

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Кандрашина Елена Александровна

Должность: Врио ректора ФГАОУ ВО «Самарский государственный экономический университет»

Дата подписания: 07.07.2023 13:20:47

Уникальный программный ключ:

b2fd765521f4c570b8c6e8e502a10b4f1de8ae0d

**Министерство науки и высшего образования Российской Федерации**  
**Федеральное государственное автономное образовательное учреждение**  
**высшего образования**  
**«Самарский государственный экономический университет»**

**Институт**      Институт экономики предприятий

**Кафедра**      Прикладной информатики

**УТВЕРЖДЕНО**

Ученым советом Университета

(протокол № 11 от 30 мая 2023 г.)

**РАБОЧАЯ ПРОГРАММА**

**Наименование дисциплины**

Б1.В.14 Программно-аппаратная защита информации

**Основная профессиональная образовательная программа**

09.03.03 Прикладная информатика программа  
Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2023

## Содержание (рабочая программа)

Стр.

- 1 Место дисциплины в структуре ОП
- 2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 3 Объем и виды учебной работы
- 4 Содержание дисциплины
- 5 Материально-техническое и учебно-методическое обеспечение дисциплины
- 6 Фонд оценочных средств по дисциплине

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

## 1. Место дисциплины в структуре ОП

Дисциплина Программно-аппаратная защита информации входит в часть, формируемая участниками образовательных отношений блока Б1. Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования, Основы проектной деятельности, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Системы искусственного интеллекта, Облачные технологии и услуги, Технологии защищенного документооборота, Правовая защита информации, Методы и средства защиты информации, Информационно-коммуникационные технологии в профессиональной деятельности, Встроенные языки программирования, Организация вычислительных процессов, Технологии работы в социальных сетях

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Проектный практикум, Проектирование информационных систем, Управление информационной безопасностью, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности, Цифровая культура в профессиональной деятельности, Интеллектуальные информационные системы, Современные цифровые технологии управления предприятием

## 2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Программно-аппаратная защита информации в образовательной программе направлено на формирование у обучающихся следующих компетенций:

### Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	<b>Планируемые результаты обучения по дисциплине</b>		
ПК-1	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по	<b>Планируемые результаты обучения по дисциплине</b>
------------------------------------	--

программе			
ПК-2	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств

ПК-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

Планируемые результаты обучения по программе	<b>Планируемые результаты обучения по дисциплине</b>		
ПК-3	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь навыки):
	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	<b>Планируемые результаты обучения по дисциплине</b>		
ПК-4	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

### 3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

#### Очная форма обучения

<b>Виды учебной работы</b>	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	36.15/1

Занятия лекционного типа	18/0.5
Занятия семинарского типа	18/0.5
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	53.85/1.5
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы	108
Зачетные единицы	3

#### заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 7
Контактная работа, в том числе:	4.15/0.12
Занятия лекционного типа	2/0.06
Занятия семинарского типа	2/0.06
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	85.85/2.38
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной программы): Часы	108
Зачетные единицы	3

#### 4. Содержание дисциплины

##### 4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Программно-аппаратная защита информации представлен в таблице.

#### Разделы, темы дисциплины и виды занятий Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	10	9	0.1	33	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК- 2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3	
2.	Программно-аппаратные средства, реализующие отдельные функциональные	8	9	0.05	20.85	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК- 2.2, ПК-2.3,	

	требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.						ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3
	Контроль	18					
	<b>Итого</b>	<b>18</b>	<b>18</b>	<b>0.15</b>		<b>53.85</b>	

#### заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе	
		Лекции	Занятия семинарского типа		ИКР			ГКР
			Практич. занятия					
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	1	1	0.1		55	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК- 2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3	
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	1	1	0.05		30.85	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК- 2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3	
	Контроль	18						
	<b>Итого</b>	<b>2</b>	<b>2</b>	<b>0.15</b>		<b>85.85</b>		

## 4.2 Содержание разделов и тем

### 4.2.1 Контактная работа

#### Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	лекция	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
		лекция	Категории и модели информационной безопасности
		лекция	Идентификация и аутентификация пользователей. Понятие

			несанкционированного доступа.
		лекция	Основные подходы к защите данных от НСД
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	лекция	Программно-аппаратные средства шифрования.
		лекция	Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
		лекция	Биометрические средства защиты информации и разграничения доступа
		лекция	Программно-аппаратные средства защиты информации в сетях передачи данных
		лекция	Аудит безопасности корпоративных систем

\*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

#### Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	практическое занятие	Обеспечение безопасности доступа к данным информационной системы организации с помощью продуктов Microsoft и Aladdin. Типовые решения.
		практическое занятие	Применение программно-аппаратного комплекса Dallas Lock для защиты информации от несанкционированного доступа. (часть 1)
		практическое занятие	Применение программно-аппаратного комплекса Dallas Lock для защиты информации от несанкционированного доступа. (часть 2)
		практическое занятие	Построение виртуальных защищенных сетей ViPNet (на платформе Windows).
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы	практическое занятие	Методы и средства защиты программ от компьютерных вирусов. Инициализация антивируса Касперского
		практическое занятие	Общая характеристика электронных идентификаторов (eToken, JKarta)

	действия и технологические особенности, взаимодействие с АС.	практическое занятие	Использование инструментальных средств анализа защищённости (часть 1).
		практическое занятие	Использование инструментальных средств анализа защищённости (часть 2).
		практическое занятие	Контроль доступа в ОС Linux.

\*\* семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

### Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

#### 4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	- подготовка доклада - подготовка электронной презентации - тестирование

\*\*\* самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

## 5. Материально-техническое и учебно-методическое обеспечение дисциплины

### 5.1 Литература:

#### Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забаурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/491249>

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2020. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497002>

#### Дополнительная литература



1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/495524>

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496492>

### **Литература для самостоятельного изучения**

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем (2-е издание). – М.: МГТУ им. Н.Э. Баумана. 2018. – 252с

### **5.2. Перечень лицензионного программного обеспечения**

1. Microsoft Windows 10 Education / Astra Linux Common Edition  
2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / LibreOffice (Base, Calc, Draw, Impress, Math, Writer)

### **5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся**

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - <http://www.gov.ru/>)

2. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - <https://www.minfin.ru/ru/>)

3. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - <http://www.gks.ru/>)

### **5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся**

1. справочно-правовая система «Консультант Плюс»  
2. справочно-правовая система «ГАРАНТ-Максимум»

### **5.5. Специальные помещения**

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет», ЭИОС СГЭУ и ПО Dallas Lock 8.0К

Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет», ЭИОС СГЭУ и ПО Dallas Lock 8.0К
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет», ЭИОС СГЭУ и ПО Dallas Lock 8.0К
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет», ЭИОС СГЭУ и ПО Dallas Lock 8.0К
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

## 5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет», ЭИОС СГЭУ и ПО Dallas Lock 8.0К Лабораторное оборудование
---	--

## 6. Фонд оценочных средств по дисциплине Программно-аппаратная защита информации:

### 6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Оценка докладов	-
	Устный/письменный опрос	-
	Тестирование	+
	Практические задачи	-
	Оценка контрольных работ (для заочной формы обучения)	+
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной

образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

**6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе**

**Профессиональные компетенции (ПК):**

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-1.1: Знать:  особенности инцидентов в процессе эксплуатации автоматизированной системы	ПК-1.2: Уметь:  обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	ПК-1.3: Владеть (иметь навыки):  навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Пороговый	политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	осуществлять меры противодействия нарушениям безопасности АС с использованием различных программных и аппаратных средств защиты	навыками анализа, обработки и интерпретации результатов инцидентов в АС
Стандартный (в дополнение к пороговому)	основы администрирования программно-аппаратных средства защиты информации в АС	применять меры противодействия нарушениям информационной безопасности АС с использованием различных программных и аппаратных средств защиты	организовывать работу по программно-аппаратной защите информации в АС
Повышенный (в дополнение к пороговому, стандартному)	основные средства защиты информации в компьютерных системах и сетях и принципы их работы;	производить выбор средств обеспечения информационной безопасности для использования их АС с целью обеспечения требуемого уровня защищенности	устанавливать, настраивать и обслуживать программно-аппаратные средства защиты информации

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью

типовых программных средств

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств
Пороговый	основные стандарты и спецификации в области обеспечения информационной безопасности	использование безопасных информационных технологий в работе	навыками подготовки исходных данных для проектирования подсистем, средств обеспечения защиты информации и
Стандартный (в дополнение к пороговому)	возможности использования новых информационных технологий и их средств при практической реализации	анализировать исходные данные с целью их применения при проектировании подсистем, средств обеспечения защиты информации	навыками оценки защищенности для администрирования программно-аппаратных средств защиты информации в АС
Повышенный (в дополнение к пороговому, стандартному)	основные стандарты и спецификации при практической реализации требований отечественных и международных стандартов информационной безопасности	проводить подготовку исходных данных для технико-экономического обоснования проектных решений	Навыками аргументированного выбора механизмов защиты информации, используемых при построении системы защиты информации в АС

ПК-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь навыки):
	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в

	автоматизированной системе	системе	автоматизированной системе
Пороговый	содержание исходных данных, необходимых для проектирования подсистем, средств обеспечения защиты информации в АС	использовать методы обеспечения информационной безопасности АС в работе современной АС	формальной постановки и решения задач по программно-аппаратной защиты информации
Стандартный (в дополнение к пороговому)	содержание мер по обеспечению информационной безопасности и состав программных и программно-аппаратных средств защиты информации	содержание исходных данных, необходимых для проектирования подсистем, средств обеспечения защиты информации в АС	оформления рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности
Повышенный (в дополнение к пороговому, стандартному)	возможности использования новых информационных технологий и их средств при практической реализации требований отечественных и международных стандартов информационной безопасности	определять основные принципы функционирования и обеспечения защиты программно-аппаратных современных средств информационной безопасности в АС	организации проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации в АС

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	<b>Планируемые результаты обучения по дисциплине</b>		
	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Пороговый	критерии оценки защищенности АС	производить выбор средств обеспечения информационной безопасности для использования их в АС	навыками работы со средствами защиты информации (на основе учебных имитационных программ)
Стандартный	проблемы и	контролировать	основами

(в дополнение к пороговому)	направлениях развития аппаратных и программных средств защиты информации	эффективность мер программно-аппаратной защиты информации	администрирования программно-аппаратных средства защиты информации
Повышенный (в дополнение к пороговому, стандартному)	принципы обеспечения информационной безопасности в условиях современного информационного общества	применять в различных проектах программно-аппаратные средства обеспечения информационной безопасности.	навыками администрирования средств защиты информации и управления процессом реализации комплекса мер по обеспечению информационной безопасности на объекте защиты

### 6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка контрольных работ (для заочной формы обучения) Тестирование	Зачет
2.	Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3	Оценка контрольных работ (для заочной формы обучения) Тестирование	Зачет

### 6.4. Оценочные материалы для текущего контроля

#### Примерная тематика докладов

Раздел дисциплины	Темы

#### Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы

**Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)**

укажите задания

Задание №1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

- а) политическая разведка;
- б) промышленный шпионаж;
- в) добросовестная конкуренция; г) конфиденциальная информация;
- д) правильного ответа нет.

Задание №2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности:

- а) любая информация;
- б) только открытая информация;
- в) запатентованная информация;
- г) закрываемая собственником информация;
- д) коммерческая тайна.
- е) Метод записи чисел, представление чисел с помощью письменных знаков;
- ж) Система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов с целью их улучшения и оптимизации.

Задание №3. Кто может быть владельцем защищаемой информации

- а) только государство и его структуры;
- б) предприятия акционерные общества, фирмы;
- в) общественные организации;
- г) только вышеперечисленные;
- д) кто угодно.

Задание №4 Какие сведения на территории РФ могут составлять коммерческую тайну

- а) учредительные документы и устав предприятия;
- б) сведения о численности работающих, их заработной плате и условиях труда;
- в) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
- г) другие;
- д) любые.

Задание №5. Какие секретные сведения входят в понятие «коммерческая тайна»?

- а) связанные с производством;
- б) связанные с планированием производства и сбытом продукции;
- в) технические и технологические решения предприятия;
- г) только первый и второй вариант ответа; 5) три первых варианта ответа.

**Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)**

Раздел дисциплины	Задачи

**Тематика контрольных работ**

Раздел дисциплины	Темы
-------------------	------

Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	Идентификация и аутентификация Протоколы идентификации. Система разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа) Модели разграничения доступа; надежность систем разграничения доступа Методы и средства защиты программ от компьютерных вирусов. Требования к антивирусной защите ФСТЭК России.
Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	Общая характеристика программно-аппаратных средств защиты информации Классификация средств защиты. Государственный реестр сертифицированных средств защиты информации. Краткая характеристика средств защиты Secret Net, Пак Криптон, Secret Disk Общая характеристика электронных идентификаторов Особенности реализации идентификаторов eToken, JKarta Защита программ от программных закладок. Подходы к защите программ от несанкционированного копирования

### 6.5. Оценочные материалы для промежуточной аттестации

#### Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности АС.	Исторический подход к защите информации в КС. Информация – предмет защиты. Информация – объект защиты. Случайные угрозы информации в КС. Преднамеренные угрозы информации в КС. Защита информации в КС от случайных угроз. Способы повышения надежности и отказоустойчивости КС. Защита информации в КС от преднамеренных угроз. Основные способы НСД. Физическая защита ПЭВМ от НСД.
Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с АС.	Организация аудита ресурсов и событий системы защиты ОС. Специфические угрозы безопасности информации в базах данных. Средства защиты баз данных. Управление распределенными данными. Угрозы безопасности информации в компьютерных сетях. Задачи и направления обеспечения информационной безопасности в сетях передачи данных. Службы и механизмы информационной безопасности в сетях передачи данных. Защита информации при межсетевом взаимодействии. Сегментация сложных локальных сетей. Обеспечение безопасного обмена конфиденциальной информацией. Классификация и применение межсетевых экранов. Межсетевой экран – пакетный фильтр.



	Межсетевой экран – посредник прикладного уровня. Системы контроля содержания. Сканеры безопасности. Обеспечение защиты информации средствами VPN. Системы обнаружения атак.
--	---

**6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации**

**Шкала и критерии оценивания**

<b>Оценка</b>	<b>Критерии оценивания для мероприятий контроля с применением 2-х балльной системы</b>
<b>«зачтено»</b>	ПК-1, ПК-2, ПК-3, ПК-4
<b>«не зачтено»</b>	Результаты обучения не сформированы на пороговом уровне