

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФИНАНСОВЫЙ УНИВЕРСИТЕТ)

Калужский филиал Финуниверситета

УТВЕРЖДАЮ

Заместитель директора по учебно-методической работе Калужского филиала ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»



О.М. Орловцева

«27» мая 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

09.02.12 Техническая эксплуатация и сопровождение информационных систем

Калуга 2026 г.

РАССМОТРЕН
Предметной (цикловой) комиссией

Разработан на основе Федерального
государственного образовательного
стандарта среднего профессионального
образования по специальности 09.02.12
Техническая эксплуатация и
сопровождение информационных систем

Протокол №01

от «25» марта 2026 г.

Председатель
предметной (цикловой) комиссии


_____ И.В. Дробышева

Заместитель директора
по учебно-методической работе


_____ О.М. Орловцева

ОДОБРЕН

Учебно-методическим советом Калужского
филиала ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»

Протокол №05

от «20» апреля 2026 г.

Составители:

Винокуров И.В. - доцент кафедры «Бизнес – информатика и высшая математика», к.т.н., доцент Калужского филиала ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА.....	4
I. ОБЩАЯ ХАРАКТЕРИСТИКА ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ	8
II. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ	10
2.1 Основные печатные издания	10
2.2. Дополнительные источники:.....	11
2.3. Перечень ресурсов информационно-телекоммуникационной сети.....	11
«Интернет», необходимых для освоения дисциплины	11
III. ОЦЕНОЧНЫЕ СРЕДСТВА.....	12
IV. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	29

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Фонд оценочных средств (далее ФОС) по дисциплине ОП.06. «Основы информационной безопасности» предназначен для студентов, обучающихся по программам среднего профессионального образования (далее СПО) специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

ФОС разработан на основании:

- требований к уровню подготовки обучающихся ФГОС СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем;

- основной образовательной программы и учебного плана СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем;

- рабочей программы дисциплины ОП.06. «Основы информационной безопасности», реализуемой в соответствии с ФГОС СПО.

ФОС по дисциплине ОП.06. «Основы информационной безопасности» разработан с целью контроля и управления процессом приобретения обучающимися необходимых знаний, умений, навыков, а также уровня сформированности общих компетенций (далее ОК) и профессиональных компетенций (далее ПК) в объеме рабочей программы дисциплины по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

ФОС включает контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачета.

В результате освоения дисциплины обучающийся должен:

знать:

актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях;

основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах;

порядок оценки результатов решения задач профессиональной деятельности

номенклатура информационных источников, применяемых в профессиональной деятельности;

приемы структурирования информации; формат оформления результатов поиска информации;

современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства

психологические основы деятельности коллектива;

психологические особенности личности

правила построения простых и сложных предложений на профессиональные темы;

основные общеупотребительные глаголы (бытовая и профессиональная лексика);

лексический минимум, относящийся к описанию предметов, средств и процессов

профессиональной деятельности;

особенности произношения;

правила чтения текстов профессиональной направленности

Основы ИБ организации;

Модель угроз информационной безопасности ИС организации заказчика;

Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика;
Основы администрирования СУБД;
Основы системного администрирования;
Коммуникационное оборудование;
Сетевые протоколы;
Основы современных операционных систем;
Устройство и функционирование современных ИС;
Основы архитектуры мультиарендного программного обеспечения
Понятие и классификация инцидентов ИБ;
Типичные угрозы ИБ при работе с БД;
Процедуры и регламенты передачи информации об инцидентах в службу ИБ организации;
Средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры);
Основы работы со средствами антивирусной защиты;
Основы ИБ;
Основы деловой этики;
Правила деловой переписки

уметь:

распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять ее составные части;
определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;
владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска;
применять средства информационных технологий для решения профессиональных задач;
использовать современное программное обеспечение в профессиональной деятельности;
использовать различные цифровые средства для решения профессиональных задач
организовывать работу коллектива и команды;
взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;
участвовать в диалогах на знакомые общие и профессиональные темы;
строить простые высказывания о себе и о своей профессиональной деятельности;
кратко обосновывать и объяснять свои действия (текущие и планируемые);
писать простые связные сообщения на знакомые или интересующие профессиональные темы
Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
обеспечения
Идентифицировать инциденты ИБ при работе с БД;

Осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации);
Управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ;
Устанавливать и сопровождать антивирусное ПО

иметь практические навыки:

Распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Передачи информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Информирования заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС;
Временного блокирования доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
Распознавания инцидентов ИБ при работе с БД;
Формирования перечня инцидентов ИБ;
Передачи информации об инцидентах в службу ИБ организации;
Временного блокирования доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости);
Поддержания баз антивирусных программ в актуальном состоянии

достигнуть личностных результатов:

- Проявлять и демонстрировать уважение к труду человека, осознавать ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
- Ориентироваться на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации
- Соблюдать в своей профессиональной деятельности этические принципы: честности, независимости, профессионального скептицизма, противодействия коррупции и экстремизму, обладающий системным мышлением и умением принимать решение в условиях риска и неопределенности
- Готовый соответствовать ожиданиям работодателей: проектно- мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость
- Открытый к текущим и перспективным изменениям в мире труда и профессий
- Осознающий состояние социально-экономического развития потенциала Калужской области и содействующий его развитию
- Обладающий ключевыми цифровыми компетенциями и готовностью их применять в современных экономических условиях
- Демонстрирующий готовность к участию в инновационной деятельности Калужского региона.
- Владеющий культурой мышления и способный максимально реализовывать свой профессиональный потенциал в современной и глобальной экономике

Оценка результатов освоения обучающимися дисциплины ОП.06. «Основы информационной безопасности» осуществляется с использованием следующих форм и методов контроля:

текущий:

- устный и письменный опрос;
- выполнения тестовых заданий;
- подготовка рефератов, докладов, сообщений
- выполнение заданий контрольных работ
- выполнения ситуационных заданий;

Промежуточная аттестация – дифференцированный зачет

I. ОБЩАЯ ХАРАКТЕРИСТИКА ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине ОП.06 «Основы информационной безопасности»
по специальности 09.02.12 Техническая эксплуатация и сопровождение
информационных систем

Результаты обучения	Код и формулировка компетенции (ОК, ПК)	Наименование разделов и тем	Формы и методы оценки	
			Текущий контроль	Промежуточная аттестация
1	2	3	4	5
<p>Освоенные знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства психологические основы деятельности коллектива; психологические особенности личности правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности Основы ИБ организации; Модель угроз информационной безопасности ИС организации заказчика; Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика;</p>	<p>ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности ОК 04. Эффективно взаимодействовать и работать в коллективе и команде ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках ПК 1.7. Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем. ПК 2.5 Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных</p>	<p>Раздел 1. Теоретические основы информационной безопасности</p> <p>Тема 1.1. Основные понятия и задачи информационной безопасности</p> <p>Тема 1.2. Основы защиты информации</p> <p>Тема 1.3. Угрозы безопасности защищаемой информации</p>	<p>устный и письменный опрос; выполнения тестовых заданий; подготовка рефератов, докладов, сообщений выполнение заданий контрольных работ выполнения ситуационных заданий;</p>	<p>Промежуточная аттестация в форме дифференцированного зачета</p>

<p>Основы администрирования СУБД; Основы системного администрирования; Коммуникационное оборудование; Сетевые протоколы; Основы современных операционных систем; Устройство и функционирование современных ИС; Основы архитектуры мультитенантного программного обеспечения Понятие и классификация инцидентов ИБ; Типичные угрозы ИБ при работе с БД; Процедуры и регламенты передачи информации об инцидентах в службу ИБ организации; Средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры); Основы работы со средствами антивирусной защиты; Основы ИБ; Основы деловой этики; Правила деловой переписки</p> <p>Освоенные умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять ее составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС обеспечения Идентифицировать инциденты ИБ при работе с БД; Осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации); Управлять доступом пользователей к элементам БД</p>	<p>ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности ОК 04. Эффективно взаимодействовать и работать в коллективе и команде ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках ПК 1.7. Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем. ПК 2.5 Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных</p>	<p>Раздел 2. Методология защиты информации</p> <p>Тема 2.1. Методологические подходы к защите информации</p> <p>Тема 2.2. Нормативно-правовое регулирование защиты информации</p> <p>Тема 2.3. Защита информации в автоматизированных (информационных) системах</p>	<p>устный и письменный опрос; выполнения тестовых заданий; подготовка рефератов, докладов, сообщений выполнение заданий контрольных работ выполнения ситуационных заданий;</p>	<p>Промежуточная аттестация в форме дифференцированного зачета</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------

<p>при обнаружении инцидентов ИБ; Устанавливать и сопровождать антивирусное ПО</p> <p>Практические навыки: Распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Передачи информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Информирования заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Временного блокирования доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Распознавания инцидентов ИБ при работе с БД; Формирования перечня инцидентов ИБ; Передачи информации об инцидентах в службу ИБ организации; Временного блокирования доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости); Поддержания баз антивирусных программ в актуальном состоянии</p>				
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

II. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Перечень рекомендуемых учебных изданий, Интернет- ресурсов, дополнительной литературы.

2.1 Основные печатные издания

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948- 8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>.
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518005>.
3. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5- 534-15345-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519614>.

2.2. Дополнительные источники:

4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861>.
5. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/156401>. — Режим доступа: для авториз. пользователей.

2.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
2. Электронно-библиотечная система Znanium <http://www.znaniy.com>
3. Электронно-библиотечная система издательства «ЮРАЙТ» <https://www.biblio-online.ru>
4. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>
5. Электронная библиотека издательского дома «Гребенников» <https://grebennikon.ru>
6. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com>

III. ОЦЕНОЧНЫЕ СРЕДСТВА

Приложение 1

Вопросы устного/письменного опроса

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

1. Дайте определение информационной безопасности. Назовите три основные составляющие ИБ.
2. Что понимается под угрозой информационной безопасности? Классификация угроз.
3. Какие существуют каналы утечки информации? Приведите примеры.
4. В чем разница между преднамеренными и непреднамеренными угрозами?
5. Понятие уязвимости. Приведите примеры уязвимостей программного обеспечения.
6. Что такое политика информационной безопасности организации?
7. Назовите основные организационные меры защиты информации.
8. Каковы основные требования к паролям и их хранению?
9. Что такое идентификация и аутентификация? Методы аутентификации.
10. В чем суть двухфакторной аутентификации? Приведите примеры.
11. Дискреционная, мандатная и ролевая модели управления доступом.
12. Что такое межсетевой экран (фаервол)? Принципы работы.
13. Какие существуют типы межсетевых экранов?
14. Понятие VPN. Назначение и основные протоколы.
15. Как обеспечивается защита в беспроводных сетях Wi-Fi?
16. Классификация вредоносного программного обеспечения.
17. Какие признаки заражения компьютера вирусом вы знаете?
18. Принципы работы антивирусных программ (сигнатурный, эвристический, поведенческий).
19. Что такое «социальная инженерия»? Назовите типичные методы.
20. Как защититься от фишинговых атак?
21. Основы криптографии. Симметричное и асимметричное шифрование.
22. Что такое электронная подпись? Для чего она используется?
23. Назовите основные алгоритмы хэширования и их свойства.
24. Какие требования предъявляет Федеральный закон № 152-ФЗ «О персональных данных»?
25. Каковы права субъекта персональных данных?
26. Что такое DLP-системы? Какие задачи они решают?
27. Системы обнаружения и предотвращения вторжений (IDS/IPS).
28. Управление инцидентами информационной безопасности: основные этапы.
29. Что такое «тестирование на проникновение» (пентест)?
30. Как организуется резервное копирование данных с точки зрения ИБ?
31. Каковы основные риски использования облачных сервисов?
32. Что входит в понятие «кибергигиена»?

33. Назовите основные стандарты в области ИБ (ISO 27001, СТО БР ИББС и др.).
34. Какие меры защиты применяются для предотвращения утечек через съёмные носители?
35. Как следует реагировать на обнаружение программ-вымогателей (ransomware)?

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

Тестовые задания

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

1. Какое из определений наиболее полно соответствует понятию «информационная безопасность»?
 - а) защита информации от случайных воздействий
 - б) состояние защищённости информации, обрабатываемой техническими средствами
 - в) состояние защищённости интересов личности, общества и государства в информационной сфере
 - г) совокупность организационных и технических мер по защите информации
2. Что не относится к основным свойствам информации, обеспечиваемым ИБ?
 - а) конфиденциальность
 - б) целостность
 - в) доступность
 - г) актуальность
3. Какой метод шифрования использует один и тот же ключ для шифрования и расшифрования?
 - а) асимметричный
 - б) симметричный
 - в) хэширование
 - г) стеганография
4. Какой протокол обеспечивает защищённое соединение в сети Интернет?
 - а) HTTP
 - б) FTP
 - в) HTTPS
 - г) SMTP
5. Что такое «фишинг»?
 - а) вид компьютерного вируса
 - б) метод социальной инженерии, направленный на получение конфиденциальных данных
 - в) способ шифрования данных
 - г) программный брандмауэр
6. Какое средство предназначено для обнаружения вторжений в реальном времени?
 - а) DLP
 - б) IDS
 - в) VPN

г) SSL

7. Какой закон является основным в области персональных данных в РФ?

- а) ФЗ «Об информации, информационных технологиях и о защите информации»
- б) ФЗ «О персональных данных»
- в) ФЗ «О безопасности»
- г) ФЗ «О связи»

8. Какой из перечисленных паролей является наиболее надёжным?

- а) 123456
- б) qwerty
- в) P@ssw0rd
- г) iloveyou

9. Какой тип вредоносного ПО блокирует доступ к данным и требует выкуп?

- а) троян
- б) червь
- в) ransomware
- г) шпионское ПО

10. Что такое DLP-система?

- а) система предотвращения утечек данных
- б) система обнаружения вторжений
- в) межсетевой экран
- г) антивирус

11. Какая модель управления доступом определяет права на основе ролей пользователя?

- а) дискреционная
- б) мандатная
- в) ролевая
- г) произвольная

12. Какой протокол используется для создания VPN-соединений на уровне каналов?

- а) IPSec
- б) SSL
- в) L2TP
- г) SSH

13. Какое требование предъявляется к обработке персональных данных без согласия субъекта?

- а) согласие всегда обязательно
- б) обработка разрешена, если это необходимо для исполнения договора
- в) обработка запрещена в любом случае

г) обработка разрешена для коммерческих целей

14. Что такое «сетевая уязвимость»?

- а) недостаток в программном обеспечении, позволяющий нарушить безопасность
- б) неправильная настройка оборудования
- в) ошибка пользователя
- г) неисправность кабеля

15. Какой метод аутентификации является биометрическим?

- а) пароль
- б) смарт-карта
- в) сканер отпечатков пальцев
- г) одноразовый код из SMS

16. Какой протокол используется для защищённого удалённого управления?

- а) Telnet
- б) RDP
- в) SSH
- г) SNMP

17. Что такое «хэш-функция»?

- а) алгоритм шифрования
- б) функция, преобразующая данные произвольной длины в строку фиксированной длины
- в) метод сжатия данных
- г) протокол аутентификации

18. Какое действие не относится к организационной защите информации?

- а) установка межсетевого экрана
- б) разработка политики ИБ
- в) проведение тренингов для сотрудников
- г) определение уровня доступа к информации

19. Для чего используется электронная подпись?

- а) для шифрования сообщения
- б) для подтверждения авторства и неизменности документа
- в) для сжатия документа
- г) для ускорения передачи

20. Что означает принцип «need to know» (необходимо знать) в управлении доступом?

- а) доступ предоставляется только по служебной необходимости
- б) доступ открыт всем, кто знает пароль
- в) доступ зависит от времени суток

г) доступ ограничен по IP-адресу

21. Что такое «спуфинг»?

- а) подмена сетевого адреса или идентификатора
- б) анализ трафика
- в) удалённое управление
- г) шифрование данных

22. Какой алгоритм является асимметричным?

- а) AES
- б) RSA
- в) DES
- г) 3DES

23. Для чего предназначен протокол SSL/TLS?

- а) для маршрутизации пакетов
- б) для обеспечения шифрования между клиентом и сервером
- в) для преобразования адресов
- г) для мониторинга сети

24. Что из перечисленного является примером двухфакторной аутентификации?

- а) пароль + пин-код
- б) пароль + одноразовый код из приложения
- в) логин + пароль
- г) отпечаток пальца + имя

25. Какая из перечисленных мер позволяет защититься от перехвата данных в общедоступной сети?

- а) использование VPN
- б) отключение брандмауэра
- в) установка антивируса
- г) использование сложного пароля

26. Что такое «инцидент информационной безопасности»?

- а) любое событие, нарушающее нормальную работу системы
- б) событие, которое привело или могло привести к нарушению ИБ
- в) ошибка пользователя
- г) сбой электропитания

27. Кто несёт ответственность за обеспечение ИБ в организации?

- а) только IT-отдел
- б) руководитель организации
- в) служба безопасности
- г) все сотрудники в рамках своих обязанностей

28. Какой метод защиты используется для контроля съёмных носителей?
- а) DLP
 - б) IDS
 - в) VPN
 - г) SSL
29. Что такое «безопасность по умолчанию»?
- а) использование настроек, рекомендованных производителем
 - б) отключение всех служб
 - в) использование только бесплатного ПО
 - г) отсутствие паролей
30. Какая из перечисленных групп прав в NTFS является наивысшей?
- а) чтение
 - б) изменение
 - в) полный доступ
 - г) запись
31. Какой вид анализа позволяет выявить слабые места системы путём моделирования атаки?
- а) аудит
 - б) тестирование на проникновение
 - в) сканирование портов
 - г) резервное копирование
32. Что такое «согласие на обработку персональных данных»?
- а) устное разрешение субъекта
 - б) письменное (или электронное) добровольное волеизъявление
 - в) разрешение, данное один раз на все случаи
 - г) обязательное условие приёма на работу
33. Как часто должна пересматриваться политика ИБ?
- а) один раз в 10 лет
 - б) регулярно, но не реже одного раза в год, а также при изменениях
 - в) только при смене руководителя
 - г) никогда после утверждения
34. Что такое «antivirus»?
- а) программа для обнаружения и удаления вредоносного ПО
 - б) программа для шифрования файлов
 - в) программа для управления паролями
 - г) программа для резервного копирования
35. Какой протокол используется для защищённой передачи электронной почты?
- а) POP3

- б) IMAP
- в) S/MIME
- г) SMTP

36. Что означает аббревиатура SIEM?

- а) система управления инцидентами и событиями безопасности
- б) система защиты от утечек
- в) межсетевой экран
- г) протокол аутентификации

Критерии оценки:

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
90-100	5	отлично
76-89	4	хорошо
61-75	3	удовлетворительно
менее 60	2	неудовлетворительно

Темы рефератов, докладов, сообщений

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

1. Эволюция вредоносного программного обеспечения: от первых вирусов до современных угроз.
2. Сравнительный анализ симметричных и асимметричных криптосистем.
3. Правовое регулирование защиты персональных данных в РФ и за рубежом.
4. Методы и средства защиты от фишинговых атак.
5. Безопасность облачных вычислений: риски и способы их минимизации.
6. Роль DLP-систем в предотвращении утечек конфиденциальной информации.
7. Организация защищённого VPN-соединения: обзор технологий.
8. Социальная инженерия как один из основных методов кибератак.
9. Требования к политике паролей в современных организациях.
10. Анализ уязвимостей беспроводных сетей Wi-Fi.
11. Системы обнаружения и предотвращения вторжений (IDS/IPS): принципы работы.
12. Защита критической информационной инфраструктуры РФ.
13. Стандарты информационной безопасности серии ISO/IEC 27000.
14. Основы криптографии с открытым ключом: алгоритм RSA.
15. Психологические аспекты обеспечения информационной безопасности.
16. Тестирование на проникновение (пентест): методология и инструменты.
17. Информационная безопасность в банковской сфере.
18. Разработка и внедрение политики информационной безопасности в организации.
19. Защита информации при использовании мобильных устройств.
20. Управление инцидентами информационной безопасности: процессы и инструменты.
21. Анализ российских и зарубежных подходов к защите государственной тайны.
22. Современные методы аутентификации: от паролей до биометрии.
23. Информационная безопасность в эпоху Интернета вещей (IoT).
24. Организация безопасного удалённого доступа к корпоративным ресурсам.
25. Кибергигиена: правила безопасного поведения в сети для пользователей.
26. Применение блокчейн-технологий для обеспечения целостности данных.
27. Методики оценки рисков информационной безопасности.
28. Роль образования и повышения осведомлённости в снижении человеческого фактора.
29. Антивирусные решения: эволюция, современные технологии, сравнение.
30. Этические и правовые аспекты проведения пентестов.

Критерии оценки

Оценка «отлично» ставится, если выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично

изложено собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо» - основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются не точности в изложении материала; отсутствуют логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны не полные ответы.

Оценка «удовлетворительно» - имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.

Оценка «неудовлетворительно» - тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Варианты для выполнения контрольных работ

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

Вариант № 1

1. Раскройте понятие «информационная безопасность». Назовите три основные составляющие и приведите примеры нарушения каждой из них.
2. Каковы основные требования к паролям и их хранению? Опишите механизм хеширования.
3. Задача. Рассчитайте энтропию пароля `qwerty123` (латиница + цифры). Сравните с энтропией пароля `Tr#9kL!p`. Какой пароль надёжнее и почему?

Вариант № 2

1. Перечислите виды угроз информационной безопасности. Дайте краткую характеристику каждой группы.
2. Что такое криптографическая защита информации? В чём отличие симметричного шифрования от асимметричного?
3. Задача. Составьте матрицу прав доступа к папке `\\server\docs` для групп «Администраторы» (полный доступ), «Менеджеры» (чтение/запись), «Стажёры» (чтение). Запишите соответствующие разрешения NTFS.

Вариант № 3

1. Раскройте содержание Федерального закона «О персональных данных» № 152-ФЗ. Каковы обязанности оператора?
2. Какие существуют методы защиты от вредоносного программного обеспечения?
3. Задача. На рабочей станции обнаружены признаки заражения ransomware. Опишите пошаговые действия администратора.

Вариант № 4

1. Что такое социальная инженерия? Приведите примеры атак.
2. Опишите принцип работы межсетевого экрана. Какие типы фаерволов существуют?
3. Задача. Организация использует Wi-Fi с протоколом WPA2-Personal. Какие рекомендации по усилению безопасности вы можете дать?

Вариант № 5

1. Что такое VPN? Для каких целей используется? Назовите основные протоколы.
2. Понятие «управление доступом». Дискреционная, мандатная и ролевая модели.
3. Задача. Составьте расписание резервного копирования для сервера (данные 500 ГБ) по схеме: полное – раз в неделю, дифференциальное – ежедневно. Рассчитайте требуемый объём хранилища на месяц.

Вариант № 6

1. Понятие «электронная подпись». Области применения, принцип работы.
2. Какие мероприятия проводятся при управлении инцидентами ИБ?
3. Задача. Сотрудник сообщает, что получил письмо от «банка» с просьбой перейти по ссылке и подтвердить данные. Каковы правильные действия? Перечислите признаки фишинга.

Вариант № 7

1. DLP-системы: назначение, функции, архитектура.
2. Что такое IDS и IPS? В чём их отличие?
3. Задача. Настройте правила брандмауэра Windows, разрешающие удалённый доступ по RDP только для определённого IP-адреса.

Вариант № 8

1. Антивирусные средства: классификация, принципы работы.
2. Правовое регулирование защиты информации в РФ (149-ФЗ).
3. Задача. Проведите качественную оценку рисков для небольшого интернет-магазина, обрабатывающего данные банковских карт.

Вариант № 9

1. Основные стандарты информационной безопасности (ISO 27001, СТО БР ИББС).
2. Уязвимости программного обеспечения. Понятие CVE и CVSS.
3. Задача. Разработайте фрагмент политики паролей для организации (требования к длине, сложности, периодичности смены).

Вариант № 10

1. Классификация вредоносного ПО. Признаки заражения.
2. Организация безопасной работы в Интернете: протокол HTTPS, двухфакторная аутентификация.
3. Задача. Составьте план тестирования на проникновение для корпоративной сети (этапы, инструменты, ограничения).

Вариант № 11

1. Что такое «кибергигиена»? Перечислите основные правила для пользователей.
2. Защита информации в облачных сервисах. Модели ответственности.
3. Задача. Оцените стойкость пароля 'P@ssw0rd' с помощью онлайн-калькулятора (или расчётом). Предложите меры по усилению.

Вариант № 12

1. Биометрическая аутентификация: плюсы и минусы.
2. Организационно-распорядительные документы по ИБ.
3. Задача. Настройте правила доступа к Wi-Fi сети корпоративного уровня (WPA2-Enterprise) с использованием RADIUS-сервера.

Вариант № 13

1. Способы защиты электронной почты (шифрование, антиспам, проверка вложений).
2. Этические аспекты проведения пентестов.
3. Задача. После атаки злоумышленников были скомпрометированы учётные записи. Опишите процедуру смены паролей и восстановления.

Вариант № 14

1. Понятие «управление рисками ИБ». Этапы анализа рисков.
2. Защита информации при использовании съёмных носителей.
3. Задача. Рассчитайте энтропию пароля, генерируемого из случайного набора 12 символов (латиница, цифры, спецсимволы). Сделайте вывод.

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

Примеры ситуационных заданий

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

Задача 1. Сотрудник получил письмо якобы от системного администратора с просьбой сообщить свой пароль для «плановой проверки». Каковы должны быть действия сотрудника? Какие признаки указывают на попытку социальной инженерии? Составьте памятку для пользователей.

Задача 2. В компании используется парольная политика, разрешающая пароли длиной 6 символов (только буквы латиницы). Оцените энтропию такого пароля. Предложите новую политику, соответствующую современным стандартам.

Задача 3. Настройте права доступа к папке `\\server\files` для трёх групп: «Администраторы» – полный доступ, «Бухгалтерия» – чтение/запись, «Сотрудники» – только чтение. Опишите необходимые действия в Windows.

Задача 4. При проведении аудита выявлено, что в офисе используется Wi-Fi с протоколом WEP. Объясните, почему это опасно. Разработайте план перехода на защищённую сеть.

Задача 5. На рабочей станции обнаружены симптомы: замедление работы, появление неизвестных файлов, всплывающие окна с требованием выкупа. Опишите алгоритм действий администратора.

Задача 6. Необходимо организовать VPN для 10 удалённых сотрудников. Выберите протокол и обоснуйте выбор. Перечислите необходимое оборудование и настройки.

Задача 7. Компания планирует передать обработку персональных данных сторонней организации. Какие условия должны быть выполнены в соответствии с 152-ФЗ? Составьте проект договора (раздел об обязанностях).

Задача 8. Сотрудник случайно удалил важную папку с документами. Резервное копирование настроено: полное – раз в неделю, инкрементное – ежедневно. Восстановите документы, определив, из каких копий и в каком порядке нужно восстанавливать.

Задача 9. Настройте правила межсетевого экрана, разрешающие доступ к корпоративному веб-серверу из внутренней сети и запрещающие доступ к социальным сетям в рабочее время.

Задача 10. При проверке журналов безопасности обнаружены многочисленные неудачные попытки входа с одного IP-адреса. Какие действия необходимо предпринять? Предложите меры предотвращения подобных атак.

Задача 11. Составьте фрагмент политики информационной безопасности, регулирующий использование съёмных USB-накопителей.

Задача 12. Организация обрабатывает персональные данные клиентов. Какие документы должны быть разработаны для выполнения требований 152-ФЗ? Перечислите локальные акты.

Задача 13. Какие меры защиты необходимо применить при использовании общедоступного Wi-Fi в командировке для доступа к корпоративной почте? Обоснуйте.

Задача 14. Проведите качественную оценку рисков для небольшой компании, если известно, что на сервере хранится коммерческая тайна, а сотрудники не проходят обучение по ИБ.

Задача 15. Разработайте инструкцию по безопасному использованию электронной почты для сотрудников.

Критерии оценки:

Оценка «отлично» — работа выполнена в полном объёме с соблюдением необходимой последовательности, студент самостоятельно и рационально подготовил рабочее место и оборудование, все работы, измерения или исследования провёл в условиях, обеспечивающих получение правильных результатов и выводов, соблюдал требования техники безопасности.

Оценка «хорошо» — были выполнены требования к оценке «отлично», но студент допускал неточности.

Оценка «удовлетворительно» — результат выполненной работы был таков, что позволяет получить правильные выводы, но в ходе проведения работ, измерения или исследования были допущены ошибки, нарушались требования техники безопасности.

Оценка «неудовлетворительно» — практическая / лабораторная работа выполнена с серьёзными нарушениями техники безопасности, протокол не оформлен во время занятия или содержит грубые ошибки в оформлении и заключении, студент неправильно называет метод исследования, не может продемонстрировать методику исследования или оценить результат.

Вопросы для подготовки к дифференцированному зачету

ОК 01, ОК 02, ОК 04, ОК 09, ПК 1.7, ПК 2.5, ЛР 4, ЛР 6, ЛР 13, ЛР 14, ЛР 15, ЛР 16, ЛР 17, ЛР 18, ЛР 19

1. Понятие информационной безопасности, её цели и задачи.
2. Основные свойства информации: конфиденциальность, целостность, доступность.
3. Классификация угроз информационной безопасности.
4. Источники угроз: природные, техногенные, антропогенные.
5. Уязвимости информационных систем: примеры, способы выявления.
6. Организационная защита информации: политика ИБ, регламенты.
7. Правовые основы информационной безопасности в РФ (149-ФЗ, 152-ФЗ).
8. Федеральный закон «О персональных данных»: права субъекта, обязанности оператора.
9. Идентификация и аутентификация: методы, средства.
10. Парольная защита: требования к паролям, хранение, политики.
11. Двухфакторная и многофакторная аутентификация.
12. Модели управления доступом (дискреционная, мандатная, ролевая).
13. Межсетевые экраны: принципы, типы, правила фильтрации.
14. Виртуальные частные сети (VPN): протоколы, сценарии использования.
15. Защита беспроводных сетей: WEP, WPA, WPA2, WPA3.
16. Вредоносное программное обеспечение: классификация, признаки заражения.
17. Антивирусные средства: типы, принципы работы, обзор решений.
18. Социальная инженерия: методы и способы противодействия.
19. Фишинг: виды, распознавание, защита.
20. Криптография: симметричное и асимметричное шифрование.
21. Электронная подпись: сущность, алгоритмы, применение.
22. Хэш-функции: свойства, примеры использования.
23. Системы обнаружения и предотвращения вторжений (IDS/IPS).
24. DLP-системы: назначение, функции, примеры.
25. Резервное копирование и восстановление данных как элемент ИБ.
26. Управление инцидентами информационной безопасности.
27. Тестирование на проникновение (пентест): этапы, методологии.
28. Аудит информационной безопасности: цели, процедуры.
29. Анализ рисков: качественный и количественный подходы.
30. Стандарты ИБ: ISO/IEC 27001, СТО БР ИББС, ГОСТ.
31. Защита информации в операционных системах (Windows, Linux).
32. Защита информации в базах данных.
33. Безопасность облачных вычислений: риски, меры защиты.
34. Кибергигиена: основные правила для пользователей.
35. Защита от утечек через внешние устройства и каналы связи.
36. Организация безопасного удалённого доступа.
37. Защита информации при использовании мобильных устройств.
38. Понятие об уязвимостях нулевого дня (0-day).

39. Инструменты криптографической защиты: сертификаты, токены.
40. Этические и правовые аспекты информационной безопасности.

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

IV. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Оценка результатов освоения дисциплины ОП. 06 «Основы информационной безопасности» осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, исследований.

Результаты обучения	Критерии оценки	Методы оценки
<p>Освоенные знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства психологические основы деятельности коллектива; психологические особенности личности правила построения простых и сложных предложений на профессиональные темы; основные общепотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности Основы ИБ организации; Модель угроз информационной безопасности ИС организации заказчика; Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика; Основы администрирования СУБД; Основы системного администрирования; Коммуникационное оборудование; Сетевые протоколы; Основы современных операционных систем; Устройство и функционирование современных ИС; Основы архитектуры мультитрендного программного обеспечения Понятие и классификация инцидентов ИБ; Типичные угрозы ИБ при работе с БД; Процедуры и регламенты передачи информации об инцидентах в службу ИБ организации; Средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры); Основы работы со средствами антивирусной защиты; Основы ИБ; Основы деловой этики; Правила деловой переписки</p> <p>Освоенные умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять ее составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска;</p>	<p>Оценка «отлично» означает, что теоретическое содержание дисциплины освоено полностью, сформированы необходимые практические навыки и умения, выполнены все учебные задания, студент может обосновать свои суждения, привести необходимые примеры.</p> <p>Оценка «хорошо» означает, что теоретическое содержание дисциплины освоено полностью, сформированы необходимые практические навыки и умения не в полном объеме, выполнены все учебные задания, при выполнении которых были обнаружены ошибки и недочеты, присутствуют незначительные недочёты в последовательности и языковом оформлении излагаемого.</p> <p>Оценка «удовлетворительно» означает, что теоретическое содержание дисциплины освоено частично, но пробелы не носят существенного характера, сформированы в основном необходимые практические навыки и умения, выполнено большинство учебных заданий, при выполнении которых были обнаружены ошибки и недочеты, студент не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.</p> <p>Оценка «Неудовлетворительно» означает, что теоретическое содержание дисциплины не освоено, не сформированы необходимые практические навыки и умения, выполненные учебные задания содержат ошибки и недочеты, студент допускает ошибки в</p>	<p>Текущий контроль:</p> <ul style="list-style-type: none"> – устный и письменный опрос; – выполнения тестовых заданий; – подготовка рефератов, докладов, сообщений – выполнение заданий контрольных работ – выполнение ситуационных заданий; <p>Промежуточная аттестация – дифференцированный зачет</p>

<p>оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС обеспечения Идентифицировать инциденты ИБ при работе с БД; Осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации); Управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ; Устанавливать и сопровождать антивирусное ПО</p> <p><u>Практические навыки:</u> Распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Передачи информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Информирования заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Временного блокирования доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС Распознавания инцидентов ИБ при работе с БД; Формирования перечня инцидентов ИБ; Передачи информации об инцидентах в службу ИБ организации; Временного блокирования доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости); Поддержания баз антивирусных программ в актуальном состоянии</p>	<p>формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.</p>	
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------	--

Преподаватель



Винокуров И.В.