

УТВЕРЖДАЮ
Президент ООО «Ц-А-Р-М»

_____ М.С.Мельников
«__» _____ 2021 г.

**ДОПОЛНИТЕЛЬНАЯ
ПРОФЕССИОНАЛЬНАЯ
ПРОГРАММА**

**ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ ДАННЫХ»**

**г. Тверь
2021г.**

СОДЕРЖАНИЕ

| | |
|---|----|
| 1. ОБЩИЕ ПОЛОЖЕНИЯ | 3 |
| 1.1. Нормативные правовые основания разработки программы | 3 |
| 1.2. Цель и планируемые результаты обучения | 4 |
| 1.3. Категория слушателей | 4 |
| 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ | 5 |
| 2.1. УЧЕБНЫЙ ПЛАН | 5 |
| 2.2. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК..... | 6 |
| 2.3. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ ПРЕДМЕТОВ | 6 |
| 3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ | 10 |
| 3.1. Требования к квалификации педагогических кадров | 10 |
| 3.2. Требования к материально-техническим условиям..... | 10 |
| 3.3. Требования к информационным и учебно-методическим условиям | 10 |
| 3.4. Общие требования к организации образовательного процесса..... | 10 |
| 4. ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ | 11 |
| 5. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ..... | 13 |
| КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ..... | 18 |

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Нормативные правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

- ФЗ РФ от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
- Приказ Минтруда России от 01.11.2016 N 598н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей"

Программа реализуется исключительно с применением дистанционных образовательных технологий (ДОТ), понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Для реализации Программы с применением дистанционных образовательных технологий созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств и обеспечивающей освоение обучающимися образовательных программ в полном объеме независимо от места нахождения обучающихся.

Местом осуществления образовательной деятельности является место нахождения ООО «Ц-А-Р-М» независимо от места нахождения обучающихся.

Для реализации Программы дистанционных образовательных технологий ООО «Ц-А-Р-М» обеспечивает защиту сведений, составляющих государственную или иную охраняемую законом тайну.

Обучение по Программе осуществляется на основе договора об образовании, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение.

Базовые требования к содержанию программы/

Планируемые результаты обучения.

Слушатели, освоившие Программу обучения должны обладать следующими компетенциями.

Знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- правовые основы организации защиты информации,
- принципы и методы организационной защиты информации;

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- пользоваться нормативными документами по защите информации;
- использовать в практической деятельности правовые знания;
- анализировать основные правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности.

Владеть:

- навыками работы с нормативными правовыми актами в сфере экономической и информационной безопасности;
- навыками компьютерной обработки служебной документации, статистической информации; работы с информационно-поисковыми и информационно-справочными системами и базами данных, используемыми профессиональной деятельности;
- навыками организации и обеспечения режима секретности;
- навыками обоснования, выбора, реализации и контроля результатов управленческого решения.

1.2. Цель и планируемые результаты обучения

Целью реализации программы является подготовка слушателей и (или) повышение профессионального уровня в рамках имеющейся квалификации, направленные на совершенствование и (или) получение ими новой компетенции, необходимой для профессиональной деятельности в сфере информационной безопасности.

1.3. Категория слушателей

К освоению дополнительных профессиональных программ допускаются:

- 1) лица, имеющие среднее профессиональное и (или) высшее образование;
- 2) лица, получающие среднее профессиональное и (или) высшее образование.

(Согласно части 4 статьи 76 Федерального закона от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»).

1.4. Срок обучения: 21 час.

Форма обучения: заочная, с использованием электронного обучения и дистанционных образовательных технологий.

Режим занятий: 8 часов в день

1.5. Освоение Программы завершается итоговой аттестации слушателей в форме компьютерного тестирования. Лицам, успешно освоившим Программу и прошедшим итоговую аттестацию, выдаются удостоверения о повышении квалификации.

Образец удостоверения о повышении квалификации устанавливается ООО «Ц-А-Р-М» самостоятельно.

1.6. Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из ООО «Ц-А-Р-М», выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому ООО «Ц-А-Р-М».

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ

Структура и содержание программы представлены учебным планом, календарным учебным графиком, рабочими программами по учебным предметам

2.1. УЧЕБНЫЙ ПЛАН

Вид образования – дополнительное образование.

Подвид - дополнительное профессиональное образование.

Программа – повышение квалификации.

Наименование – «Организация и обеспечение защиты персональных данных»

Категория обучающихся – Лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование.

Срок обучения – 3 дня.

Форма обучения – заочная (заочная часть реализуется через ДОТ и ЭО).

Режим занятий – 8 часов в день

| № п/п | Наименование модулей | Всего часов | в том числе | | | Форма контроля (форма аттестации) |
|----------|---|----------------|------------------------------|-----------------------------|-------------------------------|---|
| | | | теорети ческие занятия | практич еские занятия | самостоя тельная работа | |
| | | | | | | |
| 1. | Модуль 1. Общие вопросы технической защиты информации | 4 | 4 | - | - | Тестирование |
| 2. | Модуль 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных | 14 | 14 | - | - | Тестирование |
| | Консультации | 1 | 1 | - | - | Тестирование |
| | Итоговая аттестация | 2 | 2 | - | - | Тестирование |
| | Итого | 21 | 21 | - | - | |

2.2. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график определяет количество учебных недель в соответствии с трудоемкостью и сроком освоения программы, а также понедельное распределение учебной нагрузки на обучающегося. Дата начала и окончания обучения устанавливаются по мере комплектации групп в течение всего календарного года.

| № п/п | Наименование учебных модулей | Порядковые номера недель календарного года | | Всего час. |
|----------|---|---|----------|---------------|
| | | 1 неделя | 2 неделя | |
| 1. | Модуль 1. Общие вопросы технической защиты информации | 4 | - | 4 |
| 2. | Модуль 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных | 14 | - | 14 |
| 3. | Консультации | 1 | - | 1 |
| 4. | Итоговая аттестация | 2 | - | 2 |
| 5. | Итого | 21 | - | 21 |

2.3. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ ПРЕДМЕТОВ

ТЕМАТИЧЕСКИЙ ПЛАН УЧЕБНОГО ПРЕДМЕТА «Общие вопросы технической защиты информации»

| № п/п | Наименование тем | Количество часов |
|----------|---|---------------------|
| 1. | Правовые и организационные основы технической защиты информации ограниченного доступа | 2 |
| 2. | Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа | 2 |
| | Итого | 4 |

ПРОГРАММА ПРЕДМЕТА

Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа

Основные понятия в области технической защиты информации (ТЗИ). Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи, полномочия и права управлений ФСТЭК России по федеральным округам.

Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.

Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации.

Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

ТЕМАТИЧЕСКИЙ ПЛАН УЧЕБНОГО ПРЕДМЕТА
«Организация обеспечения безопасности персональных данных в информационных системах

персональных данных»

| № п/п | Наименование тем | Количество часов |
|-------|--|------------------|
| 1. | Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 6 |
| 2. | Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 6 |
| 3. | Практические реализации типовых моделей защищенных информационных систем обработки персональных данных | 2 |
| | Итого | 14 |

ПРОГРАММА ПРЕДМЕТА

Тема № 1. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Особенности информационного элемента информационной системы персональных данных.

Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.

Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневой, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.

Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.

Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.

Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.

Основные требования и рекомендации по защите речевой информации,

циркулирующей в защищаемых помещениях.

Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

Тема №2. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.

Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.

Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.

Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.

Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации.

Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.

Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Тема № 3. Практические реализации типовых моделей защищённых информационных систем обработки персональных данных

Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или

модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных.

Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.

Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к квалификации педагогических кадров

Организационно-педагогические условия реализации Программы должна обеспечивать ее реализацию в полном объеме, соответствие качества подготовки обучающихся установленным требованиям.

Обучение проводится в оборудованном учебном кабинете.

Наполняемость учебной группы не должна превышать 25 человек.

Продолжительность учебного часа занятий составляет 1 академический час (45 минут) - 8 учебных часов в день.

Преподаватели должны иметь высшее образование или среднее профессиональное образование по направлению подготовки «Образование и педагогика» или в области, соответствующей преподаваемому предмету, без предъявления требований к стажу работы либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы или преподаватели должны иметь диплом о профессиональной переподготовке по направлению соответствующему преподаваемому предмету.

3.2. Требования к материально-техническим условиям

Материальные ресурсы (требования к оснащению аудитории):

- Программное обеспечение.
- Лекционные занятия проводятся в аудитории, оснащенной мультимедийным комплексом.

Учебный процесс обеспечен техническими средствами:

- персональными компьютерами с выходом в сеть Интернет;
- принтер сканер копир;
- мультимедийным оборудованием (проектор);
- СДО-ПРОФ-программа дистанционного обучения.

Для реализации учебного процесса используется учебный класс с компьютерами, объединенных в локальную сеть с выходом в Интернет.

3.3. Требования к информационным и учебно-методическим условиям

Методическое обеспечение образовательной программы:

- Комплекс учебных материалов (презентации к занятиям, учебные задания, тесты и др. материалы).

Виды учебных занятий и используемые технологии:

Учебный процесс предусматривает при реализации комплексного подхода использование в образовательном процессе активных форм проведения занятий.

3.4. Общие требования к организации образовательного процесса

К освоению программы допускаются лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование.

В процессе обучения особое внимание должно быть обращено на необходимость прочного усвоения и выполнения всех требований безопасности труда в соответствии с действующими нормативно - техническими документами.

В результате обучения слушатели приобретают знания, навыки и практические умения, необходимые для качественного совершенствования профессиональных компетенций.

4.ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Во время обучения проводится промежуточная аттестация обучающихся в форме дифференцированного зачета.

Освоение дополнительных профессиональных образовательных программ завершается итоговой аттестацией обучающихся (Часть 14 статьи 76 ФЗ от 29 декабря 2012 г. N 273-ФЗ «Об образовании в РФ»).

Итоговая аттестация проводится в форме зачета.

Формы промежуточной и итоговой аттестации

| № п/п | Наименование модулей | Форма промежуточной аттестации | Методы контроля |
|-------|---|---------------------------------|-----------------------------|
| 1. | Модуль 1. Общие вопросы технической защиты информации | <i>Дифференцированный зачёт</i> | тестовый контроль |
| 2. | Модуль 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных | <i>Дифференцированный зачёт</i> | тестовый контроль |
| | Консультации | | В виде собеседования |
| | Итоговая аттестация | <i>Зачет</i> | Тестирование |

Задания выполняются слушателями в произвольной последовательности. После проверки выполнения индивидуальных заданий и внесения исправлений (в случае необходимости), начинается защита слушателем выполненного задания в форме собеседования. Дополнительные вопросы задаются по схеме: одно задание - один дополнительный вопрос. Ответы оцениваются по четырёхбалльной системе.

Промежуточная аттестация по модулям проходит в форме тестирования. Результаты промежуточной аттестации заносятся в Итоговую (зачётную) ведомость учебного цикла в виде процента результативности и оценки по четырёх балльной системе.

Критерии оценки тестового контроля и итоговой аттестации по модулям

| Процент результативности (правильных ответов) | Качественная оценка индивидуальных образовательных достижений |
|---|---|
| | балл (отметка) |
| 91 ÷ 100% | 5 |
| 86 ÷ 90% | 4 |
| 80 ÷ 85% | 3 |
| менее 80% | 2 |

Критерии оценки тестового контроля по модулям

Оценка 5 (отлично) – комплексная оценка предложенной ситуации, знание теоретического материала с учетом междисциплинарных связей, правильный выбор тактики действий, последовательное, уверенное выполнение практических манипуляций, в соответствии с алгоритмами действий.

Оценка 4 (хорошо) – комплексная оценка предложенной ситуации, незначительные затруднения при ответе на теоретические вопросы, неполное раскрытие междисциплинарных связей, правильный выбор тактики действий, логическое обоснование дополнительных теоретических вопросов педагога, последовательное, уверенное выполнение практических манипуляций.

Оценка 3 (удовлетворительно) – затруднения с комплексной оценкой предложенной ситуации; неполный ответ, требующий наводящих вопросов педагога; правильное последовательное, но неуверенное выполнение манипуляций.

Оценка 2 (неудовлетворительно) – неверная оценка ситуации; неправильно выбранная тактика действий, приводящая к неправильным результатам.

Критерии и параметры оценки результатов итоговой аттестации:

Основным критерием при оценке является степень соответствия знаний и демонстрируемых умений, установленным правилам, алгоритмам, стандартам и нормативным документам.

При проведении экзамена в тестирования выставляются отметки по четырех бальной системе («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»):

-отметка «неудовлетворительно» выставляется слушателю, не показавшему освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, допустившему серьезные ошибки в выполнении предусмотренных программой заданий

-отметку «удовлетворительно» заслуживает слушатель, показавший частичное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, сформированность не в полной мере новых компетенций и профессиональных умений для осуществления профессиональной деятельности, знакомый с литературой по программе.

-отметку «хорошо» заслуживает слушатель, показавший освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, изучивших литературу, рекомендованную программой, способный к самостоятельному пополнению и обновлению знаний в ходе дальнейшего обучения и профессиональной деятельности;

-отметку «отлично» заслуживает слушатель, показавший полное освоение планируемых результатов (знаний, умений, компетенций), всестороннее и глубокое изучение литературы; умение выполнять задания с привнесением собственного видения проблемы, собственного варианта решения практической задачи, проявивший творческие способности в понимании и применении на практике содержания обучения.

Критерии оценки практической работы

Знания и умения обучающихся определяются «зачтено» («зачет») или незачет.

Оценка «Зачет» за практическую работу по программе повышения квалификации ставится при правильном выполнении работы не менее чем на 75%.

Оценка «Незачет» за практическую работу по программе повышения квалификации ставится при правильном выполнении работы менее чем на 70%.

Примеры тестовых заданий приведены в приложение №1.

5. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Нормативно-правовые документы:

1. «Конституция Российской Федерации», принята всенародным голосованием 12 декабря 1993г.
2. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1.
3. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом РФ 5 декабря 2016г. №646.
4. Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation

Кодексы:

5. «Уголовный кодекс Российской Федерации», принят Федеральным законом от 13 июня 1996г. № 63-ФЗ.
6. «Кодекс Российской Федерации об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195-ФЗ.
7. «Трудовой кодекс Российской Федерации», принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.

Федеральные законы:

8. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
10. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
11. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».
12. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».
14. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».
15. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».
16. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».

Указы Президента Российской Федерации:

17. Указ Президента Российской Федерации от 12 мая 2009г. №537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
18. Указ Президента Российской Федерации от 6 марта 1997г № 188 «Об утверждении перечня сведений конфиденциального характера».
19. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
20. Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно телекоммуникационных сетей международного информационного обмена».

Постановления Правительства Российской Федерации:

21. Постановление Правительства Российской Федерации от 16 марта 2009г.

- №228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
22. Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
23. Постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства Российской Федерации от 6 июля 2008г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
25. Постановление Правительства Российской Федерации от 4 марта 2010г. №125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».
26. Постановление Правительства Российской Федерации от 16 апреля 2012г. №313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
27. Постановление Правительства Российской Федерации от 3 марта 2012г. №171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
28. Постановление Правительства Российской Федерации от 3 февраля 2012г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации».
29. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. №912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).
30. Постановление Правительства Российской Федерации от 21 марта 2012г. №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».
- Нормативные документы ФСТЭК России:
31. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.
32. «Меры защиты информации в государственных информационных системах»,

- методический документ, утвержден ФСТЭК России 11 февраля 2013г.
33. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.
 34. «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18 февраля 2013г. № 21.
 35. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.
 36. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995г. № 199.
 37. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.
 38. «Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации», утверждены заместителем директора ФСТЭК России 25 апреля 2006г.
 39. «Сборник временных методик оценки защищённости конфиденциальной информации, обрабатываемой техническими средствами и системами», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 2001г.
 40. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
 41. «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
 42. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
 43. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
 44. «Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», утвержден решением председателя Гостехкомиссии России от 30 марта 1992г.
 45. «Руководящий документ. Требования к межсетевым экранам. Приказ ФСТЭК России от 9 февраля 2016 г. № 9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный № 41564).
 46. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.
 47. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора

ФСТЭК России 19 ноября 2007г.
Нормативные документы ФСБ России:

48. Приказ ФСБ от 10 июля 2014 г. №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».
49. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).
50. Приказ ФСБ России от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
51. Приказ ФАПСИ России от 13 июня 2001г. № 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 содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

Стандарты:

52. ГОСТ Р 51275-06. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», принят и введен в действие Постановлением Госстандарта Российской Федерации от 1 февраля 2008г.
53. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»
54. ГОСТ Р ИСО/МЭК 15408-1-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Госстандарт России.
55. ГОСТ Р ИСО/МЭК 15408-2-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности». Госстандарт России.
56. ГОСТ Р ИСО/МЭК 15408-3-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности». Госстандарт России.
57. ГОСТ Р 50922-06. «Защита информации. Основные термины и определения».
58. ГОСТ Р ИСО/МЭК 27002. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
59. ГОСТ Р ИСО/МЭК 27002 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
60. ГОСТ Р ИСО/МЭК 27003 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».

в) базы данных, информационно-справочные и поисковые системы:

1. <https://bdu.fstec.ru/threat> База данных угроз безопасности информации на сайте ФСТЭК России;
2. Официальный портал персональных данных (Роскомнадзор)
<http://rkn.gov.ru/personal-data/portal>

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Комплект контрольно-оценочных средств включает в себя примерные тестовые задания для проверки знаний.

На каждый вопрос предлагается вариант ответов, один (или несколько) из которых является правильным.

1.Автоматизированная обработка персональных данных - это

А. Обработка персональных данных с использованием средств автоматизации

В. Обработка персональных данных с помощью средств вычислительной техники

С. Обработка персональных данных пользователя с применением компьютера

2.Информационная система персональных данных - это

А. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

В. Пользователь, средства автоматизации, базы данных

С. Контролируемое пространство, в котором происходит обработка персональных данных

3.Целью Федерального закона от 27.07.2006 № 152-ФЗ является

А. Контроль за обработкой персональных данных операторами персональных данных

В. Соответствия законодательства РФ в сфере персональных данных Конвенции Совета Европы от 1981 года

С. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну

4.Что понимается под понятием «Конфиденциальность персональных данных»?

А. Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных

В. Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом

С. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.Оператор при сборе персональных данных через свой официальный сайт обязан в соответствии с ч.2 ст.18.1 152-ФЗ на сайте опубликовать документы:

А. Политику в отношении обработки персональных данных

В. Политику в отношении обработки персональных данных + Пользовательское соглашение

С. Политику в отношении обработки персональных данных + Пользовательское соглашение + Согласие пользователя

6.Что такое персональные данные?

А. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

В. Информация о частной жизни физического лица, доступ к которой он решил ограничить

С. Сведения о религиозных убеждениях, политических взглядов, расовой и национальной принадлежности субъекта персональных данных

7.Оператор персональных данных - это

А. Государственный орган, осуществляющий автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке

В. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

С. Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке

8.Обработка персональных данных - это

А. Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, осуществляемые с помощью средств вычислительной техники

В. Чтение, запись, сортировка, модификация, передача персональных данных в информационной системе

С. Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

9.Распространение персональных данных - это

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

В. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц

С. Передача персональных данных оператору персональных данных

10.Предоставление персональных данных - это

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

В. Действия, направленные на раскрытие персональных данных по мотивированному запросу

11.Уничтожение персональных данных - это

А. Действия, в результате которых становится невозможно определить субъекта персональных данных в информационной системе персональных данных

В. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

С. Удаление персональных данных из информационной системы персональных данных

12.Обезличивание персональных данных – действия, в результате которых

А. Становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

В. Невозможно распространять персональные данные

С. Выполняется уничтожение персональных данных в информационной системе

13.Каким нормативно-правовым актом Российской Федерации установлены «Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных»

А. Постановлением Правительства РФ от 13 февраля 2019 г. № 146

В. Приказом Минкомсвязи РФ от 21 января 2019 г. № 10

С. Приказом Роскомнадзора от 30 октября 2018 г. № 159

14.Какие меры по обеспечению безопасности персональных данных при неавтоматизированной обработке являются обязательными в соответствии с постановлением Правительства РФ от 15.09.2008г. № 687?

А. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

В. Использование средств контроля и управления доступом

С. Должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором

15. Какой размер штрафа установлен для организации по ст. 13.11.КоАП за не опубликование политики по обработке и защите персональных данных?

А. 10000 – 15000 рублей

В. 30 000 – 60 000 рублей

С. 20 000 – 50 000 рублей

16. Может ли являться оператором персональных данных физическое лицо?

А. Да

В. Нет

17. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, относятся:

А. К биометрическим персональным данным

В. К специальной категории персональных данных

18. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?

А. биометрические

В. общедоступные

С. специальные