Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Кандрашина Елена Александровна
Должность: И.о. ректора ФГАОУ ВО «Самарский государственный экономический университет»
Дата подписания: 11.07.2025 11:49:18
Уникальный программный ключ:
2db64eb9605ce27edd3b8e8fdd32c70e0674ddd2

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 № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины	Б1.В.04 Теория информационной безопасности и методология защиты информации
Основная профессиональная образовательная программа	09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2025

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 Теория информационной безопасности и методология защиты информации входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Основы проектной деятельности, Информационно-коммуникационные технологии в профессиональной деятельности, Технологии работы в социальных сетях, Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования

Последующие дисциплины по связям компетенций: Проектный практикум, Организационная защита информации, Техническая защита информации, Программно-аппаратная защита информации, Управление информационной безопасностью, Цифровая культура в профессиональной деятельности, Управление информационными проектами реализации комплексной безопасности, Безопасность Web-приложений, Безопасность мобильных приложений, Интеллектуальные информационные системы, Современные цифровые технологии управления предприятием, Проектирование и реализация баз данных, Разработка профессиональных приложений, Проектирование информационных систем, Моделирование процессов и систем, Компьютерная экспертиза, Специализированные ИТ в правоохранительной деятельности, Криптографическая защита информации

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

Изучение дисциплины Теория информационной безопасности и методология защиты информации в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

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

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

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 5
Контактная работа, в том числе:	56.3/1.56
Занятия лекционного типа	18/0.5
Лабораторные работы (лабораторный практикум)	36/1
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	17.7/0.49
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	 Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	108 3

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 5

Контактная работа, в том числе:	6.3/0.18
Занятия лекционного типа	2/0.06
Лабораторные работы (лабораторный практикум)	2/0.06
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	67.7/1.88
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	Экз
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 Теория информационной безопасности и методология защиты 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 Лаборат. работы	ИКР	ГКР		
1.	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	9	18	0,15	1	10	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2.	Способы защиты автоматизированных систем от угроз информационной безопасности	9	18	0,15	1	7,7	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
		34					
	Итого	**18**	**36**	**0.3**	**2**	**17.7**	

очно-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 Лаборат. работы	ИКР	ГКР		
1.	Стандарты и нормативные документы,	1	1	0,015	1	37,7	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-

	регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем						4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
2.	Способы защиты автоматизированных систем от угроз информационной безопасности	1	1	0,15	1	30	ПК-3.1, ПК-3.2, ПК -3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
	Контроль	34					
	Итого	**2**	**2**	0.3	2	**67.7**	

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.	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	лекция	Понятие информации и информационной безопасности. ГОСТы на АС. Типовые виды структуры АС. Угрозы безопасности АС и их классификация
		лекция	Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации
		лекция	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.
		лекция	Классы каналов несанкционированного получения информации непосредственно с объекта; с каналов отображения информации; получение по внешним каналам; подключение к каналам получения информации
2.	Способы защиты автоматизированных систем от угроз информационной безопасности	лекция	Пассивная и активная защита от утечки информации по техническим каналам. Определение, классификация и общая характеристика технических каналов утечки информации.(ТКУИ). Понятие контролируемой зоны и методы определения ее размеров.
		лекция	Визуальные и акустические каналы. Защита информации в телефонных каналах. Защита от побочных электромагнитных излучений и наводок (ПЭМИН).

		лекция	Технические закладки. Способы обнаружения ТКУИ. Способы и методы перекрытия ТКУИ. Требования к выбору и оборудованию помещений для АС обработки данных по условиям защиты от ТКУИ
		лекция	Программно-аппаратные средства обеспечения защиты информации от несанкционированного доступа (НСД)
		лекция	Классификация технических разведок по типу носителей аппаратуры

*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.	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	лабораторные работы	Установка виртуальной машины Oracle VM
		лабораторные работы	Захват пакетов и создание IP фильтра
		лабораторные работы	Исследование фрагментированных пакетов
		лабораторные работы	Анализ IP заголовков и трафика
		лабораторные работы	Исследование маршрутов прохождения пакетов в эмуляторе
		лабораторные работы	Исследование резервного маршрута прохождения пакетов в эмуляторе АС
		лабораторные работы	Исследование реализации угроз в беспроводных WiFi сетях
		лабораторные работы	Средства технических разведок (СТР)
		лабораторные работы	Стационарная и носимая аппаратура СТР.
2.	Способы защиты автоматизированных систем от угроз информационной безопасности	лабораторные работы	Акустический канал утечки информации. Схема.
		лабораторные работы	Вибрационный канал утечки информации. Схема.
		лабораторные работы	Проводной канал утечки информации. Схема.
		лабораторные работы	Электромагнитный канал утечки информации. Схема.
		лабораторные работы	Визуальный канал утечки информации. Схема.
		лабораторные работы	Электросетевой канал утечки информации. Схема.
		лабораторные работы	Средства съема информации.
		лабораторные работы	Аппаратура защиты информации в сетях связи
		лабораторные работы	Схема организации закрытого канала связи.

** 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.	Вредоносные закладки (ВЗ): определение, разновидности. Разрушающие действия закладок Особенности взаимодействия с программно-аппаратными средствами защиты. Методика применения средств борьбы с вредоносными закладками на этапе эксплуатации систем	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Технологии межсетевых экранов. Функции МЭ. Формирование политики межсетевого взаимодействия. Основные схемы подключения МЭ. Персональные и распределенные сетевые экраны. Проблемы безопасности МЭ. Критерии оценки межсетевых экранов.	- 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.Каракеян, В. И. Безопасность жизнедеятельности : учебник и практикум для вузов / В. И. Каракеян, И. М. Никулина. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 313 с. — (Высшее образование). — ISBN 978-5-534-05849-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510519

Дополнительная литература

1.Резчиков, Е. А. Безопасность жизнедеятельности : учебник для вузов / Е. А. Резчиков, А. В. Рязанцева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 639 с. — (Высшее образование). — ISBN 978-5-534-12794-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511426

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. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10;

ОС "Альт Образование" 10

2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

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 Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ

	Лабораторное оборудование

6. Фонд оценочных средств по дисциплине Теория информационной безопасности и методология защиты информации:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Оценка докладов	+
	Устный/письменный опрос	+
	Тестирование	+
	Практические задачи	+
	Экзамен	+
Текущий контроль	Оценка докладов	+

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-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 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	Отрывочные знания о особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной	Не в полном объеме составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Не закрепленными навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной

	системе		системе
Стандартный (в дополнение к пороговому)	Твердые знания о особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Полностью составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Устойчивыми навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
Повышенный (в дополнение к пороговому, стандартному)	Глубокие знания о особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	Оптимально составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	На творческом 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-4.1: 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	Отрывочные сведения об основных угрозах безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Поверхностно анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Не закрепленными навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Стандартный (в дополнение к пороговому)	Уверенные знания об основных угрозах безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Уверенно анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	Устойчивыми навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Повышенный (в дополнение к пороговому, стандартному)	Глубокие знания об основных угрозах безопасности информации и автоматизированной системы, возникающих в ходе ее эксплуатации	Оптимально анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	На творческом уровне навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

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:	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	Общие понятия о возможных инцидентов в процессе эксплуатации автоматизированной системы	Обнаруживать явные инциденты в процессе эксплуатации автоматизированной системы	Начальными навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Стандартный (в дополнение к пороговому)	О возможных инцидентах в процессе эксплуатации автоматизированной системы	Обнаруживать известные инциденты в процессе эксплуатации автоматизированной системы	Навыками обнаружения и идентификации известных инцидентов в процессе эксплуатации автоматизированной системы
Повышенный (в дополнение к пороговому, стандартному)	Об особенностях возможных инцидентов в процессе эксплуатации автоматизированной системы	Обнаруживать все инциденты в процессе эксплуатации автоматизированной системы	Навыками обнаружения и идентификации всех 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-2.1: 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	Начальные знания об особенностях защиты автоматизированных систем с помощью типовых программных средств	Поверхностно оценивать защищенность автоматизированных систем с помощью типовых программных средств	Поверхностными навыками защищенности автоматизированных систем с помощью типовых программных средств

Стандартный (в дополнение к пороговому)	Базовые знания об особенностях защиты автоматизированных систем с помощью типовых программных средств	Глубоко оценивать защищенность автоматизированных систем с помощью типовых программных средств	Устойчивыми навыками защищенности автоматизированных систем с помощью типовых программных средств
Повышенный (в дополнение к пороговому, стандартному)	Глубокие знания об особенностях защиты автоматизированных систем с помощью типовых программных средств	Экспертно оценивать защищенность автоматизированных систем с помощью типовых программных средств	Профессиональными навыками защищенности автоматизированных систем с помощью типовых программных средств

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.	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3	Оценка контрольных работ (для очно - заочной формы обучения) Тестирование	Экзамен
2.	Способы защиты автоматизированных систем от угроз информационной безопасности	ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3	Оценка контрольных работ (для очно - заочной формы обучения) Тестирование	Экзамен

6.4.Оценочные материалы для текущего контроля

Примерная тематика докладов

Раздел дисциплины	Темы
Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	Атаки на уровне систем управления базами данных Атаки на уровне операционной системы Атаки на уровне сетевого программного обеспечения
Способы защиты автоматизированных систем от угроз информационной безопасности	Особенности специальных исследований ПЭМИ Особенности специальных исследований ПЭМИН

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

укажите задания

Сущность и понятие информационной безопасности:

1. состояние защищённости жизненно важных интересов государства в информационной сфере
2. состояние защищённости жизненно важных интересов личности, общества и государства в информационной сфере
3. состояние защищённости жизненно важных ресурсов

Место информационной безопасности в системе национальной безопасности страны:

Виды, источники и носители защищаемой информации:

Источники угроз безопасности информации:

1. обусловленные действиями субъекта, техническими средствами, стихийными источниками
2. Обусловлены действиями антропогенного характера, техногенного, стихийного
3. обусловлены злонамеренными действиями сотрудников и внешних нарушителей

Роль факторов, воздействующие на информацию при ее обработке в автоматизированных системах:

1. составляют основу для планирования и закупку средств защиты, направленных на защиту информации на объекте информатизации
2. составляют основу для проведения работ, направленных на защиту информации на объекте информатизации
3. составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации

Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи:

1. реализация, функционирование, мониторинг соответствия
2. создание , реализация, функционирование, мониторинг соответствия
3. создание , реализация, функционирование, модернизация

Современные средства и способы обеспечения информационной безопасности:

1. идентификацию, регламентирование доступа к объектам, дешифрующую систему файлов, ключи, безопасные соединения
2. аутентификацию, регламентирование доступа к объектам, шифрующую систему файлов, ключи, безопасные соединения
3. аутентификацию, регламентирование доступа к объектам, дешифрующую систему файлов, ключи, безопасные соединения

Основные методики анализа угроз и рисков информационной безопасности основаны на:

1. потенциальном ущербе для организации, вероятностью реализации, стоимости мер защиты
2. потенциальном ущербе для организации и стоимости мер защиты
3. потенциальном ущербе для организации и вероятностью их реализации

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. ФНС
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.

Основными субъектами информационной безопасности являются:

1. руководители, менеджеры, администраторы компаний
2. органы права, государства, бизнеса
3. сетевые базы данных, фаерволлы

К основным функциям системы безопасности можно отнести все перечисленное:

1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостинг-компании
3. Внедрение аутентификации, проверки контактных данных пользователей тест

Принципом информационной безопасности является принцип недопущения:

1. Неоправданных ограничений при работе в сети (системе)
2. Рисков безопасности сети, системы
3. Презумпции секретности

Принципом политики информационной безопасности является принцип:

1. Невозможности миновать защитные средства сети (системы)
2. Усиления основного звена сети, системы
3. Полного блокирования доступа при риск-ситуациях

Принципом политики информационной безопасности является принцип:

1. Усиления защищенности самого незащищенного звена сети (системы)
2. Перехода в безопасное состояние работы сети, системы
3. Полного доступа пользователей ко всем ресурсам сети, системы

Принцип Кирхгофа:

1. Секретность ключа определена секретностью открытого сообщения
2. Секретность информации определена скоростью передачи данных
3. Секретность закрытого сообщения определяется секретностью ключа

ЭЦП – это:

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

Наиболее распространены угрозы информационной безопасности корпоративной системы:

1. Покупка нелицензионного ПО
2. Ошибки эксплуатации и неумышленного изменения режима работы системы
3. Сознательного внедрения сетевых вирусов

Наиболее распространены угрозы информационной безопасности сети:

1. Распределенный доступ клиент, отказ оборудования

2. Моральный износ сети, инсайдерство
3. Сбой (отказ) оборудования, нелегальное копирование данных

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем	1. Понятия компьютерной системы. Понятие угроз информационной безопасности. Факторы, воздействующие на информации согласно ГОСТ 51275-2006. Их классификация. 2. Понятие защищенности (безопасности) информации. Конфиденциальность, целостность и доступность информации. 3. Человеческий фактор и модель нарушителя безопасности информации 4. Угрозы конфиденциальности информации 5. Угрозы доступности информации 6. Угрозы целостности информации 7. Естественные угрозы информации 8. Искусственные угрозы информации 9. Непреднамеренные угрозы информации 10.Преднамеренные угрозы информации 8 11.Случайные угрозы информации 12.Побочные электромагнитные излучения 13.Побочные электромагнитные излучения и наводки 14.Угрозы утечки информации по техническим каналам 15.Угрозы несанкционированного доступа к информационным ресурсам 16.Недекларированные возможности программного обеспечения 17.Угрозы 1-3 типа для информационных систем персональных данных 18.Воздействие вредоносных программ на информационные ресурсы 19.Причины реализации атак на информационные сети 20.Угрозы с использованием уязвимости в программном обеспечении информационных систем
Способы защиты автоматизированных систем от угроз информационной безопасности	21.Угрозы с использованием виртуализации информационных ресурсов КС 22.Угрозы, обусловленные пропускной способностью системного ресурса 23.Ущерб как категория классификации угроз 24.Жизненный цикл информационной угрозы 25.Модель угроз 26.Модель нарушителя 27.Идентификация информационных ресурсов и угроз 28.Оценка защищенности компьютерных систем 29.Аудит информационной безопасности 30.Тестирование на проникновение 31.Метод «черного ящика» – имитация нарушителя, не обладающего никакими сведениями об организации и доступом к ее корпоративной сети. 32.Метод «серого ящика» – имитация нарушителя, обладающего ограниченными знаниями об организации, ее корпоративной сети и системе защиты. 33.Метод «белого ящика» – имитация нарушителя, который является администратором, либо иным пользователем, хорошо осведомленным о корпоративной сети и системе защиты. 34.Анализ текущего состояния КС (на физическом/канальном/сетевом уровнях) с точки зрения ИБ и непрерывности деятельности; 35.Анализ активного оборудования КС (аппаратного и программного обеспечения); 36.Анализ конфигураций средств защиты информации и управления ИБ; 37.Анализ конфигурации отдельных сетевых сервисов, ОС,

	системного и прикладного ПО; 38.Анализ сведений о событиях и инцидентах, зафиксированных в инфраструктуре; 39.Аудит технических уязвимостей компонентов КС и СИБ, оценка их применимости и потенциальных рисков их эксплуатации; 40.Анализ сетевого трафика в периметре ЛВС, используемых протоколов, пользовательской активности. 41.Формирование рекомендаций по устранению выявленных уязвимостей, недостатков и несоответствий КС и СИБ, а также перечень мероприятий организационного и технического характера по повышению уровня ИБ.

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 4-х балльной системы**
«отлично»	Повышенный ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
«хорошо»	Стандартный ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
«удовлетворительно»	Пороговый ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3, ПК- 1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне