МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00854147D9DB094CC9BCA23534D24EC1A8
Владелец: Василенко Виталий Николаевич
Действителен: с 26.09.2023 до 19.12.2024

УТВЕРЖДАЮ
И. о. проректора по учебной работе

_____ Василенко В. Н.
(подпись) (Ф.И.О.)

«30» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
(наименование в соответствии с РУП)

Направление подготовки (специальность)

38.05.01 Экономическая безопасность
(шифр и наименование направления подготовки/специальности)

Направленность (профиль)

Экономико-правовое обеспечение экономической безопасности
(наименование профиля/специализации)

Квалификация выпускника

экономист

(в соответствии с Приказом Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями)

1. Цели и задачи дисциплины

Целью освоения дисциплины является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

08 Финансы и экономика (в сферах: обеспечения экономической безопасности региона; обеспечения экономической безопасности хозяйствующих субъектов).

Дисциплина направлена на решение типов задач профессиональной деятельности: расчетно-экономический, информационно-аналитический, организационно-управленческий, контрольный, научно-исследовательский.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 38.05.01 Экономическая безопасность.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-7.	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	$ИД2_{ОПК-7}$ Применяет принципы работы современных информационных технологий и использует их для решения задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
$ИД2_{ОПК-7}$ Применяет принципы работы современных информационных технологий и использует их для решения задач профессиональной деятельности	**Знать** основные направления обеспечения цифровой безопасности, принципы работы современных информационных технологий, методы и средства защиты информации.
	Уметь выявлять угрозы информационным системам и ресурсам, применять современные информационные технологии для защиты информации
	Владеть навыками защиты информации в соответствующих сферах профессиональной деятельности

3. Место дисциплины в структуре ООП ВО

Дисциплина относится к обязательной части Блока 1 ООП. Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин и практик: Информатика, Информационные системы в экономике, Система обеспечения экономической безопасности хозяйствующего субъекта, Экономическая безопасность.

Дисциплина является предшествующей для обучающимися дисциплин и практик: преддипломная практика.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5 зачетных единицы

Виды учебной работы	Всего акад. часов	Семестр
		А
Общая трудоемкость дисциплины	108	108
Контактная работа в т.ч. аудиторные занятия:	**53,4**	**53,4**
Лекции	26	26
Практические занятия (ПЗ)	26	26

Консультации текущие	1,3	1,3
Вид аттестации (зачет)	**0,1**	**0,1**
Самостоятельная работа:	**54,6**	**54,6**
Проработка материалов по лекциям, учебникам, учебным пособиям	29	29
Подготовка к практическим занятиям	15,6	15,6
Домашняя контрольная работа	10	10

5. Содержание дисциплины, структурированное по разделам с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, ак.ч
1	Цифровая безопасность и защита информации: основные понятия и определения	Понятие цифровой безопасности и ее место в системе национальной безопасности. Информация как объект правовой защиты. Современные информационные технологии защиты информации. Государственная система обеспечения цифровой безопасности РФ.	25,1
2	Обеспечение безопасности персональных данных	Российское и международное законодательство в области персональных данных. Порядок и основные этапы работ по обработке персональных данных в организации. Определение уровня защищенности персональных данных. Основы построения системы защиты персональных данных.	40,3
3	Комплексная система обеспечения защиты информации в организации	Объекты защиты. Современные угрозы цифровой безопасности. Система управления защитой информации в современной организации. Защита информации от утечки по техническим каналам. Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи. Защита информации ограниченного доступа с использованием шифровальных (криптографических) средств.	41,2
	Консультации текущие		1,3
	Зачет		0,1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	ПЗ, ак. ч	СРО, ак. ч
1.	Цифровая безопасность и защита информации: основные понятия и определения	6	6	13,1
2	Обеспечение безопасности персональных данных	8	8	24,3
3	Комплексная система обеспечения защиты информации в организации	12	12	17,2
	Консультации текущие	1,3		
	Зачет	0,1		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Цифровая безопасность и защита информации: основные понятия и определения	Понятие цифровой безопасности и ее место в системе национальной безопасности. Информация как объект правовой защиты. Современные информационные технологии защиты информации.	2
		Государственная система обеспечения цифровой безопасности РФ.	4
2	Обеспечение безопасности персональных данных	Российское и международное законодательство в области персональных данных.	2

		Порядок и основные этапы работ по обработке персональных данных в организации. Определение уровня защищенности персональных данных	4
		Основы построения системы защиты персональных данных.	2
3	Комплексная система обеспечения защиты информации в организации	Объекты защиты. Современные угрозы цифровой безопасности.	2
		Система управления защитой информации в современной организации.	2
		Защита информации от утечки по техническим каналам	2
		Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи	2
		Защита информации ограниченного доступа с использованием шифровальных (криптографических) средств.	4

5.2.2 Практические занятия (ПЗ)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак. ч
1	Цифровая безопасность и защита информации: основные понятия и определения	Понятие цифровой безопасности и ее место в системе национальной безопасности. Информация как объект правовой защиты. Современные информационные технологии защиты информации.	2
		Государственная система обеспечения цифровой безопасности РФ.	4
2	Обеспечение безопасности персональных данных	Российское и международное законодательство в области персональных данных.	2
		Порядок и основные этапы работ по обработке персональных данных в организации. Определение уровня защищенности персональных данных	4
		Основы построения системы защиты персональных данных.	2
3	Комплексная система обеспечения защиты информации в организации	Объекты защиты. Современные угрозы цифровой безопасности.	2
		Система управления защитой информации в современной организации.	2
		Защита информации от утечки по техническим каналам	2
		Организационно-технические и правовые основы использования в информационных системах электронного документооборота и электронной подписи	2
		Защита информации ограниченного доступа с использованием шифровальных (криптографических) средств.	4

5.2.3 Лабораторный практикум - не предусмотрен

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Цифровая безопасность и защита информации: основные понятия и определения	Проработка материалов по лекциям, учебникам, учебным пособиям	9,5
		Подготовка к практическим занятиям	3,6
2	Обеспечение безопасности персональ-	Проработка материалов по лекциям, учебникам, учебным пособиям	9,5

	ных данных	Подготовка к практическим занятиям	4,8
		Домашняя контрольная работа	10
3	Комплексная система обеспечения защиты информации в организации	Проработка материалов по лекциям, учебникам, учебным пособиям	10
		Подготовка к практическим занятиям	7,2

6 Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

1.Суворова, Г. М. Информационная безопасность : учебное пособие для вузов (гриф УМО ВО) / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. https://urait.ru/bcode/544029

2.Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. https://e.lanbook.com/book/130184

6.2 Дополнительная литература

1.Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 124 с. https://e.lanbook.com/book/169817

2.Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. https://e.lanbook.com/book/176563

3.Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. https://e.lanbook.com/book/370967

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Цифровая безопасность и защита информации: методические указания и задания для самостоятельной работы для обучающихся по специальности 38.05.01 - «Экономическая безопасность», очной и заочной формы обучения / Л. Н. Чайковская - Воронеж : ВГУИТ, 2022 http:// education.vsuet.ru

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Научная электронная библиотека	*http://www.elibrary.ru/defaulttx.asp?*
Образовательная платформа «Юрайт»	*https://urait.ru/*
ЭБС «Лань»	*https://e.lanbook.com/*
АИБС «МегаПро»	*https://biblos.vsuet.ru/MegaPro/Web*
Сайт Министерства науки и высшего образования РФ	*http://minobrnauki.gow.ru*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ	*http://education.vsuet.ru*
Портал открытого on-line образования	*https://npoed.ru/*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение, современные профессиональные базы данных и информационные справочные системы: ЭИОС уни-

верситета, в том числе на базе программной платформы «Среда электронного обучения 3KL».

При освоении дисциплины используется лицензионное и открытое программное обеспечение – ОС Windows, ОС ALT Linux.

7 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения лекционных и практических занятий, оснащенные оборудованием и техническими средствами обучения (мультимедийными проекторами, настенными экранами, интерактивными досками, ноутбуками, досками, рабочими местами по количеству обучающихся, рабочим местом преподавателя) – ауд. 9, 450, 239, 244, 245, 341а или иные в соответствии с расписанием.

Допускается использование других аудиторий в соответствии с расписанием учебных занятий и оснащенных соответствующим материально-техническим обеспечением, в соответствии с требованиями, предъявляемыми образовательным стандартом.

Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к базам данных и электронной информационно-образовательной среде ФГБОУ ВО «ВГУИТ» – ауд. 251, ресурсный центр ВГУИТ.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Оценочные материалы (ОМ) для дисциплины включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и входят в состав рабочей программы дисциплины.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Приложение
к рабочей программе
Цифровая безопасность и защита информации

1. Организационно-методические данные дисциплины для заочной формы обучения

1.1 Объемы различных форм учебной работы и виды контроля в соответствии с учебным планом

Общая трудоемкость дисциплины составляет 3 зачетных единицы.

Виды учебной работы	Всего акад. часов	6 курс зимняя сессия
Общая трудоемкость дисциплины	108	108
Контактная работа в т.ч. аудиторные занятия:	**9,5**	**9,5**
Лекции	4	4
Практические занятия	4	4
Консультации текущие	0,6	0,6
Консультации по контрольной работе	0,8	0,8
Вид аттестации (зачет)	0,1	0,1
Самостоятельная работа:	**94,6**	**94,6**
Проработка материалов по лекциям, учебникам, учебным пособиям	**47**	**47**
Подготовка к практическим/лабораторным занятиям	**32,6**	**32,6**
Контрольная работа	15	15
Контроль (выполнение контрольной работы, зачет)	**3,9**	**3,9**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

ЦИФРОВАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	**ОПК-7**	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	**ИД2$_{ОПК-7}$** Применяет принципы работы современных информационных технологий и использует их для решения задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2$_{ОПК-7}$ Применяет принципы работы современных информационных технологий и использует их для решения задач профессиональной деятельности	**Знает:** основные направления обеспечения цифровой безопасности, принципы работы современных информационных технологий, методы и средства защиты информации.
	Умеет: выявлять угрозы информационным системам и ресурсам, применять современные информационные технологии для защиты информации
	Владеет: навыками защиты информации в соответствующих сферах профессиональной деятельности

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Цифровая безопасность и защита информации: основные понятия и определения	ОПК-7	Банк тестовых заданий	1-5,10,16-19, 26,28,30-31,33, 35-37, 45-46	Компьютерное тестирование (процентная шкала)
			Собеседование (вопросы для зачета)	51-54	Проверка преподавателем (оценка в системе «зачтено-не зачтено»)
			Задания для практических занятий		Проверка преподавателем (уровневая шкала)
2	Обеспечение безопасности персональных данных	ОПК-7	Банк тестовых заданий	6-9, 20-23,27,29,32,38-40, 48-50	Компьютерное тестирование (процентная шкала)
			Собеседование (вопросы для зачета)	55-57	Проверка преподавателем (оценка в системе «зачтено-не зачтено»)
			Задания для практических занятий		Проверка преподавателем (уровневая шкала)
			Задание для домашней контрольной работы		Проверка преподавателем (уровневая шкала)
3	Комплексная система обеспечения защиты инфор-	ОПК-7	Банк тестовых заданий	11-15, 24-25,34,41-44, 47	Компьютерное тестирование (процентная шкала)

	мации в организации		Собеседование (вопросы для зачета)	58-60	Проверка преподавателем (оценка в системе «зачтено-не зачтено»)
			Задания для практических занятий		Проверка преподавателем (уровневая шкала)

3 Оценочные материалы для промежуточной аттестации
Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Аттестация обучающегося по дисциплине проводится в форме тестирования и предусматривает возможность последующего собеседования (зачета, экзамена).

3.1 Банк тестовых заданий

ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

№ задания	Тестовое задание
	Выбор одного правильного ответа из предложенных вариантов ответов
1.	Защита информации от утечки это деятельность по предотвращению: 1) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; 2) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; 3) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; **4) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа.**
2.	Как называется попытка реализации угрозы информационной безопасности? **1) атака** 2) угроза 3) уязвимость 4) слабое место системы
3.	По уровню в информационной инфраструктуре наиболее распространенными являются средства анализа защищенности 1) на уровне приложений 2) на уровне СУБД **3) на уровне сети** 4) на уровне ОС
4.	Какой федеральный закон является базовым в Российском законодательстве в области информационных отношений и информационной безопасности? 1) о персональных данных 2) о техническом регулировании **3) об информации, информационных технологиях и о защите информации** 4) о лицензировании отдельных видов деятельности
5.	К средствам, позволяющим оценить защищенность сети в целом, относятся: **1) средства обнаружения и противодействия атакам** 2) программы, занимающиеся сбором данных 3) средства обнаружения уязвимостей 4) средства на отслеживание приложений, внесенных в их базы данных
6.	Персональные данные это: **1) любая информация, относящаяся к определенному, или определяемому на основании такой информации физическому лицу.** 2) сведения (сообщения, данные) независимо от формы их представления. 3) любая информация, касающаяся физиологических особенностей человека.

	4) информация, позволяющая связаться с человеком любым доступным способом.
7.	Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных? 1) субъект персональных данных 2) оператор информационной системы 3) регулятор **4) оператор персональных данных**
8.	Как называются органы, государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований ФЗ “О персональных данных”? 1) операторы **2) регуляторы** 3) контролеры 4) надзорные органы
9.	Основополагающим федеральным законом в области обеспечения безопасности персональных данных является: **1) о персональных данных** 2) об информации, информационных технологиях и о защите информации 3) о лицензировании отдельных видов деятельности 4) о безопасности
10.	Активный перехват информации это перехват, который: 1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; 2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; 3) осуществляется путем использования оптической техники; **4) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.**
11.	Криптография не обеспечивает: 1) скрытность передачи информации **2) шифрование для защиты от несанкционированного доступа** 3) конфиденциальность и аутентичность информации 4) все ответы верны
12.	Алгоритм шифрования, основанный на сложении символов исходного текста с символами некоторой случайной последовательности, называется 1) алгоритмом перестановки **2) алгоритмом гаммирования** 3) алгоритмом подстановки 4) алгоритмом простой замены
13.	Какая из 3-х видов электронной подписи создается без использования криптографии? **1) простая электронная подпись (ЭП)** 2) усиленной неквалифицированной электронная подпись (УЭП) 3) усиленной квалифицированной электронная подпись (УКЭП)
14.	Алгоритм шифрования, основанный на изменении мест шифруемого текста по определенному принципу, является: **1) алгоритмом перестановки** 2) алгоритмом гаммирования 3) алгоритмом подстановки 4) алгоритмом простой замены
15.	Какая из 3-х видов электронной подписи не позволяет установить искажение информации в ЭД после его подписи? **1) простая электронная подпись (ЭП)** 2) усиленной неквалифицированной электронная подпись (УЭП) 3) усиленной квалифицированной электронная подпись (УКЭП)
	Выбор нескольких правильных ответов из предложенных вариантов ответов
16.	Приведите степени секретности сведений, составляющих государственную тайну: **1) особой важности** 2) ограниченный доступ **3) совершенно секретно** **4) секретно**
17.	Основными органами сертификации в области технической защиты информации являются: 1) МВД России

<table>
<tr><td></td><td>2) Роскомнадзор
3) ФСТЭК России
4) ФСБ России</td></tr>
<tr><td>18.</td><td>ФЗ "Об информации, информационных технологиях и о защите информации” регулирует отношения, возникающие при:
1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий
3) обеспечении защиты информации
4) правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации</td></tr>
<tr><td>19.</td><td>Национальными интересами РФ, согласно Доктрине информационной безопасности Российской Федерации, являются:
1) все ответы верны
2) развитие информационных технологий и электронной промышленности
3) защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации
4) борьба с распространением информации о способах разработки, изготовления и использования наркотических средств, психотропных веществ</td></tr>
<tr><td>20.</td><td>Какие категории персональных данных выделяет ФЗ “О персональных данных”?
1) личные
2) общедоступные
3) физиологические
4) специальные
5) биометрические</td></tr>
<tr><td>21.</td><td>Что в праве требовать субъект персональных данных от оператора?
1) правовые основания и цели обработки
2) сроки обработки и сроки хранения
3) применяемые способы обработки
4) видеозаписи обработки данных</td></tr>
<tr><td>22.</td><td>Федеральный закон "Об электронной подписи" устанавливает следующие принципы использования ЭЦП:
1) право использовать любую технологию связи для передачи ЭЦП
2) недопустимость признания ЭЦП и документа недействительными только на основании того, что отсутствует собственноручная подпись
3) ежедневный контроль корректности ключа
4) право использовать ЭЦП любого вида</td></tr>
<tr><td>23.</td><td>Что относится к сведениям конфиденциального характера?
1) коммерческая тайна
2) государственная тайна
3) нотариальная тайна
4) врачебная тайна</td></tr>
<tr><td>24.</td><td>На сегодняшний день асимметричная криптография основывается:
1) на дискретном логарифмировании
2) на целочисленной факторизации
3) на эллиптических кривых
4) на задаче о рюкзаке</td></tr>
<tr><td>25.</td><td>К алгоритмам симметричного шифрования относится:
1) шифр Виженера
2) шифр Тритемиуса
3) алгоритм RSA
4) шифр Цезаря</td></tr>
<tr><td></td><td>Установление соответствия между двумя множествами вариантов ответов</td></tr>
<tr><td>26.</td><td>
<table>
<tr><td>Конфиденциальность</td><td>состояние защищенности информации и активов от модификации, подмены, уничтожения неправомочным способом</td></tr>
<tr><td>Целостность</td><td>состояние информационной технологии, обеспечивающее своевременный и надежный доступ к информации и (или) функциональным возможностям информационной технологии правомочным образом</td></tr>
<tr><td>Доступность</td><td>состояние защищенности информации ограниченного доступа от неправомочного раскрытия</td></tr>
</table>
Ответ
<table>
<tr><td>Конфиденциальность</td><td>состояние защищенности информации ограниченного доступа от не-</td></tr>
</table>
</td></tr>
</table>

		правомочного раскрытия.
	Целостность	состояние защищенности информации и активов от модификации, подмены, уничтожения неправомочным способом.
	Доступность	состояние информационной технологии, обеспечивающее своевременный и надежный доступ к информации и (или) функциональным возможностям информационной технологии правомочным образом.
27.	Обработка персональных данных	действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
	Распространение персональных данных	действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.
	Использование персональных данных	действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
	Обезличивание персональных данных	действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
	Ответ	
	Обработка персональных данных	действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
	Распространение персональных данных	действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
	Использование персональных данных	действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.
	Обезличивание персональных данных	действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
	Установление правильной последовательности в предложенных вариантах ответов	
28.	Установите правильную последовательность действий: Авторизация идентификация Аутентификация **Ответ: идентификация, аутентификация, авторизация**	
29.	Какая иерархия существует в подчиненности нормативно-правовых актов? Указы президента Конституция Федеральные законы Ведомственные акты **Ответ: Конституция, федеральные законы, указы президента, ведомственные акты**	
	Вставить пропущенное слово	
30.	_____ тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Вписать слово в предложение в нужном падеже с маленькой буквы **Ответ: государственная**	
31.	_____доступ к информации — доступ к информации, нарушающий правила раз-	

	граничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Вписать слово в предложение в нужном падеже с маленькой буквы **Ответ: несанкционированный**
32.	Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных называется _____ персональных данных. Вписать слово в предложение в нужном падеже с маленькой буквы **Ответ: обезличиванием**
33.	_____ - гарантирует, что данные не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей. Вписать слова в предложение в нужном падеже с маленькой буквы **Ответ: целостность данных**
34.	_____ — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Вписать слова в предложение в нужном падеже с маленькой буквы **Ответ: электронная цифровая подпись**
	Решить задачи
35.	Законно ли требование-запрос судебного пристава-исполнителя о представлении сведений о месте работы должников, если данный документ поступил в организацию посредством факсимильной связи (его подлинник не получен)? **Ответ** В законодательных актах РФ отсутствует упоминание о возможности официально направлять постановления, запросы и иные документы посредством факсимильной связи. Это распространяется и на взаимодействие с органами ФССП. Поэтому исполнение обращений, направленных по факсу, может оставаться на усмотрение организации. Никаких штрафных санкций за неисполнение факсимильного запроса не предусмотрено.
36.	Уволенный работник разгласил информацию, составляющую коммерческую тайну и ставшую ему известной в связи с исполнением трудовых обязанностей у бывшего работодателя. Вправе ли организация взыскать с уволенного работника убытки, причиненные разглашением информации? **Ответ:** Организация-работодатель вправе взыскать с уволенного работника убытки, причиненные разглашением информации, составляющей коммерческую тайну, если такая информация стала известна работнику в связи с исполнением трудовых обязанностей. Обоснование: Действующее трудовое законодательство позволяет работодателю обязать работника не разглашать сведения, составляющие коммерческую тайну, включив соответствующее условие в трудовой договор (ст. 57 Трудового кодекса РФ).
37.	ФАС России затребовал у Банка информацию о движении денежных средств по счетам, открытым в банке организацией, в отношении которой ФАС России проводится проверка по вопросу соблюдения законодательства о защите конкуренции. Обязан ли Банк предоставить указанную информацию по требованию ФАС России? и если не обязан, но не предоставит может ли Банк быть привлечен к административной ответственности?». **Ответ** : Банк обязан предоставить антимонопольному органу информацию, содержащуюся в запросе. За не предоставления информации по запросу антимонопольного органа, Банк может быть привлечен к административной ответственности по части 5 статьи 19.8 КОАП РФ. Санкция за данное правонарушение предусматривает административную ответственность для юридических лиц в виде штрафа от пятидесяти тысяч до пятисот тысяч рублей.
38.	Вы обратились в удостоверяющий центр для создания своей электронной цифровой подписи. Будет ли действителен ваш сертификат ключа подписи, если он содержит следующие сведения: • вашу фамилию, имя и отчество; • даты начала и окончания срока действия сертификата ключа подписи; • название и место нахождения удостоверяющего центра; • открытый ключ ЭЦП? **Ответ** В данном случае сертификат ключа подписи будет недействителен, так как на основании ст. 6, п. 1 закона «Об электронной цифровой подписи» в данном сертификате отсутствуют сведения об уникальном регистрационном номере, средствах ЭЦП, а также отношениях, при которых электронный документ с ЭЦП будет иметь юридическое значение.
39.	Определите, будет ли электронная подпись равнозначной собственноручной подписи, если подтверждена подлинность электронной цифровой подписи в электронном документе. **Ответ**

	Электронная подпись не будет равнозначной собственноручной подписи только лишь при подтверждении подлинности электронной цифровой подписи в электронном документе, так как на основании ст. 4, п. 1 закона «Об электронной цифровой подписи» этого условия недостаточно.
40.	Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем сертификата ключа подписи И. О. Симоновой судебного иска к удостоверяющему центру, если представители последнего не сообщили ей об аннулировании сертификата ключа подписи до истечения срока его действия? **Ответ** В данной ситуации суд вынесет решение в пользу владельца сертификата ключа подписи И. О. Симоновой, так как на основании ст. 14, п. 2 закона «Об электронной цифровой подписи» налицо нарушение обязательств сотрудниками удостоверяющего центра.
41.	В организации во исполнение норм ст. 22.1 Закона «О персональных данных» приказом генерального директора назначается ответственный за организацию обработки персональных данных. Какие изменения и дополнения необходимо внести в должностную инструкцию работника, ответственного за указанную часть работы в организации? **Ответ** В обязанности ответственного в организации за организацию обработки персональных данных согласно закону входит: - осуществление контроля над соблюдением оператором и сотрудниками организации законодательства о персональных данных и требований к их защите; - доведение до сведения работников организации положений законодательства и иных актов (например, локальных актов учреждения), регламентирующих процессы обработки персональных данных, и требований к их защите; - организация приема и обработки обращений и запросов субъектов персональных данных (работников организации и контрагентов) и осуществление контроля над их приемом и обработкой. Ответственный сотрудник получает указания непосредственно от генерального директора организации и подотчетен только ему (ч. 2 ст. 22.1 Закона «О персональных данных»). Соответствующие изменения и дополнения вносятся в должностную инструкцию работника, ответственного за указанную часть работы в организации.
42.	Согласно законодательству, обработка специальных категорий персональных данных должна осуществляться с письменного согласия субъекта персональных данных (ст. 6, 9, 10 Закона «О персональных данных», ч. 3 ст. 13 Закона № 323-ФЗ). Укажите состав сведений, которые указываются в согласии сотрудника организации на обработку его персональных данных. **Ответ** Состав сведений, указываемых в согласии сотрудника организации на обработку его персональных данных, перечислен в ст. 9 Закона «О персональных данных»: - фамилия, имя, отчество, адрес сотрудника; реквизиты документа, удостоверяющего его личность; - наименование и адрес оператора, получающего согласие; - цель обработки персональных данных; - перечень персональных данных, на обработку которых дается согласие сотрудника; - наименование и адрес лица, осуществляющего обработку персональных данных по поручению оператора; - перечень действий с персональными данными, описание способов обработки; - срок, в течение которого действует согласие, способ его отзыва; - подпись сотрудника.
43.	Согласие субъекта на обработку персональных данных должно содержать подпись субъекта персональных данных. Как быть в тех случаях, когда персональные данные предоставляются оператором через телекоммуникационные сети Интернет и личной встречи между оператором и субъектом не происходит? Достаточно ли в этом случае выражения согласия субъекта персональных данных на обработку его данных путем проставления отметки в согласии в электронном виде (например, при предоставлении по электронной почте анкет соискателей на вакансии работодателей, предоставление данных организатору конкурса, проводимого в Интернет)? **Ответ** При наличии требования федерального закона об обязательном получении в конкретных случаях письменного согласия, документ должен быть подписан либо на бумажном носителе, либо в электронной форме (посредством электронной подписи как аналога собственноручной). Закон «О персональных данных» регламентирует, что согласие на обработку персональных данных может быть дано гражданином или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае, если наличие письменного согласия в силу закона не обязательно, гражданин может выразить свое согласие на обработку персональных данных любым способом, в частности проставлением отметки в электронном виде. При этом необходимо помнить, что обязанность предоставить доказательство получения согласия субъекта персональных данных возлагается на оператора.
44.	В организацию поступил телефонный звонок от сотрудника банка с целью проверки, работает ли в организации гражданин И. Сотрудником отдела кадров была предоставлена исчерпывающая информация о работнике И. с указанием паспортных данных, ИНН и пр. Является ли это нарушением законодательства о защите ПД работника? Может ли организация отказать звонящему в предоставлении сведений о работнике?

	Ответ Да, является. Нормами ст. 88 ТК РФ установлено, что работодатель не вправе сообщать ПД третьей стороне без письменного согласия их субъекта. В случае отсутствия письменного согласия работника работодатель обязан отказать в их предоставлении.
	Выполнить ситуационное задание
45.	Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата — с целью продажи этой информации конкурирующей организации. **Ответ** Действия лиц в данной ситуации квалифицируются как противоправные на основании ст. 272, п. 2 УК РФ, так как очевиден неправомерный доступ к компьютерной информации группы лиц по предварительному сговору.
46.	Сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей. **Ответ** Действия сотрудника в данной ситуации квалифицируются как противоправные на основании ст. 273, п. 2 УК РФ, так как налицо распространение вредоносных программ для ЭВМ, которое привело к тяжким последствиям.
47.	Согласно 63-ФЗ сертификат ЭП должен храниться у ФЛ, который его получал. При наличии подозрений, что ключ используется 3-ми лицами, владельцу ЭП нужно обратиться в УЦ, выпустивший ключ, для его аннулирования. Однако, сам ключ делится на 2 части: закрытая и открытая. В 63-ФЗ также сказано, что УЦ обязан удостоверить личность будущего владельца ЭП. Может ли УЦ предоставить открытую часть ключа 3-му лицу без его идентификации? **Ответ** «Закрытый ключ», «открытый ключ» — это терминология Закона об электронной цифровой подписи, который действовал до Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (Закон № 63-ФЗ). В новом законе указанным терминам соответствует «ключ электронной подписи (ЭП)» и «ключ проверки ЭП», с их определениями Вы можете ознакомиться в Законе № 63-ФЗ. Сертификат, в который входит ключ проверки ЭП — это не конфиденциальная информация, он может храниться не только у владельца сертификата, и должен представляться контрагенту подписанта, чтобы он смог проверить действительность ЭП, с помощью которой подписан электронный документ. А вот ключ ЭП должен храниться только у его владельца. При его компрометации сертификат должен быть незамедлительно аннулирован (аннулируется сертификат, а не ключ). Кроме того, УЦ обязан предоставлять пользователям любой выпущенный таким УЦ сертификат (п. 3 ч. 2 ст. 13 Закона № 63-ФЗ).
48.	Вправе ли должностное лицо, в производстве которого находится дело об административном правонарушении, запрашивать у руководства организации персональные данные их работников? **Ответ** В соответствии со статьей 28.3 КоАП РФ протоколы об административных правонарушениях составляются должностными лицами органов, уполномоченных рассматривать дела об административных правонарушениях в пределах компетенции соответствующего органа. Требования к содержанию протокола об административном правонарушении установлены статьей 28.2 КоАП РФ. В частности, в протоколе об административном правонарушении указываются сведения о лице, в отношении которого возбуждено дело об административном правонарушении. Кроме того, статьей 26.10 КоАП РФ предусмотрено, что орган, должностное лицо, в производстве которых находится дело об административном правонарушении, вправе вынести определение об истребовании сведений, необходимых для разрешения дела. Истребуемые сведения должны быть направлены в трехдневный срок со дня получения определения в порядке, предусмотренном ст.26.10 КоАП РФ. При невозможности представления указанных сведений организация обязана в трехдневный срок уведомить об этом в письменной форме судью, орган, должностное лицо, вынесших определение. Пунктом 1 части 2 статьи 6 Закона «О персональных данных» предусмотрена обработка персональных данных на основании Федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора без согласия субъекта персональных данных. Таким образом, должностное лицо органа, уполномоченного составлять и рассматривать протоколы об административном правонарушении вправе в рамках производства по делу об административном правонарушении запрашивать у организаций персональные данные их работников, в отношении которых возбуждено дело об административном правонарушении.
49.	Родственники пациента М. обратились к главному врачу больницы с жалобой на нарушение прав

	пациента при обработке его персональных данных. В жалобе указывалось, что пациент М. при поступлении в больницу не давал письменного согласия на обработку персональных данных. При разборе жалобы выяснилось, что больной М. поступил в больницу по скорой помощи в состоянии сопора с открытой черепно-мозговой травмой и множественными переломами костей нижних конечностей. Больной госпитализирован в реанимационное отделение, перенёс несколько операций, находился в состоянии искусственной комы. Больной переведен в нейрохирургическое отделение. Обоснована ли жалоба родственников пациента? **Ответ** Нет, не обоснована. Согласие пациента на обработку ПД не требуется в следующих случаях: - медицинская помощь оказывается по программе обязательного медицинского страхования (ОМС), и персональные данные передаются только в территориальный фонд ОМС и страховую организацию (ст. 38, 39, 43, 44 и 48 Федерального закона № 326-ФЗ); - персональные данные пациента о состоянии его здоровья передаются третьим лицам (ч. 4 ст. 13 Закона № 323-ФЗ): - если пациент в результате своего состояния не способен выразить свою волю, но ему необходимо лечение; - при угрозе распространения инфекционных заболеваний, массовых отравлений; 93 - по запросу органов дознания и следствия, суда, органа уголовноисполнительной системы; - в случае оказания медицинской помощи несовершеннолетнему; - в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются основания полагать, что вред его здоровью причинен в результате противоправных действий; - в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов; - в целях расследования несчастного случая на производстве и профессионального заболевания; - при обмене информацией медицинскими организациями, в т. ч. размещенной в информационных системах, в целях оказания медицинской помощи; - в целях осуществления учета и контроля в системе обязательного социального страхования; - в целях осуществления контроля качества и безопасности медицинской помощи.
50.	В детской городской поликлинике использовались журналы самозаписи пациентов на прием к врачу. В регистратуре стоит стол, на котором в хаотичном порядке лежат папки самозаписи к врачам, в зависимости от участка, куда родители должны вписать ФИО ребенка, год рождения, полный возраст, место проживания для того, чтобы попасть на прием к своему специалисту в определенное время. Данные папки лежат в общедоступном месте, и, при желании, злоумышленник, посмотрев, когда родители приведут на лечение ребенка, в это время может обокрасть квартиру, где проживает данный ребенок, тем самым причинив значительный ущерб субъекту персональных данных. По этому факту была проведена проверка Роскомнадзора и выдано предписание на устранение нарушений. Каким образом можно исправить данное нарушение? **Ответ** Ввести систему «электронная регистратура». В журнале самозаписи на прием к врачу удалить графы с датой рождения ребенка, местом проживания. В журнале сделать приписку, что все данные, вносимые в папки самозаписи, становятся общедоступными.

3.2 Собеседование (вопросы для зачета)

3.2.1 Вопросы для зачета

ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

№ задания	Формулировка вопроса
51.	Сущность информационной безопасности и защиты информации при работе с современными информационными технологиями **Ответ** Информационная безопасность – это защищенность информации от незаконного получения, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности. Защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
52.	Каковы цели защиты информации при работе с современными информационными технологиями?

	Ответ Цели защиты информации: - целостность данных - конфиденциальность данных - доступность данных Целостность данных гарантирует, что они не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей. Конфиденциальность данных – это статус, предоставленный данным и определяющий требуемую степень их защиты. Конфиденциальность информации должна быть известна только допущенным и прошедшим проверку (авторизацию) субъектам информационной системы. Доступность данных. Условием работы с данными является доступ пользователя к ним. Под доступом к информации понимается ознакомление с ней и ее обработка, в частности копирование, модификация, уничтожение.
53.	Основные механизмы защиты информационных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к информации. **Ответ:** Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к информации используются следующие основные методы защиты (защитные механизмы): Идентификация (именование и опознавание), аутентификация (подтверждение подлинности) субъектов (пользователей) и объектов ресурсов, компонентов, служб) системы; Разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователем; Регистрация и оперативное оповещение о событиях, происходящих в системе и имеющие отношение к безопасности; Криптографическое закрытие хранимых и передаваемых по каналам связи данных Контроль целостности и аутентичности (подлинности и авторства) передаваемых и хранимых данных; Изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации путем трансляции адресов); Контроль вложений (выявление компьютерных вирусов, вредоносных кодов и их нейтрализация); Обнаружение и противодействие атакам (опасным действиям нарушителей); Выявление уязвимостей (слабых мест) системы
54.	К каким видам информации не может быть ограничен доступ согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»? **Ответ** Не может быть ограничен доступ к: -нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления - информации о состоянии окружающей среды - информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну) - информации, накапливаемой в открытых фондах библиотек, музеев, и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией - иной информации, недопустимость ограничения доступа к которой установлена федеральными законами
55.	Каковы принципы обработки персональных данных, закрепленные в соответствующем федеральном законе? **Ответ** Принципы обработки персональных данных: 1. Обработка персональных данных должна осуществляться на законной и справедливой основе. 2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. 3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой. 4. Обработке подлежат только персональные данные, которые отвечают целям их обработки. 5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

	6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных. 7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
56.	Какую информацию субъект персональных данных может потребовать от оператора? **Ответ** Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
57.	Что такое согласие на обработку персональных данных и какую информацию оно должно содержать? **Ответ** Согласие на обработку персональных данных представляет собой документ, который подтверждает добровольное решение гражданина передать оператору свою личную информацию для использования в определенных целях. В согласии на обработку персональных данных указывают правовые основания для обработки персональных данных, цели сбора данных, дату начала обработки и меры по обеспечению сохранности полученных сведений.
58.	Понятие технический канал утечки информации. Классификация каналов утечки информации **Ответ** Технический канал утечки информации — физический путь от источника информации к злоумышленнику, посредством которого может быть осуществлен несанкционированный доступ к охраняемым сведениям. Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать три основные элемента: источник сигнала, среду распространения носителя и приемник. Основным классификационным признаком технических каналов утечки информации является физическая природа носителя. По этому признаку они делятся на: • оптические; • радиоэлектронные; • акустические; • материально-вещественные.
59.	Какие виды электронной подписи существуют и их отличия? **Ответ** "Простая подпись — это знакомые всем коды доступа из СМС, коды на скретч-картах, пары “логин-пароль” в личных кабинетах на сайтах и в электронной почте. Простая подпись создается средствами информационной системы, в которой ее используют, и подтверждает, что электронную подпись создал конкретный человек. Усиленная неквалифицированная электронная подпись (далее — НЭП) создается с помощью программ криптошифрования с использованием закрытого ключа электронной подписи. НЭП идентифицирует личность владельца, а также позволяет проверить, вносили ли в файл изменения после его отправки. Усиленная квалифицированная электронная подпись — самый регламентированный государством вид подписи. Так же, как и НЭП, она создается с помощью криптографических алгоритмов и базируется на инфраструктуре открытых ключей, но отличается от НЭП в следующем: - Обязательно имеет квалифицированный сертификат в бумажном или электронном виде, структура которого определена приказом ФСБ России № 795 от 27.12.2011. - Программное обеспечение для работы с КЭП сертифицировано ФСБ России. - Выдавать КЭП может только удостоверяющий центр, который аккредитован Минкомсвязи России.
60.	Приведите примеры СЭД с применением ЭП, опишите различия симметричного и ассиметричного видов шифрования ЭП и электронных документов. **Ответ** "Принципиальное различие между этими двумя методами заключается в том, что алгоритмы сим-

	метричного шифрования используют один ключ, в то время как асимметричные используют два разных, но связанных между собой ключа. Алгоритмы симметричного шифрования используют один и тот же ключ для выполнения этой функции, алгоритм асимметричного шифрования напротив, использует один ключ для шифрования данных и другой для его дешифрования. В асимметричных системах ключ используемый для шифрования также известный как открытый (публичный), может свободно передаваться другим пользователям. С другой стороны, ключ используемый для расшифровки является приватным и должен храниться в секрете. Алгоритмы симметричного шифрования намного быстрее и требуют меньше вычислительной мощности, но их основным недостатком является распределение ключей. Поскольку один и тот же ключ используется для шифрования и дешифрования информации, этот ключ должен быть передан всем, кому потребуется доступ, что естественно создает определенные риски (как это было описано ранее). В свою очередь, асимметричное шифрование решает проблему распределения ключей, используя открытые ключи для шифрования, а приватные для дешифрования. Компромисс заключается в том, что асимметричные системы очень медленны по сравнению с симметричными и требуют гораздо большей вычислительной мощности из-за длины ключа.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

П ВГУИТ 2.4.03 Положение о курсовых, экзаменах и зачетах

П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости

Цифровая безопасность и защита информации [Электронный ресурс] : Задания и методические указания для самостоятельной работы обучающихся по направлению подготовки 38.05.01 Экономическая безопасность / Воронеж. гос. ун-т инж. технол. ; сост. Л. Н. Чайковская. Воронеж : ВГУИТ, 2023. 32 с. URL : https://education.vsuet.ru

Цифровая безопасность и защита информации [Электронный ресурс] : Задания и методические указания для практических занятий обучающихся по направлению подготовки 38.05.01 Экономическая безопасность / Воронеж. гос. ун-т инж. технол. ; сост. Л. Н. Чайковская. Воронеж : ВГУИТ, 2023. 32 с. URL : https://education.vsuet.ru

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности					
Знает	основные направления обеспечения цифровой безопасности, принципы работы современных информационных технологий, методы и средства защиты информации.	Результаты тестирования	Обучающимся даны правильные ответы менее чем на 59,99 % всех тестовых вопросов	Неудовлетворительно	Не освоена / недостаточный
			Обучающимся даны правильные ответы на 60-74,99% всех тестовых вопросов	Удовлетворительно	Освоена / базовый
			Обучающимся даны правильные ответы на 75-84,99% всех тестовых вопросов	Хорошо	Освоена / повышенный
			Обучающимся даны правильные ответы на 85-100% всех тестовых вопросов	Отлично	Освоена / повышенный
		Собеседование (зачет)	Обучающийся обладает частичными и разрозненными знаниями, только некоторые из которых может связывать между собой	Не зачтено	Не освоена / недостаточный
			Обучающийся обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Зачтено	Освоена / базовый (повышенный)
Умеет	выявлять угрозы информационным системам и ресурсам, применять современные информационные технологии для защиты информации	Решение задач на практических занятиях	Обучающийся не владеет умениями выполнения заданий; не демонстрирует умений, предусмотренных планируемыми результатами обучения	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор умений, предусмотренных планируемыми результатами обучения	Удовлетворительно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный

			Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует умения, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный
Владеет	навыками защиты информации в соответствующих сферах профессиональной деятельности	Домашняя контрольная работа	Обучающийся не владеет навыками выполнения заданий; не демонстрирует навыков, предусмотренных планируемыми результатами обучения	Неудовлетворительно	Не освоена / недостаточный
			Обучающийся испытывает затруднения при выполнении заданий по алгоритму; демонстрирует минимальный набор навыков, предусмотренных планируемыми результатами обучения	Удовлетворительно	Освоена / базовый
			Обучающийся выполняет задания с использованием алгоритма решения, при выполнении допускает незначительные ошибки и неточности, формулирует выводы; демонстрирует навыки, предусмотренные планируемыми результатами обучения	Хорошо	Освоена / повышенный
			Обучающийся выполняет задания, формируя алгоритм решения, при выполнении не допускает ошибок и неточностей, формулирует выводы; демонстрирует навыки, предусмотренные планируемыми результатами обучения	Отлично	Освоена / повышенный