АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«РЕГИОНАЛЬНЫЙ ЦЕНТР ПЕРЕПОДГОТОВКИ КАДРОВ УПРАВЛЕНИЯ»

СОГЛАСОВАНО
Руководитель
организации заказчика
_____ И.О. Фамилия
(подпись)
«____» _____ 20__ г.

(если необходимо)

УТВЕРЖДАЮ
Директор

_____Т.Б. Дубровина
(подпись)
«____» _____ 20__ г.

АНО
ДПО
"РЦПКУ"

Подписано цифровой подписью: АНО ДПО "РЦПКУ"
DN: 1.2.643.100.4=120A343832353131383830 34, 1.2.643.100.3=120B3036383632373734383133, 1.2.643.100.1=120D31313634383237303635373534, 1.2.643.3.131.1.1=120C343832333030353132313839, email=dutab@yandex.ru, c=RU, st=48 Липецкая область, l=ГОРОД ЛИПЕЦК, street=БАЛМОЧНЫХ С.Ф. УЛ,ВЛД 11,, o=АНО ДПО "РЦПКУ", cn=АНО ДПО "РЦПКУ", title=ДИРЕКТОР, givenName=ТАТЬЯНА БОРИССОВНА, sn=ДУБРОВИНА

# ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Организация работы по защите персональных данных»

г. Липецк, 2023 год

# АННОТАЦИЯ ПРОГРАММЫ

Дополнительная профессиональная программа (ДПП)

повышения квалификации

«Организация работы по защите персональных данных»

ДПП повышения квалификации направлена на:

- совершенствование компетенции, необходимой для профессиональной деятельности в области защиты персональных данных;
- получение новой компетенции, необходимой для профессиональной деятельности в области защиты персональных данных;
- повышение профессионального уровня в рамках имеющейся квалификации в области защиты персональных данных.

Программа предназначена широкому кругу специалистов, участвующих в обработке и хранение персональных данных:

- руководителям и специалистам государственных, муниципальных органов и органов местного самоуправления;
- руководителям департаментов информационных технологий и информационной безопасности;
- специалистам, работающим в области информационной безопасности;
- специалистам, отвечающим за работу с персональными данными;
- юристам, юрисконсультам предприятий-операторов персональных данных;
- работникам кадровых отделов организаций и предприятий.

Разработчик: Автономная некоммерческая организация дополнительного профессионального образования «Региональный центр переподготовки кадров управления».
Правообладатель программы: Автономная некоммерческая организация дополнительного профессионального образования «Региональный центр переподготовки кадров управления».

Нормативный срок освоения программы повышения квалификации 72 часа, при очно-заочной форме обучения с частичным отрывом от производства или заочной без отрыва от производства.

Одобрена к реализации на заседании педагогического совета протокол от «30» октября 2023 г. № 6.

СОДЕРЖАНИЕ

## **1.** ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ДПП повышения квалификации «Организация работы по защите персональных данных» направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста участвующего в обработке и хранение персональных данных.

Рабочая программа разработана в соответствии с:

- ФЗ от 29 декабря 2012 г. N 273 «Об образовании в Российской Федерации»
- приказом Министерства образования и науки РФ от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»
- профессиональным стандартом «Специалист по технической защите информации» утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 9 августа 2022 г. N 474н;
- Общероссийским классификатором занятий ОК 010-2014 (МСКЗ-08) (дата введения 01.07.2015)

Категория слушателей: специалисты предприятий и организаций, ответственные за обеспечение безопасности при работе с персональными данными.

Требования к имеющемуся уровню образования: лица, желающие освоить программу повышения квалификации, должны иметь (или получать) высшее образование, желательно в области информационной безопасности, юриспруденции и управления персоналом организации.

Срок освоения программы: 72 часа.

Форма обучения:

- Очно-заочная/заочная с применением электронного обучения и (или) дистанционных технологий.

Сфера профессиональной деятельности освоивших программу: связь, информационные и коммуникационные технологии.

Лица, завершившие освоение ДПП повышения квалификации «Организация работы по защите персональных данных», должны обладать следующими профессиональными компетенциями:

- разработка и подготовка к утверждению проектов нормативных и методических документов, регламентирующих работу по технической защите информации, положений, инструкций и других организационно-распорядительных документов.
- руководство работами по составлению актов, предписаний на право эксплуатации и другой документации по технической защите информации и обеспечению безопасности информации на объектах информатизации.
- организация разработки организационно-распорядительных документов в области технической защиты информации.
- осуществление контроля выполнения требований нормативных правовых актов и иных документов по технической защите информации.
- руководство работами по выявлению угроз безопасности информации, определению возможностей технической разведки и проведению мероприятий технической защиты информации.
- участие в обследовании объектов информатизации, их категорировании и аттестации.
- осуществление проверки выполнения требований нормативных документов по технической защите информации.

Новый вид деятельности или новая квалификация: ДПП повышения квалификации «Организация работы по защите персональных данных» при наличии высшего образование в области информационной безопасности, предоставляет возможность занятия должностей: главный специалист по технической защите информации, руководитель структурного подразделения по технической защите информации, специалист по технической защите информации.

Документ: удостоверение о повышении квалификации

## **2.** ЦЕЛЬ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

### 2.1. Цель ДПП повышения квалификации

Целью данной программы является совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалиста, участвующего в обработке и хранение персональных данных в следующих видах деятельности:

- проведение аттестации объектов информатизации на соответствие требованиям по защите информации
- организация и проведение работ по защите информации в организации

### 2.2. Результаты обучения

Обучающийся в ходе освоения программы должен знать:

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации
- порядок аттестации объектов информатизации на соответствие требованиям по защите информации
- программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее
- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее
- технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах
- технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные)

- технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных специальных электронных устройств перехвата информации в технические средства и (или) предметы интерьера помещения
- способы и средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок
- способы и средства защиты акустической речевой информации от утечки по техническим каналам
- нормативные правовые акты, методические документы в области защиты информации ограниченного доступа
- организационно-распорядительную документацию по защите информации на объекте информатизации
- эксплуатационную документацию на систему защиты информации
- организационно-распорядительную документацию по защите информации на объекте информатизации
- методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее
- порядок создания автоматизированных систем в защищенном исполнении

Обучающийся в ходе освоения программы должен уметь:

- умение определять перечень информации (сведений) ограниченного доступа, подлежащих защите в организации
- умение разрабатывать техническое задание на создание системы защиты информации в организации
- умение разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам автоматизированных (информационных) систем организации
- умение разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации
- умение анализировать данные о назначении, функциях, условиях функционирования основных технических средств и систем, установленных на объектах информатизации, и характере обрабатываемой на них информации
- умение организовывать ввод системы защиты информации в эксплуатацию

## **3.** СОДЕРЖАНИЕ ПРОГРАММЫ

### 3.1. Учебный план

ДПП повышения квалификации

«Организация работы по защите персональных данных»

| № п/п | Наименование модулей | Всего, час. | В том числе: | |
|---|---|---|---|---|
| | | | лекции | практич. и лаборат. занятия |
| 1. | Модуль 1. Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных | 11 | 11 | - |
| 2. | Модуль 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа | 11 | 11 | - |
| 3. | Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 9 | 9 | - |
| 4. | Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 16 | 10 | 6 |
| 5. | Модуль 5. Меры безопасности, применяемые при обработке персональных данных в информационных системах | 9 | 9 | - |
| 6. | Модуль 6. Создание модели системы защиты персональных данных в организации | - | - | 15 |
| Итоговая аттестация | | 1 | 1 | - |
| Итого | | 72 | 51 | 21 |

3.2. Календарный учебный график

ДПП повышения квалификации «Организация работы по защите персональных данных»

| № п/п | Наименование программы | Форма обучения | Месяцы/даты | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | январь | февраль | март | апрель | май | июнь | июль | август | сентябрь | октябрь | ноябрь | декабрь |
| 1. | Дополнительная профессиональная программа (ДПП) повышения квалификации «Организация работы по защите персональных данных» | Очно-заочная/заочная с применением дистанционных технологий, электронное обучение | По мере комплектования учебных групп в течение календарного года | | | | | | | | | | | |

3.3. Учебно-тематический план

ДПП повышения квалификации «Организация работы по защите персональных данных»

| № п/п | Наименование разделов, модулей, тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практические занятия | |
| **Модуль 1.** | Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных | 11 | 11 | - | |
| **Тема 1.1.** | Введение. Правовые основы технической защиты информации ограниченного доступа | 3 | 3 | - | Тестирование |
| **Тема 1.2.** | Организационные основы технической защиты информации ограниченного доступа | 2 | 2 | - | |
| **Тема 1.3.** | Организационные основы технической защиты информации ограниченного доступа в организации | 2 | 2 | - | |
| **Тема 1.4.** | Сертификация средств защиты и аттестация объектов информатизации | 4 | 4 | - | |
| **Модуль 2.** | Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа | 11 | 11 | - | |
| **Тема 2.1.** | Выявление угроз безопасности информации на объектах информатизации | 3 | 3 | - | Тестирование |
| **Тема 2.2.** | Основные организационные меры защиты информации от несанкционированного доступа | 4 | 4 | - | |

| № п/п | Наименование разделов, модулей, тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практические занятия | |
| **Тема 2.3.** | Основные технические и программные средства защиты информации от несанкционированного доступа | 4 | 4 | - | |
| **Модуль 3.** | Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 9 | 9 | - | |
| **Тема 3.1.** | Угрозы безопасности информации | 2 | 2 | - | Тестирование |
| **Тема 3.2.** | Утечка информации | 2 | 2 | - | |
| **Тема 3.3.** | Защита информации от утечки | 5 | 5 | - | |
| **Модуль 4.** | Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 16 | 10 | 6 | |
| **Тема 4.1.** | Основные понятия обработки персональных данных | 1 | 1 | - | Тестирование |
| Практическая работа по теме 4.1. "Основные понятия обработки персональных данных" | | - | - | 2 | Проверка практической работы |
| **Тема 4.2.** | Субъект персональных данных | 1 | 1 | - | Тестирование |
| **Тема 4.3.** | Оператор персональных данных | 1 | 1 | - | |
| **Тема 4.4.** | Меры по обеспечению безопасности персональных данных | 2 | 2 | - | |
| **Тема 4.5.** | Обработка персональных данных | 3 | 3 | - | |
| Практическая работа по теме 4.5. "Обработка персональных данных" | | - | - | 4 | Проверка практической работы |
| **Тема 4.6.** | Нарушения законодательства РФ в области персональных данных | 2 | 2 | - | Тестирование |

| № п/п | Наименование разделов, модулей, тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практические занятия | |
| **Модуль 5.** | Меры безопасности, применяемые при обработке персональных данных в информационных системах | 9 | 9 | - | |
| **Тема 5.1.** | Типовые программно-технические средства защиты информации | 2 | 2 | - | Тестирование |
| **Тема 5.2.** | Организация защиты персональных данных в организации | 3 | 3 | - | |
| **Тема 5.3.** | Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 4 | 3 | - | |
| **Модуль 6.** | Создание модели системы защиты персональных данных в организации | 15 | - | 15 | |
| Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации | | 2 | - | 2 | Проверка практической работы |
| Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе | | 2 | - | 2 | |
| Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации | | 2 | - | 2 | |
| Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации | | 3 | - | 3 | |

| № п/п | Наименование разделов, модулей, тем | Всего часов | В том числе: | | Формы контроля |
|---|---|---|---|---|---|
| | | | лекции | практические занятия | |
| Практическая работа № 5. Определение перечня организационно-распорядительных документов необходимых для регламентации защиты персональных данных в организации | | 3 | - | 3 | |
| Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации | | 3 | - | 3 | |
| | Итоговая аттестация | 1 | 1 | - | Итоговое тестирование |
| | Итого: | 72 | 51 | 21 | |

## 3.4. Содержание учебных модулей

Модуль 1. Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных

Тема 1.1. Правовые основы технической защиты информации ограниченного доступа

Основные понятия и определения в области защиты информации. Доктрина информационной безопасности Российской Федерации. Информационная безопасность как одно из стратегических направлений национальной безопасности Российской Федерации. Концептуальные вопросы защиты информации.

Тема 1.2. Организационные основы технической защиты информации ограниченного доступа

Силы обеспечения информационной безопасности. Задачи ФСБ России по обеспечению общей и информационной безопасности. Основные задачи ФСО России. Деятельность Минобороны России и МВД России по обеспечению информационной безопасности. Деятельность Минкомсвязи России в сфере информационной безопасности. Полномочия Роскомнадзора в сфере информационной безопасности. Полномочия ФСТЭК России. Задачи ФСТЭК России. Деятельность органов власти и местного самоуправления в сфере информационной безопасности РФ.

Тема 1.3. Организационные основы технической защиты информации ограниченного доступа в организации

Структура и функции органов и подразделений по технической защите информации в организации. Система обеспечения информационной безопасности. Лицензирование деятельности в области защиты информации.

Тема 1.4. Сертификация средств защиты и аттестация объектов информатизации

Нормативно-правовая база сертификации средств защиты и аттестации объектов информатизации. Формы подтверждения соответствия. Декларирование соответствия. Сертификат соответствия. Нормативно-правовая база сертификация средств защиты информации. Сертификация средств защиты информации (СЗИ). Электронная цифровая подпись. Аттестация объектов информатизации

Модуль 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Тема 2.1. Выявление угроз безопасности информации на объектах информатизации

Угрозы информационной безопасности. Классификация угроз информационной безопасности Классификация источников угроз. Уязвимости безопасности информации.

Тема 2.2. Основные организационные меры защиты информации от несанкционированного доступа

Аттестация объектов информатизации. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Разработка программы и методики аттестационных испытаний. Заключение договоров на аттестацию. Заключение по результатам аттестации. Рассмотрение апелляций. Аттестат соответствия. Аттестация объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

Тема 2.3. Основные технические и программные средства защиты информации от несанкционированного доступа

Особенности программно-математического воздействия в сетях общего пользования. Защита информации в локальных вычислительных сетях.

Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Тема 3.1. Угрозы безопасности информации

Угрозы безопасности информации. Случайные и преднамеренные угрозы. Традиционный шпионаж и диверсии. Системы подсушивания. Видеоразведка. Закладные устройства. Несанкционированный доступ к информации. Электромагнитные излучения и наводки. Несанкционированная модификация структур. Вредительские программы. Классификация злоумышленников.

Тема 3.2.Утечка информации

Утечка информации по техническим каналам. Физическая природа передачи информации. Каналы утечки информации. Особенности каналов утечки информации. Побочные электромагнитные излучения и наводки (ПЭМИН)

Тема 3.3. Защита информации от утечки

Защита информации от утечки по техническим каналам в общем плане. Защита информации от утечки по визуально-оптическим каналам. Средства и способы защиты информации от утечки по визуально-оптическому каналу. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным каналам. Защита от утечки за счёт электромагнитного излучения. Программно-аппаратный комплекс «Зарница». Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания. Защита от утечки за счет взаимного влияния проводов и линий связи. Взаимные влияния в линиях связи. Защита информации от утечки по материально-вещественным каналам.

Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных

данных при их обработке в информационных системах персональных данных

Тема 4.1. Основные понятия обработки персональных данных

Основные понятия, используемые в ФЗ от 27 июля 2006 г. N 152 "О персональных данных". Принципы и условия обработки персональных данных. Условия обработки персональных данных.

Практическая работа по теме 4.1. "Основные понятия обработки персональных данных"

Тема 4.2. Субъект персональных данных

Права субъекта персональных данных. Согласие субъекта персональных данных на обработку его персональных данных.

Тема 4.3. Оператор персональных данных

Обязанности оператора при сборе персональных данных. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ от 27 июля 2006 г. N 152 "О персональных данных".

Тема 4.4. Меры по обеспечению безопасности персональных данных

Меры по обеспечению безопасности персональных данных при их обработке. Состав и содержание мер по обеспечению безопасности персональных данных.

Тема 4.5. Обработка персональных данных

Уведомление об обработке персональных данных. Лица, ответственные за организацию обработки персональных данных в организациях. Обработка персональных данных без средств автоматизации. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

Практическая работа по теме 4.5. "Обработка персональных данных"

Тема 4.6. Нарушения законодательства РФ в области персональных данных

Ответственность за нарушение законодательства Российской Федерации в области персональных данных при обработке персональных данных работника. Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Модуль 5. Меры безопасности, применяемые при обработке персональных данных в информационных системах

Тема 5.1. Типовые программно-технические средства защиты информации

Правовая база. Межсетевой экран. Брандмауэр. Криптография. Цифровая подпись.

Тема 5.2. Организация защиты персональных данных в организации

Защита персональных данных работника (общие положения). Требования к обработке персональных данных. Защита персональных данных. Организация доступа работников к персональным данным других работников.

Тема 5.3. Требования к защите, состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

Модуль 6. Создание модели системы защиты персональных данных в организации

Практическая работа № 1. Определение условий функционирования системы обработки персональных данных в организации

Практическая работа № 2. Определение актуальных угроз безопасности персональных данных в организации при их обработке в информационной системе

Практическая работа № 3. Определение необходимого уровня защищенности персональных данных в организации

Практическая работа № 4. Определение перечня нормативно-правовых актов при определении/описании создаваемой с учетом уже существующих средств защиты персональных данных в организации

Практическая работа № 5. Определение перечня организационно-распорядительных документов необходимых для регламентации защиты персональных данных в организации

Практическая работа № 6. Определение на основании разработанной/спроектированной системы защиты средства защиты, нейтрализующих актуальных угроз безопасности в организации

## **4.** УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

### 4.1. Материально-техническое оснащение программы

Процесс обучения в очно-заочной с применением электронного обучения и дистанционных технологий предусматривает теоретическое обучение и практические занятия в АНО ДПО «РЦПКУ», размещенной по адресу: Липецкая обл., г. Липецк, ул. Балмочных С.Ф., влд 11.

Помещение, используемое для образовательного процесса, находится на 3 этаже офисного 9 этажного здания. Общая площадь учебного класса составляет 20,3 кв.м и рассчитана на 10 человек.

Учебный класс оборудован столами и стульями, столом для преподавателя. Оснащен доступом к сети Интернет. Для демонстрации лекционного материала размещен ноутбук с проектором и доска.

В качестве инструмента дистанционного обучения используется система дистанционного обучения (СДО) «Учи.Про» (sdo.uchi.pro), размещенная по адресу в сети Интернет: https://v3588.upft.ru/

Процесс обучения в заочной форме с применением дистанционных технологий предусматривает теоретическое обучение и практические занятия с использованием:

- информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников;
- системы дистанционного обучения (СДО) «Учи.Про» (sdo.uchi.pro), размещенная по адресу в сети Интернет: https://v3588.upft.ru/.

### 4.2. Информационное обеспечение программы.

Нормативные документы:

1. Конституция РФ.
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ (КоАП РФ).
3. Федеральный закон от 28 июня 2014 г. N 172-ФЗ «О стратегическом планировании в Российской Федерации».
4. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности».
5. Федеральный закон от 3 апреля 1995 г. N 40-ФЗ «О федеральной службе безопасности».
6. Федеральный закон от 27 мая 1996 г. N 57-ФЗ «О государственной охране».

7. Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».
8. Федеральный закон от 26 декабря 2008 г. N 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».
9. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
10. Федеральный закон от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании».
11. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».
13. Закон РФ от 21 июля 1993 г. N 5485-I «О государственной тайне».
14. Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации».
15. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
16. Указ Президента РФ от 7 августа 2004 г. N 1013 «Вопросы Федеральной службы охраны Российской Федерации».
17. Указ Президента РФ от 16 августа 2004 г. N 1082 «Вопросы Министерства обороны Российской Федерации».
18. Указ Президента РФ от 1 марта 2011 г. N 248 «Вопросы Министерства внутренних дел Российской Федерации».
19. Указ Президента РФ от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
20. Указ Президента РФ от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
21. Указ Президента РФ от 11 марта 2003 г. N 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации».
22. Постановление Правительства РФ от 2 июня 2008 г. N 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».
23. Постановление Правительства РФ от 16 марта 2009 г. N 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
24. Постановление Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

25. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
26. Постановление Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
27. Постановление Правительства РФ от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
28. Постановление Правительства РФ от 8 августа 2022 г. N 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации».
29. Постановление Правительства РФ от 18 мая 2009 г. N 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».
30. Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации».
31. Постановление Правительства РФ от 21 апреля 2010 г. N 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения и о внесении изменения в Положение о сертификации средств защиты информации».
32. Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
33. Постановление Правительства РФ от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными

правовыми актами, операторами, являющимися государственными или муниципальными органами».

34. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
35. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
36. Приказ ФСБ РФ от 13 ноября 1999 г. N 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».
37. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями и дополнениями).
38. Приказ Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. N 55 «Об утверждении Положения о системе сертификации средств защиты информации».
39. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
40. Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
41. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных».
42. Приказ Федеральной службы по техническому и экспортному контролю от 29 апреля 2021

г. N 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

43. Приказ Министерства труда и социальной защиты РФ от 9 августа 2022 г. N 474н «Об утверждении профессионального стандарта "Специалист по технической защите информации"».
44. Руководящий документ. «Защита от несанкционированного доступа к информации. Термины и определения» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).
45. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).
46. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
47. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).
48. Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25 июля 1997 г.).
49. Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования».
50. Руководящий документ «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин автоматизированных кассовых систем и требования по защите информации».
51. Руководящий документ. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. N 114).
52. Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (введен в действие приказом Государственной

технической комиссии при Президенте РФ от 19 июня 2002 г. N 187).

53. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
54. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 года).
55. ГОСТ Р 50752-95.
56. ГОСТ 30373-95/ГОСТ 50414-92.
57. ГОСТ 29339-92

Основные документы:

1. Информационные технологии в юридической деятельности : учебник для вузов / П. У. Кузнецов [и др.] ; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 325 с.

2. Инновационный менеджмент : учебник для вузов / под общей редакцией Л. П. Гончаренко. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 487 с.

3. Трудовое право. Особенная часть : учебник для вузов / М. О. Буянова [и др.] ; ответственный редактор М. О. Буянова. — Москва : Издательство Юрайт, 2023. — 542 с.

4. Корнеев, И. К. Документирование управленческой деятельности : учебник для вузов / И. К. Корнеев, А. В. Пшенко, В. А. Машурцев. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 438 с.

5. Шульц, В. Л. Безопасность предпринимательской деятельности : учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 585 с.

## 4.3. Кадровое обеспечение реализации программы

Педагогические работники, реализующие программу, должны удовлетворять квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям и (или) профессиональных стандартах.

## **5.** ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Освоение ДПП завершается итоговой аттестацией слушателей в форме - квалификационного экзамена в виде тестирования.

Лицам, успешно освоившим ДПП и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

Результаты итоговой аттестации оформляются протоколом.

### 5.1. Контрольно-оценочные материалы (типовые задания) для оценки знаний

По окончании ДПП осуществляется контроль уровня освоения заявленных компетенций в форме итоговой аттестации - квалификационного экзамена. Квалификационный экзамен проводится дистанционно.

В качестве экзаменационного задания слушателям необходимо выполнить тест, включающий 30 тестовых заданий. Тестовые задания подбираются случайно из всех вопросов, закрепленных за лекционными материалами в модулях обучения.

Предъявляемые слушателям тестовые задания – это задания закрытой формы с выбором одного, редко — нескольких правильных ответов.

Итоги квалификационного экзамена оформляются локальным актом образовательной организации (протоколом).

При несогласии экзаменуемого с результатами квалификационного экзамена составляется акт, подписываемый членами экзаменационной комиссии и обучаемым, в котором отражается предмет спора. В этом случае в целях соблюдения гарантий объективности и независимости оценки качества подготовки, обучающемуся предоставляется возможность обратиться к руководству образовательной организации, а также к представителям работодателей и их объединений.

Типовые задания для проведения квалификационного экзамена

Задания итогового теста

Правильный вариант ответа в тексте выделен жирным шрифтом

**Модуль 1.** Законодательство РФ в области защиты персональных данных. Основные понятия в законодательстве о персональных данных. Организация работы по защите персональных данных

**Тема 1.1.** Правовые основы технической защиты информации ограниченного доступа

1. Целью информационной безопасности является обеспечение:

1. Понятности, полезности, доступности данных

2. Доступности, целостности, конфиденциальности данных

3. Сохранности данных

2. Система безопасности это:

1. Нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации

2. Нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия

3. Организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающая защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз

3. Что из перечисленного не входит в перечень задач, решаемых службой информационной безопасности:

1. Определение информационных и технических ресурсов, подлежащих защите

2. Выявление полного множества потенциально возможных угроз и каналов утечки информации

3. Определение требований к системе защиты информации

4. Все пункты входят в перечень задач

4. Государственная система лицензирования деятельности в области технической защиты информации включает в себя две составляющие:

1. Допуск предприятий и организаций к оказанию услуг по защите информации

2. Создание единой системы норм и регламентов деятельности служб, органов, реализующих защиту информации

3. Контроль качества и эффективности оказываемых услуг в процессе их деятельности

5. Обязательное подтверждение соответствия средств защиты информации требованиям по защите сведений соответствующей степени секретности осуществляется в формах:

1. Экспертизы соответствия

2. Декларирования соответствия

3. Обязательной сертификации

6. Субъект персональных данных имеет право:

1. На получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных

2. На доступ к персональным данных своих близких родственников

3. На доступ к персональным данных своих близких родственников при условии подачи запроса, содержащего номер основного документа, удостоверяющего личность субъекта

7. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. То есть целостность предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации - это

1. Доступность
2. Целостность
3. Конфиденциальность

8. Защита от несанкционированного доступа к информации - это

1. Доступность
2. Целостность
3. Конфиденциальность

9. Целью информационной безопасности является обеспечение:

1. Понятности, полезности, доступности данных
2. Доступности, целостности, конфиденциальности данных
3. Сохранности данных

10. Согласно терминологии Доктрины информационной безопасности РФ, осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления - это

1. Обеспечение информационной безопасности
2. Средства обеспечения информационной безопасности
3. Система обеспечения информационной безопасности

11. Укажите, верно ли утверждение: Реализация Доктрины осуществляется на основе отраслевых документов стратегического планирования РФ.

1. Да
2. Нет

12. Согласно Стратегии национальной безопасности РФ, реализация органами публичной власти во взаимодействии с институтами гражданского общества и организациями политических, правовых, военных, социально-экономических, информационных, организационных и иных мер, направленных на противодействие угрозам национальной безопасности - это

13. Национальная безопасность Российской Федерации

1. Обеспечение национальной безопасности
2. Угроза национальной безопасности
3. Система обеспечения национальной безопасности

14. Система безопасности это:

1. Нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия
2. Организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающая защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз
3. Нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации

15. Положения концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в ИС:

1. направление - защита информации от утечки по техническим каналам

2. направление - защита информации в ИС от несанкционированного доступа

3. направление — защита информации в ИС от сбоев, ведущих к потере информации

4. направление - зашита от неавторизованного создания или уничтожения данных

**Тема 1.2.** Организационные основы технической защиты информации ограниченного доступа

1. Какие направления по обеспечению информационной безопасности Правительство РФ реализует в рамках своих полномочий:

1. разрабатывает и принимает на основе Конституции РФ законодательную базу в области обеспечения информационной безопасности

2. проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации

3. разрабатывает федеральные целевые программы и выделяет необходимые финансовые средства для их реализации

4. осуществляет меры по предотвращению угроз информационной безопасности и организационному обеспечению этой деятельности

5. издает постановления и распоряжения в области обеспечения информационной безопасности и контролирует их обязательное исполнение

2. Задачи и функции ФСБ России определены:

1. ФЗ «О Федеральной службе безопасности»

2. Стратегией национальной безопасности РФ

3. ФЗ «О безопасности»

4. Положением о Федеральной службе безопасности Российской Федерации

3. Укажите, верно ли утверждение: ФСО России в соответствии с законодательством РФ обеспечивает безопасность при подключении к сети Интернет федеральных органов государственной власти и органов государственной власти субъектов РФ.

1. Да

2. Нет

4. МВД России в рамках законодательства и в пределах своих полномочий обеспечивает:

1. организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах

2. осуществляет разведывательную деятельность в интересах обороны и в пределах своей компетенции — в интересах безопасности Российской Федерации

3. организацию предупреждения, выявления, пресечения, раскрытия и расследования преступлений, а также предупреждения и пресечения административных правонарушений, совершаемых в информационной сфере

5. Укажите федеральный орган исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных, а также использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним:

1. Минкомсвязи России

2. Роскомнадзор России

3. ФСТЭК России

6. Укажите федеральный орган исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, а также по защите прав субъектов персональных данных

1. Минкомсвязи России

2. Роскомнадзор России

3. ФСТЭК России

7. Укажите федеральный орган исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности

1. Минкомсвязи России

2. Роскомнадзор России

3. ФСТЭК России

8. Органы власти субъектов РФ в пределах предметов ведения:

1. разрабатывают и принимают нормативные правовые акты в области обеспечения информационной безопасности

2. обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности Российской Федерации

3. рассматривают проекты официальных документов по вопросам обеспечения информационной безопасности

**Тема 1.3.** Организационные основы технической защиты информации ограниченного доступа в организации

1. Что из перечисленного не входит в перечень задач, решаемых службой информационной безопасности:

1. Определение информационных и технических ресурсов, подлежащих защите

2. Выявление полного множества потенциально возможных угроз и каналов утечки информации

3. Определение требований к системе защиты информации

4. Все пункты входят в перечень задач

2. Что из перечисленного входит в компетенцию службы информационной безопасности организации:

1. выявление нелояльных сотрудников

2. мониторинг психологического климата в коллективе

3. адаптирование сотрудника к новому коллективу

4. контроль за исполнением сотрудником возложенных на него функций

3. Укажите, к каким средствам обеспечения информационной безопасности относятся криптографические средства защиты информации.

1. методическим

2. финнсовым

3. нормативно-правовым

4. техническим

4. Укажите, в состав каких средств обеспечения информационной безопасности входит методическое обеспечение.

1. финансовое и материального

2. нормативно-правового

3. технологического

5. Государственная система лицензирования деятельности в области технической защиты информации включает в себя:

1. Допуск предприятий и организаций к оказанию услуг по защите информации

2. Создание единой системы норм и регламентов деятельности служб, органов, реализующих защиту информации

3. Контроль качества и эффективности оказываемых услуг в процессе их деятельности

6. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет

1. ФСТЭК России

2. Минкомсвязи России

3. Роскомнадзор России

**Тема 1.4.** Сертификация средств защиты и аттестация объектов информатизации

1. Укажите срок, который должны обеспечить операторы федеральных государственных информационных систем при восстановлении информации, измененной или уничтоженной вследствие несанкционированного доступа к ней.

1. не более 8 часов

2. не более 12 часов

3. не более 24 часов

4. не более 3 дней

2. Согласно требованию какого документа, допускается использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия

1. Положение о лицензировании деятельности по технической защите конфиденциальной информации

2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных

3. ФЗ «О техническом регулировании»

3. Согласно Постановлению правительства РФ 18 мая 2009 г. N 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» операторы федеральных государственных ИС обязаны обеспечить:

1. защиту информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и блокирования доступа к ней

2. постоянный контроль возможности доступа неограниченного круга лиц к информационным системам общего пользования

3. информационную безопасность при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям

4. Формой осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров называется:

1. сертификация

2. схема подтверждения соответствия

3. оценка соответствия

4. декларирование соответствия

5. Форма подтверждения соответствия продукции требованиям технических регламентов — это

1. сертификация

2. схема подтверждения соответствия

3. оценка соответствия

4. декларирование соответствия

6. Обязательное подтверждение соответствия средств защиты информации требованиям по защите сведений соответствующей степени секретности осуществляется в формах:

1. Экспертизы соответствия

2. Декларирования соответствия

3. Обязательной сертификации

7. Форма и схемы обязательного подтверждения соответствия могут устанавливаться

1. техническим регламентом

2. правительством РФ

3. государственными (контрактными) договорами

8. Что должен содержать технический регламент подтверждения соответствия?

1. описание объектов технического регулирования

2. требования к объектам технического регулирования

3. правила их идентификации в целях применения технического регламента

4. особенности оценки соответствия указанных объектов

5. все перечисленное

9. Срок действия декларации о соответствии определяется

1. техническим регламентом

2. Федеральным органом исполнительной власти по техническому урегулированию

3. уполномоченным Правительством РФ Федеральным органом исполнительной власти

10. Форма сертификата соответствия

1. определяется соответствующим техническим регламентом

2. утверждается федеральным органом исполнительной власти по техническому регулированию

3. утверждается уполномоченным Правительством РФ Федеральным органом исполнительной власти

11. Какой вид ЭП позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания

1. простая электронная подпись

2. усиленная неквалифицированная электронная подпись

3. усиленная квалифицированная электронная подпись

12. У какого вида ЭП ключ проверки электронной подписи указан в квалифицированном сертификате

1. простая электронная подпись

2. усиленная неквалифицированная электронная подпись

3. усиленная квалифицированная электронная подпись

13. Укажите, верно ли утверждение: К объектам информатизации, аттестуемыми по требованиям безопасности информации, помещения в которых установлены системы связи,

предназначенные для обработки и передачи информации, подлежащей защите НЕ ОТНОСЯТСЯ.

1. Да

2. Нет

14. Что дает право обработки информации с определённым уровнем конфиденциальности на объекте информатизации:

1. наличие действующего «Аттестата соответствия»

2. наличие договора с уполномоченными федеральными органами по аттестации объектов информатизации по требованиям безопасности информации

3. перечень организационно-технических мероприятий в результате которых подтверждается, что объект соответствует требованиям стандартов, утверждённых уполномоченными федеральными органами исполнительной власти

15. Укажите, кто несёт юридическую и финансовую ответственность за качество проведённых работ по аттестации объектов информатизации

1. руководитель органа по аттестации объектов информатизации

2. сотрудники органа по аттестации объектов информатизации, проводившие работы

3. руководитель органа по аттестации объектов информатизации и сотрудники, проводившие работы

16. Укажите группу классов защищенности АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности

1. 1 группа

2. 2 группа

3. 3группа

**Модуль 2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

**Тема 2.1.** Выявление угроз безопасности информации на объектах информатизации

1. К антропогенным источникам угроз информационной безопасности относятся:

1. Магнитные бури

2. Представители надзорных организаций и аварийных служб

3. Сети инженерных коммуникации

2. К антропогенным источникам угроз информационной безопасности относятся:

1. Угроза безопасности объекта

2. Источник угрозы

3. Уязвимость объекта

4. Атака

3. Возможное воздействие на объект, которое прямо или косвенно может нанести ущерб его безопасности – это

1. Угроза безопасности объекта

2. Источник угрозы

3. Уязвимость объекта

4. Атака

4. Присущие объекту причины, приводящие к нарушению безопасности информации на объекте – это

1. Угроза безопасности объекта

2. Источник угрозы

3. Уязвимость объекта

4. Атака

5. Укажите свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям.

1. Конфиденциальность информации

2. Доступность информации

3. Целостность информации

6. Укажите нарушения при обеспечении конфиденциальности

1. утрата (неумышленная потеря, утечка) информации и средств ее обработки

2. блокирование информации

3. отрицание подлинности информации

7. Укажите нарушения при обеспечении целостности

1. хищение (копирование) информации и средств ее обработки

2. уничтожение информации и средств ее обработки

3. модификация (искажение) информации

8. Укажите критериев сравнения степень опасности, который определяет степень влияния уязвимости на неустранимость последствий реализации угрозы

1. Фатальность

2. Доступность

3. Количество

9. К объективным уязвимостям информационной безопасности относятся:

1. Сопутствующие техническим средствам излучения: электромагнитные, электрические, звуковые

2. Ошибки (халатность) при подготовке и использовании программного обеспечения, эксплуатации технических средств; старение и размагничивание носителей информации

3. Отказы и неисправности технических средств, сбои программного обеспечения

**Тема 2.2.** Основные организационные меры защиты информации от несанкционированного доступа

1. Аттестация НЕ является обязательной в случае:

1. Государственной тайны

2. Управлении экологически опасными объектами

3. Деятельности медицинских учреждений

2. В качестве заявителей аттестации могут выступать

1. заказчики, владельцы

2. разработчики аттестуемых объектов информатизации

3. отраслевые и региональные учреждения

4. предприятия и организации по защите информации

5. специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию

3. В качестве органов по аттестации могут выступать

1. заказчики, владельцы

2. разработчики аттестуемых объектов информатизации

3. отраслевые и региональные учреждения

4. предприятия и организации по защите информации

5. специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию

4. Укажите функции осуществляемые в рамках аттестации органами по аттестации

1. осуществление контроля за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией

2. формирование фонда нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке

3. рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации

4. организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации

5. проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации

6. предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию

5. Заключение договора между заявителем и органом по аттестации выполняется после

1. подача и рассмотрение заявки на аттестацию

2. предварительного ознакомления с аттестуемым объектом

3. испытания в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте

4. разработки программы и методики аттестационных испытаний

5. проведение аттестационных испытаний объекта информатизации

6. Укажите, верно ли утверждение: Заключение по результатам аттестации подписывается членами аттестационной комиссии и представляется заявителю.

1. Да

2. Нет

7. Аттестат соответствия выдается

1. не более чем на 3 года

2. не более чем на год

3. не более чем на 2 года

8. Утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77 определяет порядок организации и проведения работ по аттестации объектов информатизации

1. на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

2. на соответствие требованиям о защите информации ограниченного доступа, составляющей государственную тайну

3. на соответствие требованиям о защите информации ограниченного доступа

9. Назначение экспертов органов по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну из числа работников, участвующих в разработке и (или) внедрении системы защиты информации объекта информатизации

1. не допускается

2. допускается

10. Срок проведения работ по аттестации объекта информатизации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

1. устанавливается владельцем объекта информатизации по согласованию с органом по аттестации

2. устанавливается владельцем объекта информатизации без согласования с органом по аттестации

3. устанавливается органом по аттестации

4. не может превышать четырех месяцев

5. не может превышать одного месяца

6. не может превышать трех месяцев

11. В ходе аттестационных испытаний объекта информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну владельцем объекта информатизации

1. могут вноситься изменения в объект информатизации, с том числе в архитектуру его системы защиты информации

2. не могут вноситься изменения в объект информатизации

12. Укажите пропущенное словосочетание: Заключение и протоколы в течение _____ после утверждения органом по аттестации объекта информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, направляются владельцу объекта информатизации.

1. 5 рабочих дней

2. 5 дней

3. 3 рабочих дней

4. 3 дней

5. 10 дней

13. Укажите срок, в который протоколы контроля защиты информации ограниченного доступа, не составляющей государственную тайну предоставляются на аттестованном объекте информатизации предоставляются в ФСТЭК России (территориальный орган ФСТЭК России)

1. не реже одного раза в два года

2. не реже одного раза в три года

3. не реже одного раза в год

4. не предоставляются

14. Укажите, что является основанием для приостановления действия аттестата соответствия

1. непредставление протоколов контроля защиты информации в ФСТЭК России (территориальный орган ФСТЭК России)

2. любые изменения архитектуры системы защиты информации аттестованного объекта информатизации

3. не устранение недостатков, выявленных ФСТЭК России (территориальным органом ФСТЭК России)

**Тема 2.3.** Основные технические и программные средства защиты информации от несанкционированного доступа

1. Программная закладка "троянский конь" это:

1. Программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба

2. Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения

3. Тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей

2. Для обнаружения вирусов антивирусные программы используют следующие методы:

1. Сигнатурный

2. Дедуктивный

3. Эвристический

3. Укажите троянскую программу, которая способна выполнять удаленное управление зараженным компьютером

1. Backdoor

2. Rootkit

3. Trojan-Dropper

4. Укажите троянскую программу, которая способна выполнять удаленное управление зараженным компьютером.

1. Trojan-Notifier

2. Trojan-PSW

3. Trojan-DDoS

5. Стадии жизненного цикла классического трояна

1. активация

2. выполнение вредоносных действий

3. проникновение на чужой компьютер

4. поиск объектов для заражения

5. внедрение копий

6. подготовка копий

6. Подозрительная сетевая активность может быть вызвана …

1. логической бомбой

2. сетевым червем

3. трояном

4. P2P-червем

7. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.

1. нет

2. да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы

3. да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

8. Преимущества эвристического метода антивирусной проверки над сигнатурным

1. более надежный

2. не требует регулярного обновления антивирусных баз

3. существенно менее требователен к ресурсам

4. позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

**Модуль 3.** Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

**Тема 3.1.** Угрозы безопасности информации

1. Какие угрозы безопасности информации являются преднамеренными:

1. ошибки персонала

2. открытие электронного письма, содержащего вирус

3. не авторизованный доступ

2. Целью создания любой компьютерной сети является

1. удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости)

2. сохранение конфиденциальности и достоверности информации

3. своевременное получение информации

3. Конфиденциальностью называется:

1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

2. описание процедур

3. защита от несанкционированного доступа к информации

4. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

4. корыстными устремлениями злоумышленников

5. ошибками при действиях персонала

5. Искусственные угрозы безопасности информации вызваны:

1. деятельностью человека

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения

3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека

4. корыстными устремлениями злоумышленников

5. ошибками при действиях персонала

6. Укажите принцип действия устройства, позволяющего на расстоянии фиксировать разговор в помещении с закрытыми окнами

1. анализ отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн

2. преобразование механических колебаний стекол в электрический сигнал с последующей передачей по радиоканалу

3. преобразование акустических колебания в электрические

7. Укажите принцип действия стетоскопного микрофона

1. анализ отраженного луча лазера от стекла окна помещения, которое колеблется от звуковых волн

2. преобразование механических колебаний стекол в электрический сигнал с последующей передачей по радиоканалу

3. преобразование акустических колебания в электрические

8. Электромагнитные излучения используются злоумышленниками для

1. получения информации

2. уничтожения информации

3. получения и уничтожения информации

9. Закладка – это

1. несанкционированное изменение структуры компьютерной сети

2. обход средств защиты информации

3. использование привилегированных режимов работы

10. Программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах и выполняемые только при соблюдении определенных условий называются

1. Логические бомбы

2. Черви

3. Троянские кони

4. Компьютерные вирусы

11. Программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии называются

1. Логические бомбы

2. Черви

3. Троянские кони

4. Компьютерные вирусы

**Тема 3.2.** Утечка информации

1. Какой из пунктов не относится к видам каналов утечки информации с точки зрения физической природы:

1. Визуально-оптические, акустические

2. Фотонные, динамические

3. Электромагнитные, материально-вещественные

2. Укажите, верно ли утверждение: Большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

1. Да

2. Нет

3. Укажите, верно ли утверждение: С позиции передачи информации человек рассматривается как носитель информации

1. Да

2. Нет

4. Под структурным звуком понимают

1. механические колебания в твердых средах

2. распространение звука в воздушном пространстве

3. распространение звука в воде

5. Утечка информации – это …

1. процесс раскрытия секретной информации

2. несанкционированный процесс переноса информации от источника к злоумышленнику

3. процесс уничтожения информации

4. непреднамеренная утрата носителя информации

**Тема 3.3.** Защита информации от утечки

1. Защита информации от утечки это деятельность по предотвращению:

1. 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

2. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений

3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа

4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации

2. Защита информации это:

1. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

2. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям

3. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

3. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации

2. пользователи

3. сотрудники службы безопасности

4. представители конкурирующих организаций

5. лица, нарушившие пропускной режим

4. Аэрозольные завесы и дымообразующие вещества используются в качестве защиты информации от утечки по

1. визуально-оптическому каналу

2. техническим каналам

3. акустическим каналам

4. электромагнитным каналам

5. Для общих целей используется шумомер

1. нулевого класса

2. первого класса

3. второго класса

4. третьего класса

6. Укажите класс шумомеров, которые чаще всего используются на практике для оценки степени защищенности акустических каналов

1. нулевого класса

2. первого класса

3. второго класса

4. третьего класса

7. Электростатическое экранирование

1. заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведенных зарядов на массу и на землю

2. основано на замыкании силовых линий магнитного поля источника в толще экрана, обладающего малым магнитным сопротивлением для постоянного тока и в области низких частот

8. Укажите особенно опасные нежелательные излучения

1. побочные электромагнитные излучения (ПЭМИ)

2. внеполосные

3. шумовые

9. Установка экранирующих устройств может производиться

1. в непосредственной близости от источника излучения

2. на самом источнике

3. оба варианта верны

10. Паразитные емкостные связи обусловлены

1. электрической емкостью между элементами, деталями и проводниками устройств, несущих потенциал сигнала

2. наличием взаимоиндукции между проводниками и деталями аппаратуры, главным образом между его трансформаторами

3. возникновением между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами и резонансной частотой определенного порядка

11. Укажите, верно ли утверждение: Применение коаксиальных кабелей и волоконно-оптических линий практически полностью решает проблему защиты цепей и трактов линий связи от взаимного влияния.

1. Да

2. Нет

**Модуль 4.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

**Тема 4.1.** Основные понятия обработки персональных данных

1. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц - это

1. Распространение персональных данных

2. Уничтожение персональных данных

3. Обезличивание персональных данных

4. Предоставление персональных данных

2. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

1. Распространение персональных данных

2. Уничтожение персональных данных

3. Обезличивание персональных данных

4. Предоставление персональных данных

3. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию

1. по достижении целей обработки

2. в случае утраты необходимости в достижении этих целей

3. в случае обнаружения ошибки ввода данных

4. в случае использования персональных данных в другой информационной системе

4. Укажите, верно ли утверждение: Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных.

1. Да

2. Нет

5. Укажите, верно ли утверждение: Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано получать согласие субъекта персональных данных на обработку его персональных данных.

1. Да

2. Нет

6. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет

1. оператор

2. лицо, осуществляющее обработку персональных данных по поручению оператора

3. ответственность не определена

**Тема 4.2.** Субъект персональных данных

1. Укажите, верно ли утверждение: Субъект персональных данных не 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.

1. Да

2. Нет

2. Сведения предоставляются субъекту персональных данных или его представителю оператором в течение

1. десяти рабочих дней с момента обращения

2. пяти рабочих дней с момента обращения

3. трех рабочих дней с момента обращения

3. Срок предоставления сведений субъекту персональных данных или его представителю оператором может быть продлен в случае

1. направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации

2. направления оператором в адрес субъекта персональных данных мотивированного уведомления без указания причин продления срока предоставления запрашиваемой информации

3. не может быть продлен

4. Уведомление с указанием причин продления срока предоставления запрашиваемой информации

5. может быть направлен в форме электронного документа и подписан электронной подписью

6. может быть направлен в форме электронного документа, подпись электронной подписью необязательна

7. не может быть направлен в форме электронного документа

4. Укажите, верно ли утверждение: Согласие на обработку персональных данных не может быть отозвано субъектом персональных данных.

1. Да

2. Нет

5. Укажите, верно ли утверждение: Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

1. Да

2. Нет

**Тема 4.3.** Оператор персональных данных

1. Укажите, верно ли утверждение: Оператор может быть освобожден от обязанности предоставить субъекту персональных данных сведения.

1. Да

2. Нет

2. Перед кем оператор персональных данных несет ответственность?

1. Перед субъектом персональных данных

2. Перед Роскомнадзором

3. Вышестоящей организацией

3. Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных:

1. В течение 3 рабочих дней после начала обработки

2. В течение 10 рабочих дней после начала обработки

3. До начала обработки

4. В течение 7 рабочих дней после начала обработки

4. Укажите, верно ли утверждение: Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по обработке персональных данных.

1. Да

2. Нет

**Тема 4.4.** Меры по обеспечению безопасности персональных данных

1. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться

1. на материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения

2. на любых материальных носителях информации

3. на материальных носителях информации и с обеспечением защиты этих данных от неправомерного или случайного доступа к ним

4. Управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа обеспечивают

5. Меры по управлению доступом

6. Меры по идентификации и аутентификации

7. Меры по ограничению программной среды

2. Обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации обеспечивают

1. Меры по антивирусной защите

2. Меры по ограничению программной среды

3. Меры по обнаружению (предотвращению) вторжений

3. Защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных обеспечивают

1. Меры по защите информационной системы, ее средств, систем связи и передачи данных

2. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных

3. Меры по ограничению программной среды

4. В информационных системах 1 уровня защищенности персональных данных применяются

1. средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса

2. средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса

3. средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса

5. В информационных системах 4 уровня защищенности персональных данных применяются

1. средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса

2. средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса

3. средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 6 класса

6. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать:

1. Управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа

2. Присвоение субъектам и объектам доступа уникального признака, сравнение предъявляемого субъектом (объектом) доступа уникального признака с перечнем присвоенных уникальных признаков

7. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1. Уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных

2. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных

3. Правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также процедуру регистрации и учета всех действий

**Тема 4.5.** Обработка персональных данных

1. В случае изменений сведений в оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных обо всех произошедших за указанный период изменениях

1. не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения

2. не позднее 30-го числа месяца, следующего за месяцем, в котором возникли такие изменения

3. не позднее 3-го числа месяца, следующего за месяцем, в котором возникли такие изменения

2. В случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение

1. 10 рабочих дней с даты прекращения обработки персональных данных

2. 30 рабочих дней с даты прекращения обработки персональных данных

3. 5 рабочих дней с даты прекращения обработки персональных данных

3. Уполномоченный орган по защите прав субъектов персональных данных вносит сведения реестр операторов в течение

1. 30 дней с даты поступления уведомления об обработке персональных данных

2. 10 дней с даты поступления уведомления об обработке персональных данных

3. 90 дней с даты поступления уведомления об обработке персональных данных

4. Лицо, ответственное за организацию обработки персональных данных, получает указания

1. от исполнительного органа организации, являющейся оператором

2. от уполномоченного органа по защите прав субъектов персональных данных

5. Лицо, ответственное за организацию обработки персональных данных НЕ обязано:

1. осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных

2. доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных

3. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов

4. осуществлять сбор сведений, относящейся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)

6. Обработка персональных данных считается неавтоматизированной, если такие действия с персональными данными осуществляются

1. при непосредственном участии человека

2. без использования информационной системы

3. без использования персонального компьютера

7. Свойство обезличенных данных, обеспечивающее сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания называется

1. Полнота

2. Структурированность

3. Релевантность

8. Свойство обезличенных данных, обеспечивающее невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации называется

1. Анонимность

2. Структурированность

3. Релевантность

9. Свойство обезличенных данных, обеспечивающее сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания называется

1. Анонимность

2. Структурированность

3. Релевантность

10. Метод обезличивания, заключающийся в разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств называется

1. метод введения идентификаторов

2. метод изменения состава или семантики

3. метод декомпозиции

4. метод перемешивания

11. Укажите метод обезличивания, НЕ обеспечивающий полноту обезличенных данных.

1. Метод изменения состава или семантики

2. Метод введения идентификаторов

3. Метод декомпозиции

12. Укажите метод, который может использоваться совместно с методами введения идентификаторов и декомпозиции

1. Метод перемешивания

2. Метод изменения состава или семантики

**Тема 4.6.** Нарушения законодательства РФ в области персональных данных

1. Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных влечет наложение административного штрафа на должностных лиц в размере

1. от одной тысячи до трех тысяч рублей

2. от пяти тысяч до десяти тысяч рублей

3. от десяти тысяч до двадцати тысяч рублей

4. от тридцати тысяч до пятидесяти тысяч рублей

2. Какой размер штрафа установлен для организации за не опубликование политики по обработке и защите персональных данных?

1. от семисот до одной тысячи пятисот рублей

2. от трех тысяч до шести тысяч рублей

3. от пяти тысяч до десяти тысяч рублей

4. от пятнадцати тысяч до тридцати тысяч рублей

5. от двадцати пяти тысяч до сорока пяти тысяч рублей

3. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных влечет предупреждение или наложение административного штрафа

1. на должностных лиц

2. на юридических лиц

3. на индивидуальных предпринимателей

4. на граждан

4. Нарушение законодательства Российской Федерации в области персональных данных регламентировано

1. КоАП РФ

2. УК РФ

3. ТК РФ

4. НК РФ

5. Укажите, верно ли утверждение: Увольнение работника (при наличии всех признаков дисциплинарного проступка) за разглашение персональных данных НЕ возможно в случае, если он не проконтролировал исполнение требования о хранении персональных данных

1. Да

2. Нет

6. Укажите нормативно-правовой акт, который устанавливает ответственность в случаях превышения должностными лицами работодателя своих полномочий по доступу к информации о частной жизни работника.

1. УК РФ

2. ТК РФ

3. КоАП РФ

7. Укажите нормативно-правовой акт, который устанавливает ответственность за нарушение права работников на свободный бесплатный доступ к своим персональным данным.

8. КоАП РФ

9. УК РФ

10. ТК РФ

**Модуль 5.** Меры безопасности, применяемые при обработке персональных данных в информационных системах

**Тема 5.1.** Типовые программно-технические средства защиты информации

1. Некоторая последовательность символов, сохраняемая в секрете и предъявляемая пользователем при обращении к компьютерной системе:

1. аутентификатор
2. пароль
3. идентификатор

2. Устройство, программа, которые осуществляют фильтрацию данных на основе заранее заданной базы правил:

1. авторизация
2. мониторинг
3. межсетевой экран

3. Основная задача брандмауэра:

1. защита сети от удаленных атак
2. выполняет функцию внешнего маршрутизатора
3. защита от вирусов
4. запрещает доступ к любым другим компьютерам

4. Укажите брандмауэр, позволяющий контролировать тип и объем трафика, поступающего на узел:

1. Брандмауэр сетевого уровня
2. Брандмауэры уровня приложения
3. Брандмауэр уровня соединения

5. Сколько ключей используется в системах с открытым ключом?

1. 1
2. 2
3. 3

6. Электронной подписью называется

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

7. Укажите, верно ли утверждение: В системах электронных платежей применяется «слепая подпись»

1. Да
2. Нет

**Тема 5.2.** Организация защиты персональных данных в организации

1. Укажите наиболее часто встречающуюся формулировку жалобы в области персональных данных на действия работодателя:

1. «распространение информации о работнике третьим лицам»
2. «нарушение права работников на свободный бесплатный доступ к своим персональным данным»
3. «несвоевременное предоставление запрошенной информации»

2. Какой нормативно-правовой акт закрепляет права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя:

1. ТК РФ
2. УК РФ
3. КоАП РФ

3. В каком случае работодатель вправе разглашать персональные данные работника третьей стороне или в коммерческих целях

1. если работник дал устное согласие
2. если работник дал письменное согласие
3. если работник дал письменное согласие, заверенное нотариусом

4. Работодатель не нарушит права работника в сфере персональных данных если передал персональные данные работника:

1. в пределах одной организации
2. по мотивированному запросу только специально уполномоченным лицам
3. новому работодателю
4. в пределах организаций партнеров

5. Являются ли следующие сведения о сотрудниках: фамилии, имена и отчества, занимаемые ими должности, с указанием структурных подразделений, сведения о номерах корпоративных и внутренних телефонов, адреса их электронной почты персональными данными?

1. Да
2. Нет