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.07 Методы и средства защиты 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.

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

1. Место дисциплины в структуре ОП

Дисциплина Методы и средства защиты информации входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Философия, История России, Математические методы в экономике, Основы алгоритмизации и программирования, Общая теория статистики, Основы финансовых расчетов, Эконометрика, Управление человеческими ресурсами, Основы менеджмента, Хранение, обработка и анализ данных, Технологии работы в социальных сетях, Информационно-коммуникационные технологии в профессиональной деятельности, Основы проектной деятельности

Последующие дисциплины по связям компетенций: Моделирование процессов и систем, 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

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

Изучение дисциплины Методы и средства защиты информации в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Универсальные компетенции (УК):

УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
УК-1	УК-1.1: Знать:	УК-1.2: Уметь:	УК-1.3: Владеть (иметь навыки):
	методы поиска, анализа и синтеза информации	осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	навыками поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач

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	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 в автоматизированной системе	защиты информации в автоматизированной системе	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 5
Контактная работа, в том числе:	74.3/2.06
Занятия лекционного типа	18/0.5
Занятия семинарского типа	54/1.5
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	35.7/0.99
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	 Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	6.3/0.18
Занятия лекционного типа	2/0.06
Занятия семинарского типа	2/0.06
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	103.7/2.88
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	 Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Методы и средства 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: Практич. занятия	ИКР	ГКР		
1.	Общие положения. Предмет и задачи теории защиты информации	8	18	0,1	1	15	УК-1.1, УК-1.2, УК -1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	10	36	0,2	1	20,7	УК-1.1, УК-1.2, УК -1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**18**	**54**	**0.3**	**2**	**35.7**	

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.	Общие положения. Предмет и задачи теории защиты информации	1		0,1	1	50	УК-1.1, УК-1.2, УК -1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	1	2	0,2	1	53,7	УК-1.1, УК-1.2, УК -1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**2**	**2**	0.3	2	**103.7**	

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.	Общие положения. Предмет и задачи теории защиты информации	лекция	Общие положения теории защиты информации.
		лекция	Предмет и задачи теории защиты информации. лекция Цель проектирова
		лекция	Цель проектирования СЗИ.
		лекция	Базовые термины и определения
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	лекция	Классификация угроз безопасности
		лекция	Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характиристики.
		лекция	Классификация угроз уязвимостей и уровней защищености
		лекция	Объекты защиты и моделирования.
		лекция	Основополагающие методы и абстрактые модели контроля доступа.

*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.	Общие положения. Предмет и задачи теории защиты информации	практическое занятие	Общие положения теории защиты информации.
		практическое занятие	Предмет и задачи теории защиты информации
		практическое занятие	Цель проектирования СЗИ.
		практическое занятие	Базовые термины и определения.
		практическое занятие	Система защиты информации
		практическое занятие	Источники угрозы безопасности информации
		практическое занятие	Уязвимость ИС
		практическое занятие	Эффективность ЗИ
		практическое занятие	Оценка риска ИБ оргагизации
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	практическое занятие	Классификация угроз безопасности
		практическое занятие	Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характиристики
		практическое занятие	Классификация угроз уязвимостей и уровней защищености
		практическое занятие	Объекты защиты и моделирования.
		практическое занятие	Основополагающие методы и абстрактые модели контроля доступа
		практическое занятие	Метод и абстрактная модель дискеционного контроля доступа
		практическое занятие	Альтернативный метод и абстрактная модель избирательного контроля доступа
		практическое занятие	Метод и абстрактная модель мандатного контроля доступа.
		практическое занятие	Методы и абстрактные модели контроля доступа к создаваемым объектам

** 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.	Общие положения. Предмет и задачи теории защиты информации	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	- 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. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138

Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520063

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. 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. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/
2. Электронная библиотечная система Юрайт Издательство Юрайт https://biblio-online.ru/

3. Платформа «Библиокомплектатор» http://www.bibliocomplectator.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	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интренет» и ЭИОС СГЭУ Лабораторное оборудование

6. Фонд оценочных средств по дисциплине Методы и средства защиты информации:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Тестирование	+
	Практические задачи	+
Промежуточный контроль	Экзамен	+

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

Универсальные компетенции (УК):

УК-1 - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	УК-1.1: Знать:	УК-1.2: Уметь:	УК-1.3: Владеть (иметь навыки):
	методы поиска, анализа и синтеза информации	осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	навыками поиска, критического анализа и синтеза информации, применения системного подхода для решения поставленных задач
Пороговый	теоретические основы поиска, критического анализа и синтеза информации.	формулирует цели поиска и анализа информации	навыки осуществления критического анализа информации на основе системного подхода;
Стандартный (в дополнение к пороговому)	современные источники информации.	выбирает источники информации	навыки нахождения источников информации
Повышенный (в дополнение к пороговому, стандартному)	сущность системного подхода для решения поставленных задач.	использует информационно - коммуникационные технологии для поиска информации	опыт применения научно-исследовательски х знаний в профессиональной деятельности

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,	составлять комплекс правил, процедур,	навыками составления комплекса правил,

	процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
Пороговый	особенности составления комплекса правил обеспечения защиты информации в автоматизированной системе	составлять комплекс правил обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил обеспечения защиты информации в автоматизированной системе
Стандартный (в дополнение к пороговому)	особенности составления комплекса правил, процедур, практических приемов, принципов и методов защиты информации в автоматизированной системе	составлять комплекс правила и процедуры практических приемов и методов защиты информации в автоматизированной системе	практическими приемами и методами обеспечения защиты информации
Повышенный (в дополнение к пороговому, стандартному)	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-4.1: 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	методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	навыками установки, настройки программных средств защиты информации в автоматизированной системе;
Стандартный (в дополнение к пороговому)	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;	тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программноаппаратных

			средств защиты информации
Повышенный (в дополнение к пороговому, стандартному)	типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	навыками решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

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.	Общие положения. Предмет и задачи теории защиты информации	УК-1.1, УК-1.2, УК- 1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК- 4.2, ПК-4.3	Тестирование Практические задачи	Экзамен
2.	Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	УК-1.1, УК-1.2, УК- 1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК- 4.2, ПК-4.3	Тестирование Практические задачи	Экзамен

6.4.Оценочные материалы для текущего контроля

Ссылка на текущую академическую активность, точки текущего контроля для всех оценочных материалов, размещенных в БРСО ЭИОС СГЭУ: https://lms2.sseu.ru/course/index.php?categoryid=1918

Примерная тематика докладов

Раздел дисциплины	Темы
Общие положения. Предмет и задачи теории защиты информации	1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности. 2. Понятие безопасности и её составляющие. Безопасность информации. 3. Обеспечение информационной безопасности: содержание и структура понятия. 4. Национальные интересы в информационной сфере. 5. Источники и содержание угроз в информационной сфере. 6. Соотношение понятий «информационная безопасность» и «национальная безопасность» 7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. 8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание. 9. Система обеспечения информационной безопасности. 10.Обеспечение информационной безопасности Российской Федерации.

	11.Понятие информационной войны. Проблемы информационной войны. 12. Информационное оружие и его классификация. 13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне. 14. Уровни ведения информационной войны. Информационные операции. Психологические операции. 15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети
Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	16.Основные положения государственной информационной политики Российской Федерации. 17.Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности. 18.Виды защищаемой информации в сфере государственного и муниципального управления. 19.Обеспечение информационной безопасности организации. 20.Характеристика эффективных стандартов по безопасности. 21.Требования к полноте эффективных стандартов по безопасности. 22.Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере. 23. Информация - фактор существования и развития общества. 24.Обеспечение информационной безопасности: содержание и структура понятия. 25.Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации. 26.Обеспечение информационной безопасности Российской Федерации. 27.Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности 28.Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. 29. Административный уровень обеспечения информационной безопасности. 30.Организационные структуры системы обеспечения информационной безопасности предприятия (организации). 31.Корпоративная нормативная база по защите информации. 32.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 33.Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия). 34.Нормативно-методические документы по обеспечению безопасности информации.

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

Обеспечение информационной безопасности не зависит от:
руководства организаций;
системных и сетевых администраторов;
внутренних пользователей;
внешних пользователей.

При анализе стоимости защитных мер не следует учитывать:
расходы на закупку оборудования
расходы на закупку программ
расходы на обучение персонала

расходы на премии персонала

В число универсальных сервисов безопасности входят:
управление доступом
управление информационными системами и их компонентами
управление носителями

Не являются сервисами безопасности:
идентификация и аутентификация
шифрование
контроль целостности
регулирование конфликтов
экранирование
обеспечение безопасного восстановления

В число архитектурных принципов, направленных на обеспечение высокой доступности информационных сервисов, не входит:
управляемость процессов, контроль состояния частей
невозможность обхода защитных средств
автоматизация процессов

Цифровой сертификат содержит:
открытый ключ удостоверяющего центра
секретный ключ удостоверяющего центра
имя удостоверяющего центра "

В число направлений физической защиты не входят:
физическая защита пользователей
защита поддерживающей инфраструктуры
защита от перехвата данных

Криптография необходима для реализации следующих сервисов безопасности:
шифрование
туннелирование
разграничение доступа

В число целей политики безопасности верхнего уровня не входит:
решение сформировать или пересмотреть комплексную программу безопасности
обеспечение базы для соблюдения законов и правил
+обеспечение конфиденциальности почтовых сообщений

В число целей программы безопасности верхнего уровня входят:
управление рисками
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

В рамках программы безопасности нижнего уровня не осуществляется:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков

В число целей политики безопасности верхнего уровня входят:

формулировка административных решений по важнейшим аспектам реализации
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

В число целей программы безопасности верхнего уровня входят:
составление карты информационной системы
координация деятельности в области информационной безопасности
пополнение и распределение ресурсов

Контроль целостности может использоваться для:
предупреждения нарушений ИБ
обнаружения нарушений
локализации последствий нарушений

Нужно ли включать в число ресурсов по информационной безопасности серверы с информацией органов лицензирования и сертификации по данной тематике:
да, поскольку наличие лицензий и сертификатов при прочих равных условиях является важным достоинством
нет, поскольку реально используемые продукты все равно не могут быть сертифицированы
не имеет значения, поскольку если информация о лицензиях или сертификатах понадобится, ее легко найти

Программно-технические меры безопасности не включают:
превентивные, препятствующие нарушениям информационной безопасности
меры обнаружения нарушений
меры воспроизведения нарушений

В число направлений повседневной деятельности на процедурном уровне входят:
поддержка пользователей
поддержка программного обеспечения
поддержка унаследованного оборудования

Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
способна противостоять только информационным угрозам, как внешним, так и внутренним
способна противостоять только внешним информационным угрозам

Методы повышения достоверности входных данных
Отказ от использования данных
Проведение комплекса регламентных работ
Введение избыточности в документ первоисточник
Многократный ввод данных и сличение введенных значений

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

Раздел дисциплины	**Задачи**
Общие положения. Предмет и задачи теории защиты информации	1. Общие положения теории защиты информации. 2. Предмет и задачи теории защиты информации 3. Цель проектирования СЗИ. 4. Базовые термины и определения.

	5. Система защиты информации 6. Источники угрозы безопасности информации 7. Уязвимость ИС 8. Эффективность ЗИ 9. Оценка риска ИБ оргагизации
Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	1. Классификация угроз безопасности 2. Интерпретация угрозы атаки. Понятие надежности безопасности, параметры и характиристики 3. Классификация угроз уязвимостей и уровней защищености 4. Объекты защиты и моделирования. 5. Основополагающие методы и абстрактые модели контроля доступа 6. Метод и абстрактная модель дискеционного контроля доступа 7. Альтернативный метод и абстрактная модель избирательного контроля доступа 8. Метод и абстрактная модель мандатного контроля доступа. 9. Методы и абстрактные модели контроля доступа к создаваемым объектам

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Общие положения. Предмет и задачи теории защиты информации	1. Что такое информационная безопасность? 2. Какие предпосылки и цели обеспечения информационной безопасности? 3. В чем заключаются национальные интересы РФ в информационной сфере? 4. Что включает в себя информационная борьба? 5. Какие пути решения проблем информационной безопасности РФ 6. существуют? 7. Каковы общие принципы обеспечения защиты информации? 8. Какие имеются виды угроз информационной безопасности предприятия(организации)? 9. Какие источники наиболее распространенных угроз информационной 10. безопасности существуют? 11. Какие виды сетевых атак имеются? 12. .Какими способами снизить угрозу сниффинга пакетов? 13. Какие меры по устранению угрозы IP -спуфинга существуют? 14. Что включает борьба с атаками на уровне приложений? 15. В чем заключается распределенное хранение файлов? 16. Что включают в себя требования по обеспечению комплексной системы информационной безопасности? 17. Какие уровни информационной защиты существуют, их основные составляющие?
Классификация угроз безопасности и уровней защиты. Интерпретация угрозы атаки. Понятие надежной безопасности. Методы и абстрактные модели защиты информации.	18. Какая программа называется логической бомбой? 19. Какими способами можно проверить систему безопасности? 20. Что является основными характеристиками технических средств защиты информации? 21. Какие требования предъявляются к автоматизированным системам защиты третьей группы? 22. Какие требования предъявляются к автоматизированным системам защиты второй группы? 23. Какие требования предъявляются к автоматизированным системам защиты первой группы?

	24. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности? 25. Какие требования предъявляются к межсетевым экранам? 26. Какие имеются показатели защищенности межсетевых экранов? 27. Какие атаки системы снаружи вы знаете? 28. Какая программа называется вирусом? 29. Какая атака называется атакой отказа в обслуживании? 30. Какие виды вирусов вы знаете? 31. Какие вирусы называются паразитическими? 32. Как распространяются вирусы? 33. Какие методы обнаружения вирусов вы знаете? 34. Какая программа называется монитором обращения? 35. Что представляет собой домен? 36. Как осуществляется защита при помощи ACL -списков? 37. Какой список называется перечнем возможностей? 38. Какие способы защиты перечней возможностей вы знаете? 39. Из чего состоит высоконадежная вычислительная база (ТСВ)? 40. Какие модели многоуровневой защиты вы знаете? 41. .В чем заключается организация работ по защите от не санкционированного доступа интегрированной информационной системы управления предприятием?

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 УК-1.1, УК-1.2, УК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3
«хорошо»	Стандартный УК-1.1, УК-1.2, УК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3
«удовлетворительно»	Пороговый УК-1.1, УК-1.2, УК-1.3, ПК-3.1, ПК-3.2, ПК-3.3, ПК- 4.1, ПК-4.2, ПК-4.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне