знаний	**2**
ПЗ-6	Биометрическая идентификация и аутентификация пользователя	**2**
ПЗ-7	Парольная аутентификация	**2**
ПЗ-8	Система разграничения доступа к информации в кс	**2**
ПЗ-9	Методы разграничения доступа	**2**
ПЗ-10	Организация доступа к ресурсам кс	**2**
ПЗ-11	Обеспечение целостности и доступности информации в кс	**2**
ПЗ-12	Защита информации в пэвм	**2**
ПЗ-13	Виды мероприятий по защите информации	**2**
ПЗ-14	Современные системы защиты пэвм от несанкционированного доступа к информации	**2**
ПЗ-15	Основные методы защиты от копирования	**2**
Семестр №8		
16	Методы противодействия динамическим способам снятия защиты программ от копирования	**2**
ПЗ-17	Защита при помощи компьютерных компакт-дисков	**2**
ПЗ-18	Протокол аутентификации и распределения ключей для симметричных криптосистем	**2**
ПЗ-19	Уязвимость компьютерных систем	**2**
ПЗ-20	Механизмы защиты	**2**
ПЗ-21	Идентификация и аутентификация пользователя	**2**
ПЗ-22	Протоколы идентификации с нулевой передачей знаний	**2**
ПЗ-23	Биометрическая идентификация и аутентификация пользователя	**2**
ПЗ-24-25	Парольная аутентификация	**4**
Итого по дисциплине		**50**

5.2.4 Темы курсовых работ (проектов)

1. Анализ аппаратных средств защиты ПК
2. Разработка ПС на основе асимметричного шифрования для защиты ОС.
3. Разработка ПС для защиты ОС с помощью цветовой схемы.
4. Разработка программно-аппаратного комплекса для защиты ОС.
5. Разработка электронного ключа для защиты от несанкционированного доступа к ПК

6. Разработка ПС для защиты от спама
7. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
8. Анализ существующих методов защиты ОС
9. Разработка ПС для защиты от фишинговых атак
10. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
11. Разработка электронного ключа для доступа к ПК
12. Разработка межсетевого экрана
13. Создание системы защиты локальной сети от несанкционированного доступа
14. Разработка системы управления сайтом с дополнительной аутентификацией пользователя
15. Разработка ПС для аутентификации пользователя с помощью графического изображения.
16. Разработка аппаратно-программного комплекса защиты ПК
17. Анализ существующих ПС по защите локальных сетей от внешних атак
18. Анализ существующих методов защиты ОС Linux
19. Разработка программного средства защиты ОС Linux
20. Разработка комплексной системы защиты серверной ОС

5.2.5 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Основные понятия программно-аппаратной защиты информации	Основные процессы жизненного цикла АС. Оценка защищенности КС. Взаимосвязь между стандартными процессами и стадиями.	8
2.	Идентификация пользователей КС-субъектов доступа к данным	Идентификация объекта. Защита при обмене. Сведения о системе защиты информации. Знания о КС и умения работать с ней.	10
3.	Средства и методы ограничения доступа к файлам.	Идентификация и аутентификация субъекта доступа Проверка прав доступа субъекта к объекту	4
4.	Методы и средства ограничения доступа к компонентам ЭВМ	Обеспечение некопируемости дистрибутивных дисков стандартными средствами. Обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами	4
5.	Защита программ и данных от несанкционированного копирования	Использование типовых СЗИ. Использование типовых	4

		структурно-ориентированных компонентов СЗИ	
6.	Управление криптографическими ключами	Криптографические методы. Метод привязки к идентификатору	6
Итого по дисциплине			

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Аверченков В.И. Разработка системы технической защиты информации: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - М.: ФЛИНТА, 2011 г. – 187 с.
2. Аверченков В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М.: ФЛИНТА, 2011 г. - 184 с.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - М.: ФЛИНТА, 2011 г. - 224 с.
2. Аверченков В.И. Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, М.В. Рудановский, А.В. Кувыклин. - М.: ФЛИНТА, 2011 г. - 100 с.
3. Аверченков В.И. Методы и средства инженерно-технической защиты информации: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин . - М.: ФЛИНТА, 2011 г. - 187 с.

6.3 Методические материалы для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:
- конспект лекций;
- методические материалы по выполнению лабораторных работ;
- методические материалы по выполнению практических (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие, включающее:
- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям;
- методические рекомендации по выполнению курсовой работы (проекта).

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Open Office
2. JoliTest (JTRun, JTEditor, TestRun)

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.intuit.ru/studies/courses/1162/285/lecture/7164?page=2

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение лабораторных работ

Номер ЛР	Тема лабораторной работы	Название лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ЛР-1	Предмет и задачи программно-аппаратной защиты информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ЛР-2	Политика безопасности в компьютерных системах	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ЛР-3	Нормативно-методическое обеспечение создание АС	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ЛР-4	Основные понятия и концепции	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ЛР-5	Взаимная проверка подлинности пользователей	941 аудитория – лаборатория программно-аппаратных	ПЭВМ	Офисный пакет OpenOffice

		средств защиты информации		
ЛР-6	Схема идентификации Гиллоу-Куискуотера	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ЛР-7	Защита информации в КС от несанкционированного доступа	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ЛР-8	Концепция построения систем разграничения доступа	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ЛР-9	Защита информации в ПЭВМ	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;

Таблица 7.2 – Материально-техническое обеспечение практических работ

Номер ПЗ	Тема занятия	Название аудитории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Основные понятия	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-2	Уязвимость компьютерных систем	941 аудитория – лаборатория программно-	ПЭВМ	Операционные системы Windows XP/7;

		аппаратных средств защиты информации		
ПЗ-3	Механизмы защиты	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-4	Идентификация и аутентификация пользователя	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-5	Протоколы идентификации с нулевой передачей знаний	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-6	Биометрическая идентификация и аутентификация пользователя	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-7	Методы разграничения доступа	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-8	Защита информации в пэвм	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-9	Виды мероприятий по защите	941 аудитория – лаборатория	ПЭВМ	Интегрированный пакет MS Office

	информации	программно-аппаратных средств защиты информации		Standard;
ПЗ-10	Современные системы защиты пэвм от несанкционированного доступа к информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-11	Основные методы защиты от копирования	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-12	Методы противодействия динамическим способам снятия защиты программ от копирования	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-13	Защита при помощи компьютерных компакт-дисков	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-14	Протокол аутентификации и распределения ключей для симметричных криптосистем	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-15	Протокол аутентификации и распределения ключей Kerberos	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;

ПЗ-16	Модель взаимодействия клиента с серверами	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-17	Криптографические методы	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-18	Метод привязки к идентификатору	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-19	Автокорреляция	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-20	Переустановка векторов прерываний	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-21	Разграничение доступа к файлам, каталогам, дискам	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-22	Защита процесса загрузки ОС	941 аудитория – лаборатория программно-аппаратных	ПЭВМ	Офисный пакет OpenOffice

		средств защиты информации		
ПЗ-23	Проверка целостности информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-24-25	Исключение несанкционированного использования хранящихся в ПЭВМ программ	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): _____ Ю.В. Полищук