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

Институт Институт экономики предприятий

Кафедра Информационной безопасности (ПГУТИ)

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 11 от 30 мая 2023 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.О.32 Информационная безопасность

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа Интеллектуальные цифровые системы и сервисы в управлении

Квалификация (степень) выпускника Бакалавр

Самара 2023

Содержание (рабочая программа)

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

1. Место дисциплины в структуре ОП

Дисциплина Информационная безопасность входит в обязательную часть блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Иностранный язык, Основы права, Проектирование баз данных, Современные цифровые платформы, Операционные системы и оболочки, Информационные технологии цифровой экономики

Последующие дисциплины по связям компетенций: Надежность интеллектуальных систем, Реинжиниринг и управление бизнес-процессами, Имитационное моделирование

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

Изучение дисциплины Информационная безопасность в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Универсальные компетенции (УК):

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
УК-2	УК-2.1: Знать:	УК-2.2: Уметь:	УК-2.3: Владеть (иметь навыки):
	основные принципы и концепции в области целеполагания, методы генерации альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения, основные нормативно-правовые документы, регламентирующие процесс принятия реше- ний в конкретной предметной области	системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения, использовать инструментальные средства для разработки и принятия решений, выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	навыками разработки проектов в избранной профессиональной сфере с учетом надежности предлагаемых решений, их безопасности и эффективности навыками работы с нормативно-правовой документацией

Общепрофессиональные компетенции (ОПК):

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОПК-3	ОПК-3.1: Знать:	ОПК-3.2: Уметь:	ОПК-3.3: Владеть (иметь навыки):
	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	навыками поиска и работы с информацией и подготовки материалов и документации по научно-исследовательской работе с учетом требований информационной безопасности

ОПК-2 - Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ОПК-2	ОПК-2.1: Знать:	ОПК-2.2: Уметь:	ОПК-2.3: Владеть (иметь навыки):
	современные информационные технологии и программные средства, в том числе отечественного производства, используемые при решении задач профессиональной деятельности	понимать принципы работы и выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	навыками использования современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПКМ-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

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

ОПКМ-6	ОПКМ-6.1: Знать:	ОПКМ-6.2: Уметь:	ОПКМ-6.3: Владеть (иметь навыки):
	принципы работы информационных технологий; основные методы и программные средства сбора, обработки и анализа информации	понимать принципы работы информационных технологий; использовать методы и программные средства сбора, обработки и анализа данных для обеспечения информационно-аналитической поддержки принятия управленческих решений	навыками использования современных информационных технологий и программных средств для выбора управленческих решений

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:	50.15/1.39
Занятия лекционного типа	22/0.61
Занятия семинарского типа	14/0.39
Лабораторные работы (лабораторный практикум)	14/0.39
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	39.85/1.11
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 Информационная безопасность представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа					Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа		ИКР	ГКР		
			Практич. занятия	Лаборат. работы				
1.	Основные понятия информационной безопасности.	2	-	-			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -

								2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
2.	Принципы криптографической защиты информации.	2	2	-			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
3.	Современные симметричные криптосистемы.	2	2	2			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
4.	Асимметричные криптосистемы.	2	2	2			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
5	Идентификация и проверка подлинности.	2	-	2			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
6.	Электронная цифровая подпись.	2	2	2			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
7.	Управление криптографическими ключами.	2	-	-			44	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
8.	Политика ИБ	2	2	-			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1,

								ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
9.	Оценка рисков ИБ	4	4	2			4	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
10.	Программные средства защиты информации	2	-	4			3,85	УК-2.1, УК-2.2, УК -2.3, ОПК-3.1, ОПК -3.2, ОПК-3.3, ОПК -2.1, ОПК-2.2, ОПК -2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ -6.3
	Контроль	18						
	Итого	**22**	**14**	**14**	**0.15**		**39.85**	

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.	Основные понятия информационной безопасности.	лекция	Классификация угроз безопасности корпоративных сетей. Обеспечение безопасности сетей передачи данных. Базовые технологии безопасности сетей.
2.	Принципы криптографической защиты информации.	лекция	Схема симметричной криптосистемы. Схема асимметричной криптосистемы. Аппаратно-программные средства защиты компьютерной информации.
3.	Современные симметричные криптосистемы.	лекция	Классическая сеть Фейстеля. Стандарт симметричного шифрования. Комбинирование блочных алгоритмов. Отечественный стандарт шифрования данных. Блочные и поточные шифры.

4.	Асимметричные криптосистемы.	лекция	Однонаправленные функции. Ассиметричная криптосистема шифрования данных. Комбинированный метод шифрования.
5.	Идентификация и проверка подлинности.	лекция	Идентификация и аутентификация. Взаимная проверка подлинности пользователей.
6.	Электронная цифровая подпись.	лекция	Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритмы электронной цифровой подписи. Цифровые подписи с дополнительными функциональными свойствами.
7.	Управление криптографическими ключами.	лекция	Генерация ключей. Распределение ключей. Хранение ключей. Концепция ключевой иерархии.
8.	Политика ИБ	лекция	Лица, ответственные за соблюдение политик или процедур. Порядок идентификации пользователей. Управление доступом. Процедура системного администрирования. Конфиденциальная информацию внутри организации и способы ее защиты. Технические требования к защите ИС.
9.	Оценка рисков ИБ	лекция	Управление рисками ИБ. Методики оценки рисков информационной безопасности.
		лекция	Расчет рисков ИБ.
10.	Программные средства защиты информации	лекция	Методы защиты информации от несанкционированного доступа. Анализ уязвимости программного обеспечения. Методы защиты от вредоносных программ. Средства идентификация и аутентификации пользователей.

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

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Основные понятия информационной безопасности.	-	-

2.	Принципы криптографической защиты информации.	Практическое занятие	Методы шифрования
3.	Современные симметричные криптосистемы.	Лабораторная работа	Изучение отечественного стандарта шифрования ГОСТ 28147-89
		Практическое занятие	Алгоритм DES
4.	Асимметричные криптосистемы.	Лабораторная работа	Изучение алгоритма шифрования с открытым ключом RSA
		Практическое занятие	Решение расширенного алгоритма Евклида
5.	Идентификация и проверка подлинности.	Лабораторная работа	Многоуровневая аутентификация
6.	Электронная цифровая подпись.	Лабораторная работа	Изучение алгоритма электронной цифровой подписи RSA
		Практическое занятие	Алгоритмы электронной цифровой подписи
7.	Управление криптографическими ключами.	-	-
8.	Политика ИБ	Практическое занятие	Разделы политики безопасности
9.	Оценка рисков ИБ	Лабораторная работа	Анализ и управление информационными рисками
		Практическое занятие	Оценка рисков предприятия
		Практическое занятие	Анализ рисков предприятия
10.	Программные средства защиты информации	Лабораторная работа	Сканер уязвимостей
		Лабораторная работа	Настройка усиленной аутентификации

** 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 ***
5.	Идентификация и проверка подлинности.	- подготовка доклада - подготовка электронной презентации
8.	Политика ИБ	- подготовка доклада - подготовка электронной презентации

*** 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. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519780

Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

Литература для самостоятельного изучения

1.

5.2. Перечень лицензионного программного обеспечения

1. РЭД ОС
2. LibreOffice

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

Аудитории для лабораторных занятий	Количество посадочных мест по количеству обучающихся. Компьютеры с выходов в сеть «Интернет»

6. Фонд оценочных средств по дисциплине Информационная безопасность:

6.1. Контрольные мероприятия по дисциплине

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

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

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

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

Универсальные компетенции (УК):

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	УК-2.1: Знать:	УК-2.2: Уметь:	УК-2.3: Владеть (иметь навыки):
	основные принципы и концепции в области целеполагания, методы генерации альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения, основные нормативно-правовые документы, регламентирующие процесс принятия реше- ний в конкретной предметной области	системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения, использовать инструментальные средства для разработки и принятия решений, выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	навыками разработки проектов в избранной профессиональной сфере с учетом надежности предлагаемых решений, их безопасности и эффективности навыками работы с нормативно-правовой документацией
Пороговый	частично основные принципы и концепции в области целеполагания, методы генерации альтернатив решений и приведения их к сопоставимому виду для выбора оптимального	успешно, но не систематически системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения, использовать инструментальные средства для разработки и принятия решений,	частично навыками разработки проектов в избранной профессиональной сфере с учетом надежности предлагаемых решений, их безопасности и эффективности навыками работы с нормативно-правовой документацией

	решения,		
Стандартный (в дополнение к пороговому)	хорошо, но может допускать несущественные ошибки в основных принципах и концепции в области целеполагания, методсх генерации альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения, основных нормативно-правовых документах, регламентирующих процесс принятия решений в конкретной предметной области	в целом успешно, иногда под руководством преподавателя анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения, использовать инструментальные средства для разработки и принятия решений, выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	хорошо навыками разработки проектов в избранной профессиональной сфере с учетом надежности предлагаемых решений, их безопасности и эффективности навыками работы с нормативно-правовой документацией
Повышенный (в дополнение к пороговому, стандартному)	хорошо и в полном объеме основные принципы и концепции в области целеполагания, методы генерации альтернатив решений и приведения их к сопоставимому виду для выбора оптимального решения, основные нормативно-правовые документы, регламентирующие процесс принятия реше- ний в конкретной предметной области	самостоятельно и наилучшим образом системно анализировать поставленные цели, формулировать задачи и предлагать обоснованные решения, использовать инструментальные средства для разработки и принятия решений, выбирать оптимальные решения исходя из действующих правовых норм, имеющихся ресурсов и ограничений	свободно навыками разработки проектов в избранной профессиональной сфере с учетом надежности предлагаемых решений, их безопасности и эффективности навыками работы с нормативно-правовой документацией

Общепрофессиональные компетенции (ОПК):

ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

коммуникационных технологий и с учетом основных требований информационной безопасности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ОПК-3.1: Знать:	ОПК-3.2: Уметь:	ОПК-3.3: Владеть (иметь навыки):
	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	навыками поиска и работы с информацией и подготовки материалов и документации по научно-исследовательской работе с учетом требований информационной безопасности
Пороговый	Частично принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	успешно, но не систематически решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Частично навыками поиска и работы с информацией и подготовки материалов и документации по научно-исследовательской работе с учетом требований информационной безопасности
Стандартный (в дополнение к пороговому)	хорошо, но может допускать несущественные ошибки в принципах, методах и средствах решения стандартных задач профессиональной деятельности на основе	в целом успешно, иногда под руководством преподавателя решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом	хорошо навыками поиска и работы с информацией и подготовки материалов и документации по научно-исследовательской работе с учетом требований информационной безопасности

	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	основных требований информационной безопасности	
Повышенный (в дополнение к пороговому, стандартному)	хорошо и в полном объеме принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	самостоятельно и наилучшим образом решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	свободно навыками поиска и работы с информацией и подготовки материалов и документации по научно-исследовательской работе с учетом требований информационной безопасности

ОПК-2 - Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решения задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ОПК-2.1: Знать:	ОПК-2.2: Уметь:	ОПК-2.3: Владеть (иметь навыки):
	современные информационные технологии и программные средства, в том числе отечественного производства, используемые при решении задач профессиональной деятельности	понимать принципы работы и выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	навыками использования современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Пороговый	частично современные	успешно, но не систематически понимать	частично навыками использования

	информационные технологии и программные средства, в том числе отечественного производства, используемые при решении задач профессиональной деятельности	принципы работы и выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Стандартный (в дополнение к пороговому)	хорошо, но может допускать несущественные ошибки в современных информационных технологиях и программных средствах, в том числе отечественного производства, используемых при решении задач профессиональной деятельности	в целом успешно, иногда под руководством преподавателя понимать принципы работы и выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	хорошо навыками использования современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
Повышенный (в дополнение к пороговому, стандартному)	хорошо и в полном объеме современные информационные технологии и программные средства, в том числе отечественного производства, используемые при решении задач профессиональной деятельности	самостоятельно и наилучшим образом понимать принципы работы и выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	свободно навыками использования современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПКМ-6 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ОПКМ-6.1: Знать:	ОПКМ-6.2: Уметь:	ОПКМ-6.3: Владеть (иметь навыки):
	принципы работы информационных технологий; основные методы и	понимать принципы работы информационных технологий; использовать методы и программные средства сбора,	навыками использования современных информационных технологий и программных

	программные средства сбора, обработки и анализа информации	обработки и анализа данных для обеспечения информационно-аналитической поддержки принятия управленческих решений	средств для выбора управленческих решений
Пороговый	частично принципы работы информационных технологий; основные методы и программные средства сбора, обработки и анализа информации	успешно, но не систематически понимать принципы работы информационных технологий; использовать методы и программные средства сбора, обработки и анализа данных для обеспечения информационно-аналитической поддержки принятия управленческих решений	частично навыками использования современных информационных технологий и программных средств для выбора управленческих решений
Стандартный (в дополнение к пороговому)	хорошо, но может допускать несущественные ошибки в принципах работы информационных технологий; основных методах и программных средствах сбора, обработки и анализа информации	в целом успешно, иногда под руководством преподавателя понимать принципы работы информационных технологий; использовать методы и программные средства сбора, обработки и анализа данных для обеспечения информационно-аналитической поддержки принятия управленческих решений	хорошо навыками использования современных информационных технологий и программных средств для выбора управленческих решений
Повышенный (в дополнение к пороговому, стандартному)	хорошо и в полном объеме принципы работы информационных технологий; основные методы и программные средства сбора, обработки и анализа информации	самостоятельно и наилучшим образом понимать принципы работы информационных технологий; использовать методы и программные средства сбора, обработки и анализа данных для обеспечения информационно-аналитической поддержки принятия управленческих решений	свободно навыками использования современных информационных технологий и программных средств для выбора управленческих решений

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный

1.	Основные понятия информационной безопасности.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
2.	Принципы криптографической защиты информации.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
3.	Современные симметричные криптосистемы.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
4.	Асимметричные криптосистемы.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
5.	Идентификация и проверка подлинности.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
6.	Электронная цифровая подпись.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
7.	Управление криптографическими ключами.	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
8.	Политика ИБ	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2,	Тестирование. Устный/письменный опрос	зачет

		ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3		
9.	Оценка рисков ИБ	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет
10.	Программные средства защиты информации	УК-2.1, УК-2.2, УК- 2.3, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПКМ-6.1, ОПКМ-6.2, ОПКМ-6.3	Тестирование. Устный/письменный опрос	зачет

6.4.Оценочные материалы для текущего контроля

Вопросы для устного/письменного опроса

Раздел дисциплины	**Вопросы**
Основные понятия информационной безопасности	Основные понятия информационной безопасности передачи данных. Что включают базовые технологии информационной безопасности? Обеспечение безопасности сетей передачи данных. Классификация угроз безопасности корпоративных сетей. Чем обеспечивается целостность данных?
Принципы криптографической защиты информации.	Обобщенная схема симметричной криптосистемы. Пути реализации угроз безопасности информационных систем. Понятие политики безопасности и ее основные виды. Обобщенная схема асимметричной криптосистемы. Аппаратно-программные средства обеспечения компьютерной безопасности.
Современные симметричные криптосистемы.	Классическая сеть Фейстеля. Американский стандарт шифрования DES. Схема трехкратного алгоритма DES. Отечественный стандарт шифрования данных. Сущность принципа рассеивания. Блочные и поточные шифры.
Асимметричные криптосистемы.	Однонаправленные функции. Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Процедура шифрования в криптосистеме RSA. Схема шифрования Полига-Хеллмана. Комбинированный метод шифрования. Схема шифрования Эль Гамаля. Сущность систем шифрования с обратной связью.
Идентификация и проверка подлинности.	Основные понятия аутентификации и идентификации. Основные концепции аутентификации и идентификации. Основные типовые схемы идентификации пользователей. Основные

	типовые схемы аутентификации пользователей. Взаимная аутентификация пользователей. Принцип процедуры «рукопожатия». Схема идентификации Гиллоу-Куискуотера.
Электронная цифровая подпись.	Что из себя представляет электронная цифровая подпись? Назначение однонаправленных хэш-функций. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля.
Управление криптографическими ключами.	Назначение и особенности генерации ключей. Назначение и особенности хранения ключей. Концепция иерархии ключей. Назначение и особенности распределения ключей. Протокол аутентификации и распределения ключей для симметричных криптосистем. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей. Алгоритм открытого распределения ключей Диффи-Хеллмана.
Политика ИБ	Конфиденциальная информацию внутри организации и способы ее защиты. Процедура системного администрирования. Основные разделы политики ИБ. Способы организации управления доступом.
Оценка рисков ИБ	Управление рисками ИБ. Методики оценки рисков информационной безопасности. Расчет рисков ИБ.
Программные средства защиты информации	Защита информации от несанкционированного доступа (НСД). Анализ уязвимости программного обеспечения. Методы защиты от вредоносных программ. Средства идентификация и аутентификации пользователей.

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

1. Конфиденциальность данных (информации) это?
-внутреннее свойство информации;
-статус, представляемый данным и определяющий степень их защиты;
-значительные объемы информации;
-информация, предназначенная для передачи.
2. В чём отличие санкционированного (СД) и несанкционированного (НСД) доступа к информации?
-НСД не нарушает установленные правила;
-СД не нарушает установленные правила разграничения доступа;
-СД обеспечивает конфиденциальность информации;
-СД обеспечивает целостность информации.
3. Субъект информационной системы это?
-пользователь системы;
-активный компонент системы, который может стать причиной потока информации от объекта к субъекту;
-отправитель сообщения;
-получатель сообщения.
4. Объект информационной системы это?
-межсетевой экран
- шифратор;
-пассивный компонент системы, хранящий, принимающий или передающий информацию;
-скремблер

5. Целостность информации это:
-скрытность информации;
-важность информации;
-подлинность информации;
-объем информации
6. Угроза безопасности сети это:
-возможные разрушительные воздействия на сеть;
-нарушение работоспособности сети;
-отказ каналообразующего оборудования;
-отказ коммутационного оборудования.
7. Уязвимость сети это:
- отсутствие межсетевых экранов в сети;
-неудачное свойство сети, провоцирующее возникновение и реализацию угрозы;
-отсутствие средств активной защиты;
-отсутствие средств анализа защищенности
8. Атака на сеть это:
-нарушение конфиденциальности;
-нарушение целостности;
-нарушение доступности;
-реализация угрозы безопасности.
9. Политика безопасности это:
-организационно-правовое обеспечение информационной безопасности;
-административные меры обеспечения информационной безопасности;
-нормы, правила и практические рекомендации, регламентирующие работу средств защиты сетей;
-технические средства обеспечения информационной безопасности.
10. Дискреционная политика безопасности основана на:
-симметричном шифровании;
-асимметричном шифровании;
-электронной цифровой подписи;
-множестве заданных администратором разрешенных отношений доступа субъектов к объектам.
11. Полномочная политика безопасности основана на:
-алгоритме распределения ключей;
- представлении доступа в зависимости от метки конфиденциальности информации и уровня доверия пользователя;
- протоколах идентификации;
- протоколах аутентификации.
12. Цель процедуры идентификации заключается в:
-предъявлении субъектом своего уникального имени по запросу системы;
-доказательстве подлинности;
- доказательстве целостности;
-применении электронной цифровой подписи.
13. Цель процедуры аутентификации заключается в:
-управлении криптографическими ключами;
-антивирусной защите;
-доказательстве подлинности;
-противодействии угрозам безопасности
14. Назначение средств авторизации заключается в:
-распределении ключей;
- контроле доступа легальных пользователей к ресурсам системы;
-построении VPN;
-криптографической защите данных.
15. Назначение технологии аудита в информационной системе:
-обеспечение целостности;

-обеспечение конфиденциальности;
-фиксация в системном журнале событий, связанных с доступом к защищаемым ресурсам;
-устранение уязвимостей.
16. Симметричная криптосистема основана на применении:
-криптоалгоритма и одного секретного ключа;
- одного секретного ключа;
- двух секретных ключей;
-электронной цифровой подписи.
17. Асимметричная криптосистема основана на применении:
- защищенного канала;
-криптоалгоритма, открытого и секретного ключей;
-алгоритма скрытой передачи ключей;
-алгоритмов аутентификации.
18. Основные функции управления криптографическими ключами:
-шифрование ключей;
-распределение ключей;
-генерация, хранение и распределение ключей;
-сертификация ключей.
19. Цель сертификации открытых ключей:
-повышение защищенности системы;
-повышение надежности системы;
-обеспечение целостности открытых ключей;
-повышение быстродействия системы
20. Классической сетью Фейстеля называется:
-корпоративная сеть;
-виртуальная частная сеть VPN;
-методика обратимых преобразований данных;
-инфраструктура открытых ключей PKI.
21. Размер ключа стандарта ГОСТ 28147-86:
-128;
-512;
-256;
-64.
22. Количество раундов стандарта ГОСТ 28147-89:
-16;
-8;
-32;
-64.
23. Имитозащитой называется:
-идентификация;
-аутентификация;
-защита системы связи от навязывания ложных данных;
-генерация ключей.
24. Поточным шифрованием называется:
-стандарт DES;
-стандарт ГОСТ 28147-89;
-посимвольное шифрование;
-блочное шифрование.
25. Какое многократное шифрование позволяет увеличить длину результирующего ключа:
-шифрование DES;
-шифрование 3DES;
-шифрование ГОСТ 28147-89;
-шифрование RSA.
26. Криптосистема RSA относится:

-к симметричным криптосистемам;
-к асимметричным криптосистемам;
-к системам двукратного шифрования;
-к системам трехкратного шифрования;
27. Комбинированный метод шифрования предназначен для:
-формирования ЭЦП;
-проверки ЭЦП;
-скрытного (защищенного) распределения секретных ключей по открытому каналу;
-идентификации и аутентификации.
28. Протокол Гиллоу-Куискуотера предназначен для:
-шифрования данных;
-расшифрования данных;
-идентификации с нулевой передачей знаний;
- авторизации.
29. Электронная цифровая подпись (ЭЦП) предназначена для:
-шифрования данных;
-идентификации абонентов;
-аутентификации отправителя и контроля целостности электронного сообщения;
-обеспечения конфиденциальности.
30. Меры информационной безопасности направлены на защиту от:
-нанесения неприемлемого ущерба;
-НСД к информации;
-нанесения любого ущерба.

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	**Вопросы**
Основные понятия информационной безопасности	К какому типу угроз безопасности относится нарушение конфиденциальности информации либо ресурсов? Что понимается под безопасностью сети? Что такое уязвимость сети?
Принципы криптографической защиты информации.	Чем определяется стойкость шифра? Методика обратимых преобразований текста, при которой значение, вычисленное от одной из частей текста, накладывается на другие части? В каком режиме для обновления сдвигового регистра необходимо отбросить старшие k биты и дописать справа Pi?
Современные симметричные криптосистемы.	Чему равна длина ключа алгоритма IDEA? Чему равна длина ключа стандарта ГОСТ 28147-89? Для аутентификации данных используются какие режимы алгоритма DES? Чему равна длина ключа алгоритма DES? При каком режиме алгоритма DES вырабатывается код аутентификации сообщения? Чем определяется стойкость шифра?
Асимметричные криптосистемы.	Чему равна длина ключа алгоритма AES?
Идентификация и проверка подлинности.	К каким мерам относится организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией? К какой группе аппаратно-программных средств защиты относятся биометрические системы?
Электронная цифровая подпись.	К какому типу угроз безопасности относится нарушение конфиденциальности информации либо ресурсов? К какой группе аппаратно-программных средств

	защиты относится электронная цифровая подпись? Для чего предназначена цифровая подпись?
Управление криптографическими ключами	Прямой обмен ключами между пользователями. Протокол управления ключами.
Политика ИБ	Совокупность правил предоставления доступа в зависимости от метки конфиденциальности информации и уровня доступа пользователя? Что понимается под политикой безопасности?
Оценка рисков ИБ	. К какому типу стандартов могут относиться современные документы RFC? К правовым методам, обеспечивающим информационную безопасность, относятся какие методы?
Программные средства защиты информации	Программные или аппартно-программные системы анализа и диагностики локальных сетей, которые ограничиваются функциями мониторинга и анализа трафика? Сетевая атака на локальную сеть, происходящая, когда хакер, находящийся внутри сети или вне ее, выдает себя за санкционированного пользователя?

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»	УК-2, ОПК-3, ОПК-2, ОПКМ-6
«не зачтено»	Результаты обучения не сформированы на пороговом уровне