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 № 9 от 31 мая 2022 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 2022

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	**Планируемые результаты обучения по дисциплине**		
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 программе	**Планируемые результаты обучения по дисциплине**		
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	**Планируемые результаты обучения по дисциплине**		
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	**Планируемые результаты обучения по дисциплине**		
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

Виды учебной работы	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 Зачетные единицы	108 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 Зачетные единицы	108 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: Практич. занятия	ИКР	ГКР		
1.	Основы информационной безопасности. Характеристика угроз.	9	9	0.1		33.85	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
2.	Организационные и технические меры защиты информации.	9	9	0.05		20	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					
	Итого	**18**	**18**	**0.15**		**53.85**	

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: Практич. занятия	ИКР	ГКР		
1.	Основы информационной безопасности. Характеристика угроз.	1	1	0.1		45.85	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
2.	Организационные и технические меры защиты информации.	1	1	0.05		40	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					
	Итого	**2**	**2**	0.15		**85.85**	

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.	Основы информационной безопасности. Характеристика угроз.	лекция	Задачи политики информационной безопасности РФ
		лекция	Угрозы объектам КИИ
		лекция	Аттестация объектов информатизации
		лекция	Группы и классы по ЗИ
2.	Организационные и технические меры защиты информации.	лекция	Организация RAID массива в ИС
		лекция	Средства идентификации пользователей при доступе в КЗ
		лекция	Защита помещения, сервера, рабочей станции
		лекция	Электронная подпись
		лекция	Основы криптографии

*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.	Основы информационной безопасности. Характеристика угроз.	практическое занятие	Правоприменительная практика по ЗИ
		практическое занятие	Описать угрозы безопасности учебных заведений
		практическое занятие	Описать угрозы безопасности промышленных предприятий
		практическое занятие	Описать угрозы безопасности ПДн
2.	Организационные и технические меры защиты информации.	практическое занятие	Подготовить ИСПДн к аттестации. ч.1
		практическое занятие	Подготовить ИСПДн к аттестации. ч.2
		практическое занятие	Базовые средства защиты корпоративной почты
		практическое занятие	Использование ПО PGP для передачи эл. почты
		практическое занятие	Симметричный и асимметричный алгоритмы шифрования

** 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.	Основы информационной безопасности. Характеристика угроз.	- тестирование
2.	Организационные и технические меры защиты информации.	- 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. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

Литература для самостоятельного изучения

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)

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» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
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 Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ 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, утвержденными Ученым советом ФГАОУ ВО СГЭУ, протокол № 9 от 31.05.2022; 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	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
Пороговый	особенности инцидентов в процессе эксплуатации средств защиты от НСД	обнаруживать и идентифицировать инциденты в процессе эксплуатации средств защиты от НСД	навыками обнаружения и идентификации инцидентов в процессе эксплуатации средств защиты от НСД
Стандартный (в дополнение к пороговому)	особенности инцидентов в процессе эксплуатации СЗИ	обнаруживать и идентифицировать инциденты в процессе эксплуатации СЗИ	навыками обнаружения и идентификации инцидентов в процессе эксплуатации СЗИ
Повышенный (в дополнение к пороговому, стандартному)	особенности инцидентов в процессе эксплуатации СЗИ и СКЗИ	обнаруживать и идентифицировать инциденты в процессе эксплуатации СЗИ и СКЗИ	навыками обнаружения и идентификации инцидентов в процессе эксплуатации СЗИ и СКЗИ

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	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	особенности защиты автоматизированных систем с помощью ПО SecretNetStudio	оценивать защищенность автоматизированных систем с помощью ПО SecretNetStudio	навыками защищенности автоматизированных систем с помощью ПО SecretNetStudio
Стандартный (в дополнение к пороговому)	особенности защиты автоматизированных систем с помощью ПО SecretNetStudio и PryptoPro	оценивать защищенность автоматизированных систем с помощью ПО SecretNetStudio и PryptoPro	навыками защищенности автоматизированных систем с помощью ПО SecretNetStudio и PryptoPro
Повышенный (в дополнение к пороговому, стандартному)	особенности защиты автоматизированных систем с помощью ПО SecretNetStudio, PryptoPro и TLS -клиент	оценивать защищенность автоматизированных систем с помощью ПО SecretNetStudio, PryptoPro и TLS -клиент	навыками защищенности автоматизированных систем с помощью ПО SecretNetStudio, PryptoPro и TLS -клиент

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	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
Пороговый	особенности составления комплекса правил, процедур	составлять комплекс правил, процедур	навыками составления комплекса правил, процедур
Стандартный (в дополнение к пороговому)	особенности составления комплекса правил, процедур, практических приемов, принципов и методов	особенности составления комплекса правил, процедур, практических приемов, принципов и методов	навыками составления комплекса правил, процедур, практических приемов, принципов и методов
Повышенный (в дополнение к пороговому, стандартному)	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств

	обеспечения защиты информации	защиты информации	обеспечения защиты информации

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

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
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
Пороговый	основные угрозы безопасности информации для АП	анализировать изменения угроз безопасности информации для АП	навыками анализа изменения угроз безопасности информации для АП
Стандартный (в дополнение к пороговому)	основные угрозы безопасности информации для компьютерной сети	анализировать изменения угроз безопасности информации для компьютерной сети	навыками анализа изменения угроз безопасности информации для компьютерной сети
Повышенный (в дополнение к пороговому, стандартному)	основные угрозы безопасности информации для информационной системы	анализировать изменения угроз безопасности информации для информационной системы	навыками анализа изменения угроз безопасности информации для информационной системы

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.	Основы информационной безопасности. Характеристика угроз.	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.	Организационные и технические меры защиты информации.	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

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами) https://lms2.sseu.ru/course/index.php?categoryid=1918
укажите задания

Наибольшую угрозу информационным системам представляют:

1 пользователи
2 хакеры
3 спецслужбы
4 операторы связи.

Техническое подтверждение того, что меры безопасности и контроля для ИС соответствуют требованиям это:

1 аттестация
2 сертификация
3 пролонгация
4 ассенуация.

Вид деятельности требующая лицензирование:

1 передача секретных данных
2 продажа секретных данных
3 техническое обслуживание техники с секретными данными.
4 продажа шифровальных устройств.

Выдает сертификаты, лицензии на СЗИ:

1 ФСБ
2 ФСТЭК
3 ФТЭК
4 ФТС

Контролируемая зона это:

1 территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа
2 территория объекта, на которой установлена аппаратура видеонаблюдения для исключения неконтролируемого пребывания лиц не имеющих доступа нужного уровня секретности
3 территория объекта, на которой установлена охранная сигнализация с огороженным периметром для исключения неконтролируемого пребывания лиц, не имеющих допуска.

Криптографические алгоритмы используются для:

1 хранения и передачи информации по защищенным линиям связи
2 хранения и передачи информации по открытым каналам связи
3 ни то ни другое
4 и то и другое

Симпатические чернила используют:

1 особенности каллиграфии
2 особенности физического носителя
3 особенности интеллектуальных навыков человека
4 особенности физических навыков человека.

При обработке ПДн применяется защита от:

1 НДР
2 КПР
3 НСД
4 СНД

Федеральная система «Госуслуги» предоставляет доступ на основе:

1. Простой ЭП
2. Не квалифицированной ЭП
3. Квалифицированной ЭП

В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:

1. электрические
2. электромагнитные
3. параметрические
4. внешние
5. дистанционные

По источникам появления угрозы подразделяют на:

1. внешние и внутренние
2. естественные и искусственные
3. пользовательские и сетевые

По отношению к защищаемой информации существуют следующие угрозы

1. несанкционированный доступ
2. утечка
3. сокрытие
4. разглашение

Защита информации - это …

1. совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой
2. состояние информации, при котором изменять её могут только уполномоченные лица
3. комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации
4. данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность

Для любой информационной системы характерны следующие понятия

1. непредвиденное обстоятельство
2. происшествие
3. злоумышленник
4. уязвимость
5. угроза

Тематика контрольных работ

Раздел дисциплины	Темы
Основы информационной безопасности. Характеристика угроз.	1.Технические, организационные и правовые методы обеспечения компьютерной безопасности. 2.Общие проблемы безопасности. Роль и место информационной безопасности. 3.Защита информации в автоматизированных системах обработки данных. 4. Криптографические методы защиты информации. 5. Защита информации в персональных компьютерах. 6. Компьютерные вирусы и антивирусные программы. 7. Защита информации в сетях ЭВМ. 8. Комплексное обеспечение безопасности. 9. Информационная безопасность и защита информации. 10. Противодействия угрозам информационной безопасности.

	11.Проблемы безопасности локальных вычислительных сетей и интегрированных информационных систем управления предприятием.
Организационные и технические меры защиты информации.	12.Уязвимость информационных систем. 13. Криптосистемы с открытым ключом. 14.Современные шифры с секретным ключом. 15. Исторический аспект развития криптографии. 16. Стандарты информационной безопасности. 17.Криптографическая защита информации. 18. Автоматизированные системы как объекты обработки и защиты информации. 19.Современные методы защиты информации. 20. Методы оценки уровня безопасности информации в автоматизированных системах. 21. Основные нормативные акты Российской Федерации по информационной безопасности

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Основы информационной безопасности. Характеристика угроз.	Государственное регулирование в области ЗИ Правовые аспекты ИБ и ЗИ Цели защиты информации Какие государственные органы РФ уполномочены на ведение лицензионной деятельности в области защиты информации Приведите классификацию информации по режиму доступа Что такое сертификат на средство защиты информации, и для чего он нужен Понятие целостности данных Понятие конфиденциальности данных Назовите группы людей, от которых могут исходить угрозы информационным ресурсам организации Что является основными целями защиты информации в информационных системах Дайте характеристику основным направлениям информационно-аналитической работы Назовите, какие существуют виды охраны объектов Характеристики программных вирусов Системные ценности. Угрозы. Носитель угрозы. Годовые потери Основные цели ЗИ в информационных системах На основе каких данных выполняется поиск каналов НСД к ценной информации Физическая природа ПЭМИН Определение КЗ, виды КЗ, зоны R1 и R2
Организационные и технические меры защиты информации.	На что направлена деятельность по ЗИ Приведите определение закладочного устройства Какие задачи обеспечения ИБ решаются на организационном уровне Перечислите виды объектов защиты Назовите возможные каналы утечки информации Назовите демаскирующие признаки сетевых акустических закладок. Дайте характеристику основным элементам системы ЗИ Назовите известные в природе средства переноса информации Укажите на основные особенности канала для сигналов ИК-диапазона Назовите аппаратуру контроля линий связи Чем принципиально отличаются методы пассивной и активной

	защиты речевой информации Для чего предназначены средства пространственного зашумления Охарактеризуйте криптографические средства ЗИ Защита КЗ Средства защиты от НСД

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

Шкала и критерии оценивания

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