МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 2

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Основы управления информационной безопасностью
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Ассистент
Ковтун Д.Б.

Профессор, д.э.н.
Назаров Д.М.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины Основы управления информационной безопасностью является формирование у студентов компетенции обучающегося в области основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта, целостного представления об информации, информационной безопасности, информационных системах и технологиях обработки данных; о роли информационной безопасности в современном обществе; раскрытие возможностей управления информационной безопасностью при решении профессиональных задач; развитие навыков использования средств и методов информационной безопасности для совершенствования профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Зачет	144	64	32	32	80	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД-1.ОПК-1 Знает основы информационной культуры

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД-2.ОПК-1 Умеет решать стандартные задачи профессиональной деятельности с использованием информационных технологий с соблюдением требований информационной безопасности
	ИД-3.ОПК-1 Владеет навыками использования информационных технологий для поиска и обработки информации
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ИД-1.ОПК-2 Знать: программные средства системного, прикладного и специального назначения, инструментальные средства, в том числе отечественного производства
	ИД-2.ОПК-2 Уметь: выбирать и применять необходимые инструментальные средства для решения профессиональных задач
	ИД-3.ОПК-2 Владеть навыками работы в программные средства системного, прикладного и специального назначения, инструментальными средствами, в том числе отечественного производства

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ИД-1.ОПК-6 Знать: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области
	ИД-2.ОПК-6 Уметь: пользоваться нормативными документами по защите информации; обеспечивать сохранность и неизменность обрабатываемой информации
	ИД-3.ОПК-6 Владеть навыками: защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 6		30					
Тема 1.	Введение. Базовая терминология (ОПК-1)	30	2	8		20	

Семестр 6		23					
Тема 2.	Обеспечение информационной безопасности бизнеса (ОПК-1, ОПК-6)	23	4	4		15	
Семестр 6		13					
Тема 3.	Система управления информационной безопасностью бизнеса (ОПК-1, ОПК-6)	13	2	2		9	
Семестр 6		16					
Тема 4.	Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6)	16	5	2		9	
Семестр 6		11					
Тема 5.	Социальные аспекты системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6)	11	9	2			
Семестр 6		18					
Тема 6.	Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (ОПК-1, ОПК-2, ОПК-6)	18	5	4		9	
Семестр 6		19					
Тема 7.	Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (ОПК-1, ОПК-2, ОПК-6)	19	5	5		9	
Семестр 6		14					
Тема 8.	Аудит методов и средств обеспечения информационной безопасности предприятия (ОПК-1, ОПК-2, ОПК-6)	14		5		9	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1. Введение. Базовая терминология	Контрольная работа №1 (Приложение 4)	Контрольная работа состоит из 5 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 2. Обеспечение информационной безопасности бизнеса	Контрольная работа №2 (Приложение 4)	Контрольная работа состоит из 5 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

Тема 3. Система управления информационной безопасностью бизнеса	Доклад, сообщение (Приложение 4)	Предлагается список из 8 тем	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса	Тест № 1 (Приложение 4)	Тест состоит из 10 вопросов	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса	Доклад, сообщение (Приложение 4)	Предлагается список из 10 тем	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации	Доклад, сообщение (Приложение 4)	Предлагается список из 10 тем	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации	Доклад, сообщение (Приложение 4)	Предлагается список из 10 тем	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

Тема 8. Аудит методов и средств обеспечения информационной безопасности предприятия	Доклад, сообщение (Приложение 4)	Предлагается список из 10 тем	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Промежуточная аттестация(Приложение 5)			
6 семестр (За)	Билет для зачета (Приложение 5)	20 билетов 1 теоретический и 1 практический вопрос	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Введение. Базовая терминология (ОПК-1) Введение в процесс управления информационной безопасностью. Базовая терминология.
Тема 2. Обеспечение информационной безопасности бизнеса (ОПК-1, ОПК-6) Деятельность по обеспечению информационной безопасностью организации. Основные методы управления информационной безопасностью. Управление информационной безопасностью информационно-телекоммуникационными технологиями организации.
Тема 3. Система управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Система управления информационной безопасностью бизнеса.
Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Основные способы и параметры оценки показателей СУИБ в бизнесе
Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Социальный инжиниринг: основные направления угроз для ИБ организации
Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (ОПК-1, ОПК-2, ОПК-6) Методы управления информационными рисками.
Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (ОПК-1, ОПК-2, ОПК-6) Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Обеспечение информационной безопасности бизнеса (ОПК-1, ОПК-6) Построение классификации базовых способов обеспечения ИБ в организации
Тема 3. Система управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Способы применения СУИБ в бизнесе
Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.
Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Применение СУИБ с учетом социального аспекта, как угрозы для информационной безопасности предприятия

Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (ОПК-1, ОПК-2, ОПК-6) Анализ влияния информационного риска на деятельность организации.
Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (ОПК-1, ОПК-2, ОПК-6) Проведение плановых мероприятий по профилактике и предотвращению угроз ИБ
Тема 8. Аудит методов и средств обеспечения информационной безопасности предприятия (ОПК-1, ОПК-2, ОПК-6) Аудит методов и средств обеспечения информационной безопасности предприятия

7.3. Содержание самостоятельной работы

Тема 2. Обеспечение информационной безопасности бизнеса (ОПК-1, ОПК-6) Обеспечение информационной безопасности бизнеса
Тема 3. Система управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Изучение и анализ современных СУИБ
Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (ОПК-1, ОПК-6) Изучение альтернативных методов оценки и анализа показателей СУИБ
Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (ОПК-1, ОПК-2, ОПК-6) Способы оценки и анализа влияния информационного риска на деятельность организации
Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (ОПК-1, ОПК-2, ОПК-6) Современное представление в СУИБ о плановых мероприятиях по предотвращению угроз ИБ
Тема 8. Аудит методов и средств обеспечения информационной безопасности предприятия (ОПК-1, ОПК-2, ОПК-6) Изучение основных методов и подходов к проведению аудита информационной безопасности

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Курсовые работы не предусмотрены

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
учебным планом не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
учебным планом не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие. - Москва: Издательский Центр РИО, 2022. - 336 – Режим доступа: https://znanium.ru/catalog/product/1861657

3. Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю. Криптографическая защита информации [Электронный ресурс]:Учебное пособие : Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2025. - 321 – Режим доступа: https://znanium.com/catalog/product/2169480

4. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2025. - 355 – Режим доступа: https://znanium.com/catalog/product/2173934

5. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 357 – Режим доступа: https://urait.ru/bcode/560516

6. Внуков А. А. Защита информации [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 161 – Режим доступа: https://urait.ru/bcode/561313

7. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2025. - 336 – Режим доступа: https://znanium.com/catalog/product/2178344

Дополнительная литература:

2. Гришина Н. В. Основы управления информационной безопасностью [Электронный ресурс]:Учебно-методическая литература. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 99 – Режим доступа: https://znanium.com/catalog/product/1859951

3. Бабаш А.В., Баранова Е.К. Моделирование системы защиты информации: Практикум [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО&#65533;, 2023. - 320 – Режим доступа: https://znanium.com/catalog/product/2038247

4. Гришина Н. В. Основы информационной безопасности предприятия [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 216 – Режим доступа: https://znanium.com/catalog/product/2131865

5. Внуков А. А. Защита информации [Электронный ресурс]:учебное пособие для вузов. - Москва: Юрайт, 2024. - 161 – Режим доступа: https://urait.ru/bcode/537247

6. Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 357 – Режим доступа: https://urait.ru/bcode/555950

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

Вопросы к зачету

1. Стоимостные характеристики информации и их соотношения.
2. Internet как среда для компьютерных преступлений.
3. Основные задачи информационной безопасности.
4. Основные методы обеспечения защиты информационной системы.
5. Определение и классификация угроз.
6. Потенциальные противники: классификация и характеристика.
7. Каналы утечки информации.
8. Классификация атак и их характеристики.
9. Сетевые атаки: основные виды.
10. Основные положения информационной безопасности.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.
14. Что понимается под системой безопасности?
15. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
16. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процесами?
17. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.
18. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
19. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.
20. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?
21. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
22. Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими? Назовите основные способы неправомерного овладения конфиденциальной информацией.
23. Какие основные понятия рассматриваются в Законе РФ "Об информации, информатизации и защите информации"?
24. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.
25. Дайте определение и перечислите основные способы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД источников конфиденциальной информации.
26. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации?

27. Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.
28. Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности.
29. Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?
30. Какие Вам известны американские законы, напрямую связанные с ИБ? Что можно сказать о законодательстве ФРГ по вопросам ИБ?
31. Что такое защита информации?
32. Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?
33. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?
34. Охарактеризуйте понятия доступности, целостности и конфиденциальности информации.
35. Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?
36. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне.
37. Прокомментируйте основные составляющие информационной безопасности РФ.
38. Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?
39. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности?
40. Приведите примерный список решений верхнего уровня политики безопасности.
41. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
42. Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными?
43. Что такое программа безопасности, ее уровни.
44. Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности.
45. Что такое канал НСД? Назовите типовые причины их возникновения.
46. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?
47. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
48. Назовите основные способы добывания конфиденциальной информации злоумышленником.
49. В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?
50. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
51. Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.
52. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
53. В чем специфика деятельности ФСТЭК России?
54. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.

55. Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.
56. Почему уровень ИБ в России в настоящее время не соответствует жизненно важным потребностям личности, общества и государства и какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
57. Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность.
58. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
59. Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
60. Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
61. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?
62. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.
63. Охарактеризуйте основные угрозы целостности конфиденциальной информации. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?
64. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности
65. Перечислите основные угрозы конфиденциальности информации.
66. Прокомментируйте возможности биометрической идентификации (аутентификации).
67. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
68. Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.
69. В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?
70. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
71. Что такое защита от разглашения?
72. Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?
73. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.
74. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.
75. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.
76. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?
77. Дайте определение персональных данных. Какие сведения могут быть

78. Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?
79. Политика безопасности информационных систем.
80. Таксономия нарушений информационной безопасности вычислительной системы.
81. Уровни правового обеспечения информационной безопасности.
82. Доктрина информационной безопасности России.
83. Основные аппаратные средства защиты. Основные программные средства защиты.
84. Основные методы идентификации и аутентификации.
85. Сервисы управления доступом.
86. Протоколирование и аудит. Задачи аудита.
87. Основы защиты Internet-подключений.
88. Стандарты обеспечения информационной безопасности.
89. Общие принципы построения защищенных систем.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

ЗАДАНИЯ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ
10.03.01 Информационная безопасность
Дисциплина: Основы управления информационной безопасностью

Компетенция ОПК-1; ОПК-2; ОПК-6

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Задания закрытого типа

1. Как называется процесс обнаружения и устранения уязвимостей в системе информационной безопасности?

A. Анализ угроз

B. Криптография

C. Проверка безопасности

D. Резервное копирование

Ответ: C

2. Какие из перечисленных ниже паролей наиболее надежны?

A. 123456

B. qwerty

C. 5f9d8bf45c1900a0

D. password

Ответ: C

3. Что такое двухфакторная аутентификация?

A. Ввод логина и пароля

B. Использование отпечатка пальца для входа в систему

C. Использование смарт-карты и пароля для входа в систему

D. Использование нескольких различных методов для подтверждения личности пользователя

Ответ: D

4. Каким образом можно защитить себя от вирусов и вредоносного ПО?

A. Использовать сложные пароли

B. Резервирование данных

C. Установка антивирусного программного обеспечения

D. Использование облачного хранилища данных

Ответ: C

5. Что такое SSL-шифрование?

A. Защита от вирусов и вредоносного ПО

B. Протокол безопасного соединения для передачи данных через Интернет

C. Формат шифрованного пароля

D. Система контроля доступа к защищенным данным

Ответ: B

6. Какой нормативный акт определяет общие принципы организации информационной безопасности в организациях и органах государственной власти Российской Федерации?

a) Федеральный закон "Об информации, информационных технологиях и о защите информации"

b) Федеральный закон "Об информационной безопасности"

c) Постановление Правительства Российской Федерации "Об утверждении правил защиты конфиденциальной информации"

d) Приказ Министерства связи и массовых коммуникаций Российской Федерации "Об утверждении требований к защите персональных данных"

Ответ: b) Федеральный закон "Об информационной безопасности"

7. Какой документ определяет требования к методам и средствам защиты информации от несанкционированного доступа, утечки и искажения?

a) ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

b) ГОСТ Р 52854-2007 "Защита информации. Термины и определения"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по организации системы защиты информации в банковской сфере

Ответ: a) ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

8. Какой тип шифрования является наиболее безопасным?
    a) DES
    b) AES
    c) RC4
    d) MD5

    Правильный ответ: b) AES.

9. Какой тип угрозы безопасности данных может привести к потере данных, если вы не сделаете резервную копию?
    a) Хакерские атаки
    b) Вирусы
    c) Кража личной информации
    d) Ошибка пользователя

    Правильный ответ: d) Ошибка пользователя.

10. Что означает термин "социальная инженерия"?
    a) Атака на базу данных
    b) Хакерский взлом
    c) Использование обмана для получения доступа к системе
    d) Использование программного обеспечения для взлома паролей

    Правильный ответ: c) Использование обмана для получения доступа к системе.

11. Какой документ содержит требования к организации процесса управления информационной безопасностью и управлению рисками?

a) ГОСТ Р 52854-2007 "Защита информации. Термины и определения"

b) Постановление Правительства Российской Федерации "Об утверждении правил защиты конфиденциальной информации"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по организации системы защиты информации в банковской сфере

Ответ: d) Методические рекомендации по организации системы защиты информации в банковской сфере

12. Какой документ содержит перечень мер по защите информации на предприятии?

a) Федеральный закон "Об информации, информационных технологиях и о защите информации"

b) Приказ Министерства связи и массовых коммуникаций Российской Федерации "Об утверждении требований к защите персональных данных"

c) Руководство по защите информации в государственных органах Российской Федерации

d) Методические рекомендации по защите информации на предприятии

Ответ: d) Методические рекомендации по защите информации на предприятии

12. Какой тип кибератаки пытается перегрузить веб-сервер, отправляя большое количество запросов?
    a) Фишинг
    b) DDoS
    c) Кросс-сайтовый скриптинг
    d) SQL-инъекция

Правильный ответ: b) DDoS.

13. Какое программное обеспечение защищает компьютеры от вредоносных программ?
    a) Антивирус
    b) Фаервол
    c) VPN
    d) Интранет

Правильный ответ: a) Антивирус.

14. Что такое пароль?
    a) Символьная строка, используемая для доступа к устройству или приложению
    b) Метка, которая идентифицирует устройство в сети
    c) Физическое устройство, которое используется для хранения данных
    d) Название компании, которая разработала операционную систему

Ответ: a

15. Что такое антивирусное программное обеспечение?
    a) Программа, которая защищает компьютер от вирусов
    b) Программа, которая создает вирусы
    c) Программа, которая удаляет важные файлы с компьютера
    d) Программа, которая ускоряет работу компьютера

Ответ: a

16. Что означает термин "фишинг" в контексте информационной безопасности?
    a) Кража паролей и логинов с уязвимых сайтов
    b) Отправка ложных сообщений с целью обмана пользователей
    c) Незаконный доступ к защищенным данным
    d) Использование вредоносного ПО для получения доступа к системе

Ответ: B

Задания открытого типа

1. Что такое пароль? Приведите пример типов паролей.
2. Какие существуют методы аутентификации пользователей? Приведите пример одного из методов.
3. Что такое безопасность веб-сервисов и как она обеспечивается? Приведите пример уязвимостей веб-сервисов и методов их защиты.
4. Как работает система защиты информации на уровне операционной системы? Приведите пример операционных систем и методов защиты информации на уровне ОС.
5. Что такое защита от DDoS-атак и как она реализуется? Приведите пример инструментов и технологий для защиты от DDoS-атак.
6. Какие существуют методы защиты от фишинга и социальной инженерии? Приведите пример инструментов и технологий для защиты от фишинга и социальной инженерии.
7. Как работает система управления доступом и как она обеспечивает безопасность в информационных системах? Приведите пример инструментов для управления доступом и методов их применения.
8. Что такое целостность данных и как она обеспечивается? Приведите пример методов обеспечения целостности данных.
9. Как работают системы обнаружения вторжений и как они помогают защитить информационные системы от кибератак? Приведите пример систем обнаружения вторжений.
10. Какие существуют методы шифрования и как они применяются для защиты данных? Приведите пример алгоритмов шифрования и
11. Что такое социальная инженерия? Приведите пример методов социальной инженерии.
12. Что такое VPN? Приведите пример популярных VPN-сервисов.

13. Что такое анализ угроз и как он используется для определения уровня риска в информационной безопасности? Приведите пример инструментов для проведения анализа угроз.
14. Какие документы регламентируют требования к хранению и обработке персональных данных в Российской Федерации? Приведите пример требований, установленных данными документами.
15. Примерный Ответ: Приказ Минкомсвязи России № 84 от 13.06.2016 "Об утверждении требований к организации хранения, обработки и передачи персональных данных" и Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". Пример требования: необходимость обеспечения конфиденциальности персональных данных и защиты от несанкционированного доступа к ним.
16. Какие нормативные акты регулируют порядок работы с государственной тайной в Российской Федерации? Приведите пример одного из них.
    Примерный Ответ: Федеральный закон "Об основах государственной тайны в Российской Федерации" и Указ Президента Российской Федерации от 11.03.2019 № 152 "О вопросах государственной тайны в Российской Федерации". Пример: необходимость проведения предварительной проверки лиц, имеющих доступ к сведениям, составляющим государственную тайну.

17. Какой документ определяет общие требования к организации системы управления информационной безопасностью в организациях и органах государственной власти Российской Федерации? Приведите пример одного из требований.
    Примерный Ответ: Федеральный закон "Об информационной безопасности" от 27.07.2006 № 149-ФЗ. Пример требования: необходимость организации регулярного анализа уязвимостей системы информационной безопасности.
18. Какие методические документы используются для определения угроз информационной безопасности? Приведите пример одного из них.
    Примерный Ответ: Методические рекомендации по организации системы защиты информации в банковской сфере и Методические рекомендации по проведению оценки уязвимости системы информационной безопасности. Пример: использование методики проведения анализа рисков и уязвимостей системы информационной безопасности.
19. Какие методические документы используются для определения угроз информационной безопасности? Приведите пример одного из них.
    Примерный ответ: Методические рекомендации по организации системы защиты информации в банковской сфере и Методические рекомендации по проведению оценки уязвимости системы информационной безопасности. Пример: использование методики проведения анализа рисков и уязвимостей системы информационной безопасности.
20. Какие требования установлены для защиты информации в области электронной торговли? Приведите пример одного из таких требований.

Ответ: Для защиты информации в области электронной торговли установлены требования к безопасности электронных платежных систем, криптографической защите информации и защите от вредоносного программного обеспечения. Пример требования: использование протоколов безопасной передачи данных (например, SSL или TLS) при работе с веб-сайтами электронной торговли.

21. Что такое вирус-шифровальщик? Приведите пример известных вирусов-шифровальщиков.
22. Что такое брутфорс? Приведите пример ситуаций, когда используется брутфорс.
23. Что такое хакер? Приведите пример разновидностей хакеров.
24. Что такое спам? Приведите пример типов спама.
25. Что такое социальная инженерия? Приведите пример методов социальной инженерии.
26. Что такое шифрование данных? Приведите пример алгоритмов шифрования.
27. Что такое VPN? Приведите пример популярных VPN-сервисов.
28. Что такое межсетевой экран?
29. Каковы основные принципы криптографии и как они используются для обеспечения информационной безопасности? Приведите пример алгоритмов криптографии.
30. Что такое ботнеты и как они используются для проведения кибератак? Приведите пример ботнетов.
31. Какие существуют методы защиты от SQL-инъекций? Приведите пример инструментов для защиты от SQL-инъекций.
32. Каковы основные уязвимости, связанные с безопасностью IoT-устройств? Приведите пример конкретных устройств и типов атак на них.