ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

**«АГЕНТСТВО ИННОВАЦИОННОГО РАЗВИТИЯ»**

Директор

ООО «Агентство инновационного развития»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Тагаев

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**ПАСПОРТ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**«Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»**

г. Ростов-на-Дону, 2020 г.

**ПАСПОРТ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**«Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»**

|  |  |
| --- | --- |
| **Версия программы** | **2** |
| **Дата Версии** | **20.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Общество с ограниченной ответственностью «Агентство инновационного развития» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 6167073166 |
| 1.4 | Ответственный за программу ФИО | Ганеева Валерия Маратовна |
| 1.5 | Ответственный должность | заместитель директора ООО «Агентство инновационного развития» |
| 1.6 | Ответственный Телефон | 89064540439 |
| 1.7 | Ответственный Е-mail | v.m.ganeeva@mail.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы» |
| 2.2 | Ссылка на страницу программы | **http://indistant.ru/** |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | ***да*** |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | 72 |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 40 академических часов – практическая работа  32 академических часа – лекционная работа |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | стоимость обучения – 25 000 рублей  <https://udcs.ru/obrazovanie/programma-povysheniya-kvalifikatsii-zashchita-konfidentsialnoy-informatsii-v-organizatsii.php>  <http://atcenter.ru/services/obuchenie-po-informatsionnoj-i-transportnoj-bezopasnosti/>  <https://www.academyit.ru/deals/deal/actions/programma-povysheniya-kvalifikatsii-po-zashchite-personalnykh-dannykh-tryekhdnevnyy-intensivnyy-kurs/>  <http://www.fsb-fstec.ru/>?  **https://infobezopasnost.ru/informacionnaya-bezopasnost-kii/** |
| 2.7 | Минимальное количество человек на курсе | 100 |
| 2.8 | Максимальное количество человек на курсе | 10000 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | - |
| 2.10 | Формы аттестации | - промежуточное тестирование по результатам прохождения образовательных модулей;  - практические задания по результатам прохождения образовательного модуля;  - итоговая аттестация (экзамен в форме тестирования) |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Новые экономические и технологические условия требуют создания и реализации подходов по содействию гражданам в освоении ключевых компетенций цифровой экономики, обеспечении массовой цифровой грамотности и персонализации процесса образования. В этой связи становится актуальным развитие и совершенствование востребованных в цифровой экономике компетенций, в частности организация процесса защиты информации и сохранения персональных данных.

Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» все юридические и физические лица, использующие в своей деятельности персональные данные, должны осуществить мероприятия по их защите. Комплекс услуг по приведению систем защиты информации и персональных данных в соответствии с законодательством Российской Федерации подразумевает следующие базовые этапы: аудит информационных систем по обработке персональных данных (включая аудит локально-вычислительных сетей), разработка организационно-распорядительной документации, поставка и установка необходимых технических средств защиты информации, разработка и внедрение политики безопасности организации.

Система информационной безопасности центров предоставления государственных и муниципальных услуг – многокомпонентная система мер по защите данных, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения или внесения изменений в конфигурацию системы. Центры «Мои документы» производят сбор и обработку персональных данных с целью оказания государственных (муниципальных) услуг, кадрового обеспечения деятельности организации, выполнения условий трудовых договоров, начисления заработной платы, подготовки и передачи налоговой отчетности, формирования документов индивидуального (персонифицированного) учета и других действий, предусмотренных действующим законодательством Российской Федерации. Следовательно, система информационной безопасности центров «Мои документы» должна не только обеспечивать сохранность баз данных и содержащихся в них массивов конфиденциальных сведений, но и осуществлять постоянное обновление ее компонентов, а также совершенствование компетенций ее операторов. При этом, специалисты, занимающиеся обработкой данных, а также администраторы информационных систем несут ответственность за их несанкционированную утечку или разглашение персональных данных сотрудников и заявителей центров «Мои документы».

В связи с вышеизложенным прохождение повышения квалификации по тематике обеспечения информационной безопасности и защиты персональных данных является важным и необходимым элементом развития общего уровня компетенций сотрудников, а также необходимым условием для цифровизации системы предоставления государственных и муниципальных услуг.

Дополнительная профессиональная программа повышения квалификации «Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы» разработана ООО «Агентство инновационного развития» совместно с экспертами компании ООО «ЭнигмаДон». Целью данной программы является приобретение, совершенствование и обновления компетенций, а также структуризация знаний специалистов, работающих в центрах «Мои документы», в области организации процесса защиты информации и построения системы информационной безопасности. Необходимость в повышении квалификации по данной программе связана также с требованием периодического обновления теоретических и практических знаний специалистов, занимающихся обработкой информации.

В процессе обучения слушателям предстоит изучить общие положения обеспечения информационной безопасности и защиты персональных центров «Мои документы», а также ознакомится порядком обеспечения информационной безопасности и защиты персональных данных в СМЭВ и при использовании ЕСИА, порядком хранения и использования электронной цифровой подписи в деятельности центров «Мои документы», использование систем электронного документооборота, взаимодействие центров «Мои документы» с государственными органами, осуществляющими контроль деятельности в области защиты информации.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

**«АГЕНТСТВО ИННОВАЦИОННОГО РАЗВИТИЯ»**

Директор

ООО «Агентство инновационного развития»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Тагаев

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА**

**повышения квалификации**

**«Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»**

г. Ростов-на-Дону, 2020 г.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

приобретение и совершенствование имеющихся компетенций, необходимых для профессиональной деятельности организации информационной безопасности центрах предоставления государственных и муниципальных услуг. Программа повышения квалификации «Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы» поможет начинающим специалистам в области обеспечения информационной безопасности, а также действующим экспертам приобрести и усовершенствовать знания в области порядка организации защиты информации и персональных данных центрах предоставления услуг, а также ознакомится механизмом обеспечения информационной безопасности и защиты персональных данных в интегрированных информационных системах МФЦ, получить практические рекомендации по организации системы защиты информационной безопасности в центрах «Мои документы».

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

- основных понятий в области информационной безопасности и защиты персональных данных;

- перечень основных законодательных актов, регулирующих вопросы защиты информации в Российской Федерации, а также дополнительные руководящие документы, приказы и стандарты, регламентирующие различные аспекты информационной безопасности и защиты персональных данных;

- основных целей и задач систем защиты информации в организациях (системы электронного документооборота, бухгалтерские и кадровые системы);

- интегрированные информационная система, обеспечивающая функционирования деятельности многофункциональных центров предоставления услуг; основные компоненты и модули информационных систем МФЦ, необходимость информационной защиты данных в каждом из модулей;

- получение статуса оператора обработки персональных данных, действие или совокупность действий, совершаемых с использованием средств автоматизации или без них с персональными данными заявителей.

2.2. Умение (способность к деятельности)

- выполнения обязанностей оператора обработки и защиты информации в соответствии с требованиями законодательства и рекомендациями федеральных органов власти;

- осуществления документирования процессов по защите информации с построение системы уровневой иерархии;

- предотвращать все виды информационных угроз в организациях, обеспечивать идентификацию/ аутентификацию пользователя во внутренних системах обеспечения функционирования образовательного учреждения, обеспечивать защиту оборудования и технических средств системы, помещения, где они размещаются, от утечки конфиденциальной информации по техническим каналам;

- разрабатывать инструкции, правила и порядок работы с документацией, регламентирующей защиту информации и персональных данных обучающихся и сотрудников; разрабатывать методические документы, контролировать эффективность принимаемых мер по обеспечению информационной безопасности;

- определить необходимые и достаточные меры защиты информации в деятельности центров «Мои документы»; размещать и устанавливать АРМ и серверы.

2.3.Навыки (использование конкретных инструментов)

- организации комплекса мер по защите информации, отвечающего требования законодательства в области защиты информации и сохранения целостности персональных данных;

- разработки модели угроз безопасности персональных данных для конкретной организации на основании требований ФСТЭК;

- формирования и ведение информационной системы, в том числе внесение в нее сведений, навыками осуществления технологического и информационного взаимодействия, разработки организационно-распорядительной и технической документации, необходимой для аттестации рабочего места;

- проведения первичных и контрольных информационных обследований подразделения организации, а также внутреннего аудита, проверки, выполнения требований нормативных документов по технической защите информации;

- навыками организации и поддержания безопасного рабочего места сотрудника центра «Мои документы», использующего цифровую подпись.

**3.Категория слушателей** (возможно заполнение не всех полей)

* 1. Граждане, имеющие высшее или среднее профессиональное образование.
  2. Общий стаж трудовой деятельности не менее 1 года.

**4.Учебный план программы** «Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»

| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| --- | --- | --- | --- | --- | --- |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Общие положения обеспечения информационной безопасности и защиты персональных данных | 29 | 12 | 12 | 5 |
| 2 | Порядок организации защиты информации в деятельности  центров «Мои документы» | 41 | 20 | 16 | 5 |
| **Итоговая аттестация** | | **2** | **экзамен в форме тестирования** | | |
| **ИТОГО** | | **72** |  | | |

**5.Календарный план-график реализации образовательной программы**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Общие положения обеспечения информационной безопасности и защиты персональных данных | **29** | **02.11.2020 – 06.11.2020** |
| 2 | Порядок организации защиты информации в деятельности центров «Мои документы» | **41** | **07.11.2020 – 16.11.2020** |
|  | **Итоговая аттестация** | **2** |
| **Всего:** | | **72** | **02.11.2020 – 16.11.2020** |

**6.Учебно-тематический план программы** «Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»

| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| --- | --- | --- | --- | --- | --- |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **Модуль 1. Общие положения обеспечения информационной безопасности и защиты персональных данных** | | **29** | **12** | **12** | **5** |
| 1. | Понятие информационной безопасности в условиях цифровой трансформации общества | **4** | 3 | - | 1 |
| 2. | Обеспечение безопасности персональных данных | **4** | 3 | - | 1 |
| 3. | Нормативно-правовое регулирование и организационные основы защиты информации | **4** | 1 | - | 3 |
| 4. | Контроль за соблюдение мер по обеспечению информационной безопасности и виды ответственности за нарушения в сфере защиты информации | **3** | 1 | 2 | - |
| 5. | Порядок осуществления защиты информации и персональных данных в организациях | **3** | 1 | 2 | - |
| 6. | Правила разработки модели защиты от внешних информационных угроз организации и порядок ее внедрения | **3** | 1 | 2 | - |
| 7. | Разработка организационно-распорядительной документации и документальное сопровождение вопросов защиты информации | **6** | 1 | 5 | - |
| 8. | Оценка эффективности мер по защите информации | **2** | 1 | 1 | - |
| **Модуль 2. Порядок организации защиты информации в деятельности**  **центров «Мои документы»** | | **41** | **20** | **16** | **5** |
| 1. | Обеспечение информационной безопасности и защиты персональных данных при использовании ЕСИА | **1** | 1 |  |  |
| 2. | Механизмы обеспечения информационной безопасности и защиты персональных данных в интегрированных информационных системах МФЦ | **6** | 2 | 2 | 2 |
| 3. | Порядок обеспечения информационной безопасности и защиты персональных данных в СМЭВ | **3** | 1 | 2 |  |
| 4. | Выпуск и применение электронной цифровой подписи в деятельности центров «Мои документы» | **4** | 2 | 2 |  |
| 5. | Использование систем электронного документооборота в деятельности центров предоставления услуг в том числе в использовании СМЭВ | **4** | 2 | 2 |  |
| 6. | Порядок обработки и защиты персональных данных заявителей центров «Мои документы» | **5** | 2 | 2 | 1 |
| 7. | Порядок обработки, защиты и хранения персональных данных сотрудников центров «Мои документы» | **4** | 2 | 2 |  |
| 8. | Организация информационной безопасности в системах бухгалтерского учета и работы кадровых служб центров «Мои документы» | **2** | 2 |  |  |
| 9. | Практические рекомендации по организации системы защиты информационной безопасности в центрах предоставления государственных и муниципальных услуг | **6** | 2 | 2 | 2 |
| 10. | Взаимодействие центров «Мои документы» государственными органами, осуществляющими контроль деятельности в области защиты информации | **4** | 2 | 2 |  |
| 11. | Обзор практики проведения проверок в области защиты информации | **2** | 2 |  |  |
| **Итоговая аттестация** | | **2** | **Экзамен в форме тестирования** | | |
| **ИТОГО** | | **72** |  | | |

**7. Учебная (рабочая) программа повышения квалификации** «Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»

**Модуль** **1. Общие положения обеспечения информационной безопасности и защиты персональных данных (29 часов)**

**Тема 1. Понятие информационной безопасности в условиях цифровой трансформации общества (4 часа)**

Основные понятия и термины, используемые в информационной безопасности: защита информации, объекты и цели защиты информации, эффективность защиты информации, защита информации от утечки, защита информации от разглашения, защита информации от несанкционированного доступа, система защиты информации, информационная безопасность, угроза безопасности автоматизированных систем, защищенная система, способы и средства защиты информации, комплекс средств защиты и техника защиты информации, угроза информации, несанкционированный доступ. Автоматизированная система и основные ее компоненты. Задачи информационной безопасности. Угрозы информационной безопасности и классификация видов угроз информационной безопасности. Ошибка пользователя. Несанкционированный доступ: понятия, виды, способы защиты.

**Тема 2. Обеспечение безопасности персональных данных (4 часа)**

Персональные данные физического лица: понятия, виды, обработка данных и субъекты обработки персональных данных. Информационная система обработки персональных данных, классификация систем на основе исходных данных. Категории обрабатываемых в информационной системе персональных данных. Типовые и специализированные информационные системы обработки персональных данных. Классы информационных систем. Мероприятия по защите персональных данных при их обработке в информационных системах от несанкционированного доступа и неправомерных действий. Средства антивирусной защиты.

**Тема 3. Нормативно-правовое регулирование и организационные основы защиты информации (4 часа)**

Перечень основных законодательных актов, регулирующих вопросы защиты информации. Обзор Конституции РФ является основным источником права в области обеспечения информационной безопасности в России. Обзор Федерального закона «Об информации, информатизации и защите информации». Перечень сведений конфиденциального характера. Доктрина информационной безопасности как система официальных взглядов на обеспечение национальной безопасности РФ в цифровой среде. Федеральный закон «О персональных данных»: основные положения, регулирование действий операторов (держателей) персональных данных. Организационная защита информации в организации.

**Тема 4. Контроль за соблюдение мер по обеспечению информационной безопасности и виды ответственности за нарушения в сфере защиты информации   
(2 часа)**

Государственные органы Российской Федерации, контролирующие деятельность в области защиты информации. Основные полномочия ФСБ России, МВД России, Роскомнадзора, ФСТЭК России в области в области информационной безопасности РФ. Дисциплинарная, административная, уголовная ответственность за несоблюдение норм законодательства Российской Федерации.

**Тема 5. Порядок осуществления защиты информации и персональных данных в организациях (3 часа)**

Уровни формирования режима информационной безопасности. Средства защиты аппаратного и программного подуровней. Четыре подсистемы комплекса программно-технических средств и организационных (процедурных) решений по защите информации от несанкционированного доступа. Показатели защищенности от несанкционированного доступа. Рекомендованные организационные мероприятия по защите информации. Классификация систем обработки персональных данных. Физические, аппаратные и программные средства защиты. Механизмы безопасности, определенные Приказом № 21ФСТЭК. Организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы.

**Тема 6. Правила разработки модели защиты от внешних информационных угроз организации и порядок ее внедрения (3 часа)**

Построение системы защиты информации. Состав и содержание 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). Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ ФСТЭК России от 11 февраля 2013г. №17). Требования к обеспечению защиты информации в автоматизированных системах (приказ ФСТЭК России от 14 марта 2014г. №31). Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (приказ ФСТЭК России от 25 декабря 2017г. №239). Методические рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Порядок разработки модели угроз, согласно документам ФСТЭК.

**Тема 7. Разработка организационно-распорядительной документации и документальное сопровождение вопросов защиты информации (5 часа)**

Разработка организационно-распорядительной и технической документации, отвечающей требованиям безопасности информации. Группы процессов, лежащие в основе разработке документированной политики информационной безопасности организации. Уровни документирования процесса обеспечения информационный безопасности.

**Тема 8. Оценка эффективности мер по защите информации (3 часа)**

Формы оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных. Этапы и порядок проведения оценки эффективности. Последовательность испытаний информационных систем на соответствие требованиям по защищенности персональных данных от угроз безопасности. Аттестация объектов информатизации. Оформление заключений и протоколов по результатам оценки.

**МОДУЛЬ 2. Порядок организации защиты информации в деятельности центров «Мои документы» (41 час)**

**Тема 1. Обеспечение информационной безопасности и защиты персональных данных при использовании ЕСИА (1 час)**

Понятие ЕСИА и основные особенности данной системы. Основные функциональные возможности ЕСИА. Перечень обязанностей оператора единой системы идентификации и аутентификации. Рекомендации пользователям ЕСИА. Требования к участникам взаимодействия в ЕСИА. Основные направления взаимодействия с ЕСИА. Процедуры регистрации и идентификации организации в ЕСИА. Функций центра регистрации с использованием установленных механизмов. Аутентификация с использованием OpenID Connect 1.0.

**Тема 2. Механизмы обеспечения информационной безопасности и защиты персональных данных в интегрированных информационных системах МФЦ (6 часов)**

Базовые принципы и правила обеспечения безопасности персональных данных в информационных системах. Организация безопасности ПД в ИСПД. Мероприятия по физическому контролю персональных данных в интегрированных информационных системах МФЦ. Классификация ИСПДн и категорирование ПДн. Оценка возможности оптимизации ИСПДн. Регламент процесса резервирования. Обеспечение эффективности процесса безопасности ПДн. Выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн.

**Тема 3. Порядок обеспечения информационной безопасности и защиты персональных данных в СМЭВ (3 часа)**

Система межведомственного электронного взаимодействия. Задачами системы межведомственного электронного взаимодействия в инфраструктуре Электронного правительства. Основные функции системы межведомственного электронного взаимодействия. ViPNet Coordinator HW1000. Сертификат организации в СМЭВ. Сертификат руководителя МФЦ. Плановая смена ключа электронной подписи.

**Тема 4. Выпуск и применение электронной цифровой подписи в деятельности центров «Мои документы» (4 часа)**

Электронная подпись. Виды электронных подписей. Юридическая значимость электронной подписи. Ключ проверки электронной подписи. Сертификация ключа проверки электронной подписи. Подтверждение подлинности электронной подписи в электронном документе. Риски использования электронной подписи. Инфраструктура открытых ключей. Удостоверяющий центр и его функции. Требования и рекомендации по обеспечению информационной безопасности на рабочем месте пользователя: персонал, размещение технических средств АРМ с установленным СКЗИ, установка программного обеспечения на АРМ, настройка операционной системы АРМ, установка и настройка СКЗИ, подключение АРМ к сетям общего пользования, обращение с ключевыми носителями, обращение с ключевой информацией, учет и контроль.

**Тема 5. Использование систем электронного документооборота в деятельности центров предоставления услуг в том числе в использовании СМЭВ (4 часа)**

Механизмом межведомственного взаимодействия: цели и задачи создания, функциональные возможности. Система электронного документооборота «ДЕЛО». Функциональные возможности системы «ДЕЛО»: работа с входящими и исходящими документами, работа с внутренними документами организации. Удаленная работа в системах электронного документооборота «ДЕЛО-WEB». Создание проектов электронных документов. Использование электронной подписи при работе в системах межведомственного взаимодействия и системах электронного документооборота. Технология применения электронной подписи: секретный и открытый ключ. Организация юридически значимого электронного документооборота. Шифрование документов. Защита хранилища данных.

**Тема 6. Порядок обработки и защиты персональных данных заявителей центров «Мои документы» (5 часов)**

Основные принципы и порядок обработки персональных данных и конфиденциальной информации заявителей в центрах предоставления государственных и муниципальных услуг. Меры и механизмы защиты персональных данных заявителей. Организационная структура СЗПДн. Функции в области обеспечения безопасности ПДн руководством организации и персоналом. Ответственные за защиту персональных данных заявителей.

**Тема 7. Порядок обработки, защиты и хранения персональных данных сотрудников центров «Мои документы» (4 часа)**

Нормативно-правовая база, регламентирующая движения персональных данных сотрудников организации. Положения о защите персональных данных работников. Правовое регулирование вопросов обеспечения защиты персональных данных работников на локальном уровне. Учетные документы движения персональных данных работников. Мероприятия по защите данных сотрудников проводимые в центрах предоставления государственных и муниципальных услуг. Планирование мероприятий по защите персональных данных. Обязанности работодателя по обеспечению защиты персональных данных работников. Порядок передачи работодателем персональных данных работников. Права и обязанности работников, связанные с обработкой и защитой их персональных данных. Система государственного надзора и контроля в области персональных данных сотрудников.

**Тема 8. Организация информационной безопасности в системах бухгалтерского учета и работы кадровых служб центров «Мои документы» (2 часа)**

Защищенность учетных данных. Угрозы безопасности с точки зрения их направленности. Умышленные и неумышленные ошибки в учете, приводящие к увеличению учетного риска. Системы бухгалтерского учета. Кадровые автоматизированные системы. Специфический аудит достоверности информации системы бухгалтерского учета. Права, обязанности и ответственность работодателя в процессе обработки учетных данных.

**Тема 9. Практические рекомендации по организации системы защиты информационной безопасности в центрах предоставления государственных и муниципальных услуг (2 часа)**

Перечня документов организации, регламентирующих обработку и защиту персональных данных. Политика конфиденциальности данных. Меры по защите обрабатываемых персональных данных от несанкционированного распространения. Блокировка персональных данных граждан. Список внутренних проверок для аудита безопасности. Физические меры защиты информации в бюджетных организациях. Наиболее эффективные меры обеспечения информационной безопасности.

**Тема 10. Взаимодействие центров «Мои документы» государственными органами, осуществляющими контроль деятельности в области защиты информации (2 часа)**

Требования к оператору персональных данных. Уведомление об обработке (намерении осуществлять обработку) персональных данных (Уведомление). Уведомление об изменении ранее предоставленных сведений персональных данных (Информационное письмо). Уведомление о прекращении обработки персональных данных (Заявление). Плановые проверки ФСБ России в области защиты персональных данных. Плановые проверки ФСТЭК РФ в области защиты информации. Проверки Роскомнадзора в области защиты информации. Проверки Государственной инспекции труда порядка работы с персональными данными сотрудников организации.

**Тема 11. Обзор практики проведения проверок в области защиты информации (2 часа)**

Порядок проведения внутреннего аудита. Сбор внутренних документов организации, необходимых для проверки. Порядок проведения проверки Роскомнадзора. Порядок проведения проверки ФСБ. Порядок проведения проверки ФСТЭК.

**Описание практико-ориентированных заданий и кейсов**

| **№ п/п** | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| --- | --- | --- | --- |
| **1** | 1.4. Контроль за соблюдение мер по обеспечению информационной безопасности и виды ответственности за нарушения в сфере защиты информации | Ответственность за нарушение норм законодательства Российской Федерации в области защиты информации | Установление соответствия между видом правонарушения в области обеспечения защиты информации и персональных данных и инкриминированной ответственностью за их нарушения с разделением на дисциплинарную, административную и уголовную |
| Контроль за соблюдение мер по обеспечению информационной безопасности | Определение зон ответственности в области соблюдения норм законодательства РФ о защите информации между контролирующими государственными органами |
| **2** | 1.5. Порядок осуществления защиты информации и персональных данных в организациях | Основы защиты информации и персональных данных в центрах «Мои документы» | Установление порядка и этапов осуществления защиты информации и персональных данных всех участников в центрах «Мои документы» |
| **3** | 1.6. Правила разработки модели защиты от внешних информационных угроз организации и порядок ее внедрения | Модель защиты от внешних информационных угроз | Составление модели внешних информационных угроз образовательной организации |
| Порядок внедрения модели защиты от внешних информационных угроз | Порядок внедрение модели защиты от внешних угроз (процедуры и необходимые локальные нормативно-правовые акты) |
| **4** | 1.7. Разработка организационно-распорядительной документации и документальное сопровождение вопросов защиты информации | Нормативно-правовое сопровождение процесса обеспечения безопасности в центрах «Мои документы» (составление локальных нормативных актов) | Составление внутренней регламентирующей документации на основании изученного материала и по установленным ключевым вехам |
| **5** | 2.2 Механизмы обеспечения информационной безопасности и защиты персональных данных в интегрированных информационных системах МФЦ | Защита информации в автоматизированных информационных системах | Процесс обеспечения безопасного движения данных в автоматизированных информационных системах МФЦ |
| Безопасная работа в личном кабинете автоматизированной информационной системе МФЦ | Безопасная работа в информационной системе МФЦ: создание учетной записи сотрудника, правила безопасной работы в личном кабинете |
| **6** | 2.3 Порядок обеспечения информационной безопасности и защиты персональных данных в СМЭВ | Обеспечения информационной безопасности и защиты персональных данных в СМЭВ | Порядок организации безопасного движения электронных документов в системах СМЭВ |
| **7** | 2.4 Выпуск и применение электронной цифровой подписи в деятельности центров «Мои документы» | Получение (обновление) цифровой подписи | Подготовка пакета документа для получения (обновления) цифровой подписи на руководителя организации и на ответственных сотрудников |
| Использование цифровой подписи в деятельности центров «Мои документы» | Использование цифровой подписи в деятельности центров «Мои документы»: установка, порядок безопасного хранения, подписания документов и тд. |
| **8** | 2.5 Использование систем электронного документооборота в деятельности центров предоставления услуг в том числе в использовании СМЭВ | Системы электронного документооборота в центрах «Мои документы» | Порядок работы специалистов центра «Мои документы» в системах электронного документооборота: администрирование, защита каналов связи, создание личных кабинетов пользователям и т.д. |
| Адаптация систем электронного документооборот в СМЭВ | Техническая организация безопасных каналов связи в процессе передачи электронных данных через СМЭВ |
| **9** | 2.6 Порядок обработки и защиты персональных данных заявителей центров «Мои документы» | Порядок обработки и защиты персональных данных заявителей центров «Мои документы» | Сбор, хранение, передача и работа с персональными данными заявителей в центрах «Мои документы» |
| **10** | 2.7 Порядок обработки, защиты и хранения персональных данных сотрудников центров «Мои документы» | Порядок обработки, защиты и хранения персональных данных сотрудников центров «Мои документы» | Создание электронной базы данных личных дел сотрудников центров «мои документы». Создание безопасной инфраструктуры движения информации и о персонале организации |
| **11** | 2.9 Практические рекомендации по организации системы защиты информационной безопасности в центрах предоставления государственных и муниципальных услуг | Система защиты информационной безопасности в центрах «Мои документы» | Разработка модели защиты информации и персональных данных в центрах «Мои документы» |
| Разработка дородной карты внедрения модели защиты информации в центрах «Мои документы» |
| Расчет ресурсов, необходимых для внедрения модели защиты информации в центрах «Мои документы» |
| **12** | 2.10 Взаимодействие центров «Мои документы» государственными органами, осуществляющими контроль деятельности в области защиты | Порядок предоставления информации в сфере организации безопасного движения данных в центрах «Мои документы» | Подготовка пакета документов для прохождения плановых и неплановых проверок государственными органами в области защиты информации |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| --- | --- | --- | --- |
| 1 | Защита информации - это? | В ФЗ РФ «О безопасности» от 05.03.1992г. № 2446-1 под информационной безопасностью понимают? | Согласно Национальному стандарт РФ ГОСТ Р 50922-2006, под защитой информации понимают? |
| Автоматизированная система обработки информации – это? | К компонентам автоматизированной системы обработки информации относят? | Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов. Какие из нижеперечисленных элементов не относится к компонентам автоматизированной системы? |
| 1 | Механизм, используемый для подтверждения прав пользователя информационных систем? | К порядку авторизации субъекта относят? | Процедура, в рамках которой осуществляется предоставление субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети) является? |
| Несанкционированный доступ к персональной информации – это? | Соотношение понятий несанкционированного доступа и промышленного шпионажа | Доступ к информации или действия с информацией, нарушающей правила разграничения доступа, предоставляемых средствами вычислительной техники или автоматизированными системами – это? |
| Система защиты информации - это? | Функции систем защиты информации | К принципам защиты информации не относят? |
| Нарушители информационной безопасности систем – это? | Нарушителей безопасности систем обработки информации и данных квалифицируют по следующим критериям: | Какое количество уровней выделяют в классификации нарушителей, предоставляемых доступ к штатным средствам автоматизированных систем и средств вычислительной техники? |
| Доступная информация и информация ограниченного доступа | Основные свойства и функции информации? | Свойство информации, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц |
| Под информационно угрозой понимают? | Согласно, законодательству Российской Федерации, под угрозой в информационной среде понимают? | Определите основные виды информационных угрозы в деятельности образовательной организации |
| Виды информации? | Виды информации, относящейся к персональным данным граждан, относят? | Под информацией, прямо или косвенно относящейся к физическому лицу понимают |
| Обработка информации – это? | Характеристика класса 2 (К2) обработки информации в информационных системах | Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн относятся к следующему классу |
| 2 | Персональные данные граждан – это? | Характеристика классов обработки персональных данных | К какой категории информации относят обезличенные и (или) общедоступные персональные данные? |
| 2 | Виды систем обработки персональных данных? | По режиму обработки персональных данных в информационной системе информационные системы подразделяются на? |
| Сбор и анализ персональных данных – это процесс по: | Правила и порядок обработки персональных данных в информационных системах? | Какие данные об информационных системах, обрабатывающих персональные данные, учитываются при их классификации? |
| Положения о защите персональных данных работников | Правовое регулирование вопросов обеспечения защиты персональных данных работников на локальном уровне |
| Обязанности работодателя по обеспечению защиты персональных данных работников | Порядок передачи работодателем персональных данных работников |
| Уведомление об обработке (намерении осуществлять обработку) персональных данных | Порядок составления электронного уведомлени |
| Уведомление об изменении ранее предоставленных сведений персональных данных |  |
| К какой категории данных относится защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности? | Виды и формы информации, содержащей сведения относящих к государственной тайне | Проведите сравнительный анализ понятий «государственная тайна» и «промышленная тайна» |
| Система стратегических взглядов и ориентиров на обеспечение национальной безопасности Российской Федерации в области безопасности информации называется | Основные компоненты Доктрины о информационной безопасности | Корреляция положений Доктрины о информационной безопасности с деятельности центров «Мои документы» |
| Цифровая подпись – это? | Характеристика видов цифровых подписей | Вид электронной подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом называется |
| 2 | Государственные органы, курирующие вопросы обеспечения безопасности информации и защиты конфиденциальных персональных данных | Орган, реализующий свои полномочий при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств | Основные полномочия и функции ФСБ России в области защиты информации и данных |
| Порядок проведения проверок на предмет соблюдения норм законодательства Российской Федерации в области защиты информации ФСБ России | Предметная область проверки ФСБ России образовательных учреждений в области защиты информации |
| Порядок проведения проверок на предмет соблюдения норм законодательства Российской Федерации в области защиты информации ФСЭК России | Предметная область проверки ФСТЭК России образовательных учреждений в области защиты информации |
| Порядок проведения проверок на предмет соблюдения норм законодательства Российской Федерации в области защиты информации МВД России | Предметная область проверки МВД России образовательных учреждений в области защиты информации |
| Порядок проведения проверок на предмет соблюдения норм законодательства Российской Федерации в области защиты информации Роскомнадзором | Предметная область проверки Роскомнадзора образовательных учреждений в области защиты информации |
| Виды ответственности за правонарушения в области защиты информации? | К какому виду ответственности относится нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) | Соотнесите нарушение в области защиты информации и данных с видом ответственности |
| Информационная система персональных данных – это? | Категория и объем персональных данных, обрабатываемых в центрах «Мои документы» | Оценка возможности оптимизации ИСПДн |
| 2 | Система межведомственного электронного взаимодействия – это? | Задачами системы межведомственного электронного взаимодействия в инфраструктуре Электронного правительства | Основные функции системы межведомственного электронного взаимодействия |
| Механизмы защиты информации при работе в СМЭВ | ViPNet Coordinator HW1000 |
| Средство криптографической защиты информации – это? | Инфраструктура открытых ключей | Порядок подтверждения подлинности электронной подписи в электронном документе |

**8.2. Описание показателей и критериев оценивания, шкалы оценивания**.

Критерии оценки

Оценка ***«отлично»*** ставится при условии, если слушатель программы обладает:

1. глубокими теоретическими знаниями и практическими знаниями в области организации и последующей эксплуатации системы защиты информации в образовательной организации, а также знания основ работы с персональными и конфиденциальными данными граждан, их защиты и порядок обработки;
2. необходимыми компетенциями в области своей профессиональной деятельности;
3. способностью применять теоретические знания на практике с целью решения поставленной задачи.

Оценка ***«хорошо»*** ставится при условии, если слушатель программы обладает:

1. твердыми теоретическими знаниями основ защиты информации в цифровой среде;
2. компетенциями в области применения форм и методов осуществления профессиональной деятельности;
3. способностью применять теоретические знания для выбора правильного алгоритма решения поставленной задачи.

Оценка ***«удовлетворительно»*** ставится при условии, если слушатель программы:

1. обладает основными теоретическими знаниями в области нормативно-правового регулирования процесса обеспечения персональных безопасности данных и защиты информации;
2. испытывает затруднения при применении теоретических знаний для выбора правильного алгоритма решения поставленной задачи.

Оценка ***«неудовлетворительно»*** ставится при условии, если слушатель программы

1. имеет значительные пробелы в теоретической части программного материала;
2. не обладает необходимыми компетенциями;
3. не освоил умения применять теоретические знания для выбора правильного алгоритма решения поставленной задачи.

Оценка «отлично»: 80% правильных ответов на тестовые задания;

Оценка «хорошо»: от 60 до 80% правильных ответов;

Оценка «удовлетворительно»: от 40 до 60% правильных ответов;

Оценка «неудовлетворительно»: менее 40% правильных ответов.

**8.3. Примеры контрольных заданий по модулям или всей образовательной программе**

**Примерные контрольные, практические задания и задания для самостоятельной работы по программе повышения квалификации**

**«Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»»**

**Задание 1. Контроль за соблюдением мер по обеспечению информационной безопасности и виды ответственности за нарушения в сфере защиты информации**

Какие из нижеперечисленных факторов информационной безопасности оказывают наибольшее влияние на деятельность Вашей организации? Выберите необходимые факторы, обоснуйте причину их появления и предложите способы минимизации их влияния

Организационно-технические методы информационной безопасности (ИБ):

* систему обеспечения информационной безопасности (под ней мы подразумеваем комплекс мероприятий (внутренние правила работы с данными, регламент передачи сведений, доступ к ним и т. д.) и технических средств (использование программ и приборов для сохранения конфиденциальности данных));
* разработку (создание новых), эксплуатацию и усовершенствование уже имеющихся средств защиты информации;
* перманентный контроль над действенностью принимаемых мер в области обеспечения информационной безопасности.

Правовые факторы ИБ:

* лицензирования деятельности в части обеспечения информационной безопасности;
* сертификации технических средств информационной защиты;
* аттестации объектов информатизации согласно соответствию нормам информационной безопасности.

Эконмические факторы:

* составление программ по обеспечению ИБ;
* определение источников их финансового обеспечения;
* разработку порядка финансирования;
* создание механизма страхования информационных рисков.

**Задание 2. Порядок осуществления защиты информации и персональных данных в организациях**

1. Дайте определение понятию «Биометрические ПДн», опишите особенности этой категории ПДн.

2. Укажите законные основания, на основе которых Ваша организация обязана обрабатывать персональные данные.

3. Составьте список угроз безопасности ПДн при их обработке в Вашей компании.

4. Продумайте и составьте правила учета машинных носителей ПДн в Вашей организации.

5. Продумайте и составьте правила обеспечения безопасности обработки ПДн сотрудников организации.

**Задание 3. Правила разработки модели защиты от внешних информационных угроз организации и порядок ее внедрения**

Модель угроз применяют при решении разных задач:

* выбор организационных и технических мер по обеспечению безопасности ПДн и их реализации в системе защиты ПДн;
* определение требуемого уровня защищенности ПДн;
* анализ защищенности от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
* разработка системы защиты ПДн, обеспечивающей нейтрализацию угроз с использованием организационных и технических мер обеспечения безопасности ПДн;
* проведение мероприятий, направленных на предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
* недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование.

Задание. Разработать модель угрозы по следующему плану:

1. титульный лист, аннотация, содержание и список сокращений;
2. в вводной части:

на основании каких нормативно-методических документов разработана модель угроз;

какую информацию она содержит;

при решении каких задач используется;

как часто может актуализироваться и пересматриваться;

какой компанией разработана и для кого предназначена.

1. специальные положения:

описание информационной системы персональных данных, включая описание информационно-технологической инфраструктуры;

структурно-функциональные характеристики;

описание угроз безопасности;

модель нарушителя;

возможные уязвимости;

способы реализации угроз;

последствия нарушения безопасности информации.

**Задание 4. Разработка организационно-распорядительной документации и документальное сопровождение вопросов защиты информации**

Помимо технических и процедурных решений создаваемой системы защиты персональных данных, оператор должен обеспечить разработку организационно - распорядительных документов, которые будут регулировать все возникающие вопросы по обеспечению безопасности ПД при их обработке в ИСПД и эксплуатации системы защиты персональных данных (далее СЗПД). Таких документов достаточно много, основные из них:

1. Положение по обеспечению безопасности ПД. Это внутренний (локальный) документ организации. Строгой формы данного документа нет, но он должен удовлетворять требованиям ТК и ФЗ-152, а, следовательно, в нем должно быть указано:

цель и задачи в области защиты персональных данных;

понятие и состав персональных данных;

в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные;

как происходит сбор и хранение персональных данных;

как они обрабатываются и используются;

кто (по должностям) в пределах фирмы имеет к ним доступ;

принципы защиты ПД, в том числе от несанкционированного доступа;

права работника в целях обеспечения защиты своих персональных данных;

ответственность за разглашение конфиденциальной информации, связанной с персональными данными работников.

Положение по обеспечению безопасности персональных данных утверждается руководителем организации или уполномоченным им лицом, вводится в действие приказом руководителя. Работодатель обязан ознакомить работника с Положением… под подпись.

2. Для организации системы допуска и учета лиц, допущенных к работе с ПД в ИСПД, - Список лиц, допущенных к обработке ПД (перечень по должностям тех, кому доступ к ПД необходим для выполнения служебных обязанностей) и Матрица доступа (должна отражать полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПД – чтение, запись, корректировка, удаление).

В первую очередь доступ необходимо оформить сотрудникам кадровой службы, поскольку они собирают и формируют данные о работнике, а также сотрудникам бухгалтерии. Помимо того, доступ к этим сведениям могут получить руководители структурных подразделений (например, начальники отделов) – и это также необходимо отразить в списке. Однако все они вправе запрашивать не любые данные, а только те, которые необходимы для выполнения конкретных трудовых функций (например, чтобы рассчитать льготы по налогам, бухгалтерия получит не все сведения о работнике, а только данные о количестве его иждивенцев). Поэтому целесообразно прописать перечень информационных ресурсов, к которым пользователи допущены.

Список лиц, допущенных к обработке ПД, можно оформить в виде приложения к Положению по обеспечению безопасности персональных данных или отдельным документом, утвержденным руководителем.

3. Частная модель угроз (если ИСПД несколько, то модель угроз разрабатывается на каждую из них) – разрабатывается по результатам предварительного обследования. ФСТЭК России предлагает Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, согласно которой при создании частной модели должны быть рассмотрены:

угрозы утечки информации по техническим каналам;

угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к ИСПД, реализующих угрозы непосредственно в ИСПД. При этом необходимо в качестве потенциальных нарушителей рассматривать легальных пользователей ИСПД;

угрозы несанкционированного доступа, связанные с действиями нарушителей, не имеющих доступа к ИСПД, реализующих угрозы из внешних сетей связи общего пользования и(или) сетей международного информационного обмена.

Разработанная модель угроз утверждается руководителем.

4. На основании утвержденной модели угроз ИСПД необходимо разработать требования по обеспечению безопасности ПД при их обработке в ИСПД. Требования, как и модель угроз, - это самостоятельный документ, который должен быть утвержден руководителем организации.

Для разработки модели угроз и требований оператору целесообразно привлекать специалистов организаций-лицензиатов ФСТЭК.

5. Инструкции в части обеспечения безопасности ПД при их обработке в ИСПД.

6. Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Задание. Разработать один из видов документов, регламентирующих порядок организации защиты информации в организации.

**Задание 5. Оценка эффективности мер по защите информации**

Задание. Определите ключевые мероприятия по оценке эффективности мер по защите информации в Вашей организации.

Согласно пункту 3 Информационного сообщения ФСТЭК России от 15.07.2013 №240/22/2637 форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, не установлены. Таким образом, решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается оператором персональных данных самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

Под оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа - «Оценка эффективности» подтверждается, что информационная система персональных данных соответствует требованиям Состава и содержания мер, утвержденных приказом ФСТЭК России от 18.02.2013 №21.

**Задание 6. Механизмы обеспечения информационной безопасности и защиты персональных данных в интегрированных информационных системах МФЦ**

Опишите основные функциональные возможности интегрированной информационной системы МФЦ и особенности обеспечения информационной безопасности и защиты персональных данных со стороны Вашей организации в данной системе

**Задание 7. Использование систем электронного документооборота в деятельности центров предоставления услуг в том числе в использовании СМЭВ**

Определите тип СЭД Вашей организации и опишите основные угрозы информационной безопасности, существующие в ней.

В зависимости от функционала системы ЭДО делятся на несколько групп:

* программы, работающие в основном как электронный архив. При выборе таких программ акцент делается на удобстве хранения документов и поиска по базе, он может быть более или менее четким или нечетким, по названию, цели, фразам из текста, другим атрибутам;
* продукты, делающие акцент на удобстве workflow (маршрутизации). Здесь четко прописывается процесс создания и обработки базовой единицы информации, который меняется на каждом этапе его путешествия. Маршрутизация обычно задается жесткая, прописанная программистами для каждого типа изначально;
* системы гибридного типа, соединяющие преимущества двух предыдущих. Для них характерна наряду с жесткой мягкая маршрутизация, когда путь конкретного файла задается самостоятельно руководителем соответствующего подразделения;
* ЭДО, предполагающие совместную работу с файлами (collaboration). Они изначально не настроены на жесткую иерархичность и создают удобство для проектных работ, когда каждый участник группы вносит свой вклад в обработку общего решения. Так как они часто используют форумный тип обсуждения и размещение файлов на открытых для общего доступа площадках, вопросы безопасности в них решены наиболее слабо;
* многозадачные продукты с дополнительными сервисами. Так, CRM может быть встроена в документооборот, а не наоборот.

Вопрос безопасности данных актуален для всех программ, но его решение зависит от еще одного уровня классификации – типа самой ЭДО. Системы могут быть:

* самостоятельными модулями;
* облачными решениями;
* модулями CRM или иной программы управления предприятием.

Можно выделить следующие основные виды СЭД, внедренные на российском рынке:

Optima WorkFlow. Ее преимуществом является возможность контролировать процесс общих работ на базе диаграммы Ганта. CRM-функционала нет. Система транспортировки и хранения документов реализована в Windows Exchange, что дает представление об общей степени защищенности.

«Е1 Евфрат». Простой электронный архив, где хранятся не файлы, а ссылки на них. Вопрос размещения архива в Интернете с условием надежности хранения службам безопасности придется решать самостоятельно.

«1С Документооборот». Задача защиты информации в ЭДО решается стандартно для семейства программ и зависит от того, где именно хранятся файлы – в облаке или иным способом, на сервере. Права пользователей ранжируются.

«Дело». Программа-маршрутизатор предназначена для оптимизированного делопроизводства. Сохранность документов всецело в руках IT-службы предприятия, так как режим безопасности и права доступа оно определяет самостоятельно.

Directum. Имеет расширенный функционал, помогает в работе с проектами, финансовыми задачами, обращениями граждан (для государственных служб). Архивирование построено по принципам российского законодательства. Безопасность информации обеспечивается тем, что для сторонних посетителей файлы представлены в формате читального зала. Реализована модель управления доступом. Применяется шифрование и ЭП.

ELMA. Многофункциональная система с хорошей версией безопасности. Реализована модель входа только с доверенных устройств, вход по токену и сертификату.

**Задание 8. Практические рекомендации по организации системы защиты информационной безопасности в центрах предоставления государственных и муниципальных услуг**

Укажите конкретные средства обеспечения информационной безопасности и защиты персональных данных в Вашем центре «Мои документы» по следующим видам:

- НСД

- Антивирус

- Межсетевой экран

- Средства анализа защищенности

- Средства обнаружения вторжений

- Модули доверенной загрузки

- Криптосредства

**Задание 9. Взаимодействие центров «Мои документы» государственными органами, осуществляющими контроль деятельности в области защиты информации**

Перечислите основные контролирующие органы в сфере обеспечения информационной безопасности и защиты персональных данных, с которыми Ваша организация должна взаимодействовать, а также основные регламентирующие нормативные правовые акты, определяющие зоны их ответственности и полномочий.

**8.4. Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий**

**Примерные тестовых задания по программе повышения квалификации**

**«Техническая защита информации и обеспечение безопасности персональных данных в центрах «Мои документы»»**

1. Согласно Национальному стандарт РФ ГОСТ Р 50922-2006, под защитой информации понимают:

**- деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**

- деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и получения защищаемой информации злоумышленниками

- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, либо владельцем информации прав или правил доступа к защищаемой информации.

- совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

2. Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов. Какие из нижеперечисленных элементов не относится к компонентам автоматизированной системы:

- аппаратные средства

- программные средства

- обслуживающий персонал и пользователи системы

**- организационные средства**

3. Процедура, в рамках которой осуществляется предоставление субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети) является:

**- авторизация субъекта**

- ассиметричное шифрование

- активация субъекта

- лицензирование субъекта

4. Доступ к информации или действия с информацией, нарушающей правила разграничения доступа, предоставляемых средствами вычислительной техники или автоматизированными системами – это:

- неквалифицированный доступ

- промышленный шпионаж

**- несанкционированный доступ**

- доступ с повышенными правами

5. К принципам защиты информации не относится:

- защита средств вычислительной техники и автоматизированных систем основывается на положениях и требованиях существующего законодательства

- защита автоматизированных систем обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер

- контроль эффективности средств защиты от несанкционированного доступа

**- возможностью создания и запуска собственных программ с новыми функциями по обработке информации**

6. Какое количество уровней выделяют в классификации нарушителей, предоставляемых доступ к штатным средствам автоматизированных систем и средств вычислительной техники:

- 3

**- 4**

- 5

- 6

7. Свойство информации, которое указывает на необходимость ограничения доступа к конкретной информации для обозначенного круга лиц:

**- конфиденциальность**

- целостность данных

- доступность информации

- достоверность

8. К угрозам информационной безопасности не относятся:

- ошибки пользователей

- аварии и стихийные бедствия

- хищение информации

**- внутренние проверки безопасности**

9. Под информацией, прямо или косвенно относящейся к физическому лицу понимают:

**- персональными данными**

- данными личного хранения

- конфиденциальной информацией

- данными, удостоверяющими личность

10. Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн относятся к следующему классу:

- класс 1 (К1)

- класс 2 (К2)

**- класс 3 (К3)**

- класс 4 (К4)

11. К какой категории информации относят обезличенные и (или) общедоступные персональные данные?

- категории 1

- категории 2

- категории 3

**- категории 4**

12. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:

**- однопользовательские и многопользовательские**

- системы без разграничения прав доступа и системы с разграничением прав доступа

- системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации

- системы, имеющие подключения к сетям международного информационного обмена, и системы, не имеющие таких подключений

13. Какие данные об информационных системах, обрабатывающих персональные данные, учитываются при их классификации:

- категория обрабатываемых в информационной системе персональных данных

- структура информационной системы

**- сбор и анализ исходных данных по информационной системе**

- режим обработки персональных данных

14. К какой категории данных относится защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности:

**- государственная тайна**

- коммерческая тайна

- стратегическая информация

- персональные данные

15. Система стратегических взглядов и ориентиров на обеспечение национальной безопасности Российской Федерации в области безопасности информации называется:

- политика обеспечения информационной безопасности

- моделью обеспечения информационной безопасности

**- доктриной информационной безопасности**

- Национальные стандарты в области информационной безопасности

16. Вид электронной подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом называется:

**- простая электронная подпись**

- усиленная неквалифицированная электронная подпись (неквалифицированная электронная подпись)

- усиленная квалифицированная электронная подпись

- специализированная подпись

17. Использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности относится к:

**- организационным мерам**

- законодательным мерам

- техническим мерам

- кадровым мерам

18. Основным источником права в области обеспечения информационной безопасности в России является:

**- Конституция Российской Федерации**

- ФЗ РФ «О персональных данных» от 27 июля 2006 г. №152-ФЗ

- ФЗ РФ «О связи» 7 июля 2003 г. №126-ФЗ

- ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. №149-ФЗ

19. Орган, реализующий свои полномочий при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств:

**- ФСБ**

- ФСТЭК

- МВД

- Роскомнадзор

20. В соответствии ч. 1 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» оператор до начала обработки персональных данных обязан уведомить о своем намерении осуществлять обработку персональных данных следующий уполномоченный орган:

- ФСБ

- ФСТЭК

- МВД

**- Роскомнадзор**

21. Обеспечение безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, обеспечение защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, осуществление экспортного контроля относится к ведению:

- ФСБ

**- ФСТЭК**

- МВД

- Роскомнадзор

22. В каких случаях предполагается административная ответственность за нарушения законодательства Российской Федерации в области защиты информации и обработки персональных данных:

- **нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных**

- неправомерный доступ к охраняемой законом компьютерной информации, повлекшей ее уничтожение, блокирование, модификацию либо копирование

- разглашение персональных данных сотрудников организации, передача о них третьим лицам

- хранению информации и обеспечению доступа к ней

23. МВД России, в рамках своих полномочий в области защиты информации, обеспечивает:

**- защиту прав и свобод человека и гражданина в информационной сфере**

- контроль и надзор за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных

- создание, формирование и ведение единой автоматизированной информационной системы «Единый реестр доменных имен»

- обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем,

24. К целям создания РИС «Образование» не относится:

- повышение эффективности государственного и муниципального управления в сфере образования за счет использования современных информационных технологий

**- проведение государственной итоговой аттестации обучающихся**

- снижение нагрузки на организации образования за счет автоматизации учета контингента и формирования отчетности, исключения многократного ввода одной и той же информации

- повышение надежности и безопасности использования информационных технологий в организациях образования, снижение расходов организаций образования за счет централизации и унификации предоставляемых сервисов и интерфейсов информационного взаимодействия

25. Контур системы, который доступен только с аттестованных рабочих мест, в котором присутствует полный функционал системы, включая работу с персональными данными, например, личные дела (портфолио учащихся), зачисление, администрирование называется:

**- закрытым контуром**

- открытым контуром

- внешним контуром

- контуром защиты персональных данных

**8.5. Описание процедуры оценивания результатов обучения** **.**

Итоговые испытания проводятся на дистанционном портале ООО «Агентство инновационного развития». Результат сдачи итоговой аттестации (в форме тестирования) выражается в процентах и количествах правильных ответов. На основании полученных результатов итоговая аттестационная комиссия принимает решение о завершении программы обучающимся на закрытом заседании простым большинством голосов членов комиссий, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов председатель комиссии (или заменяющий его заместитель председателя комиссии) обладает правом решающего голоса.

Все решения итоговых аттестационных комиссий оформляются протоколами. Протоколы заседаний итоговой аттестационной комиссии подписываются соответствующей итоговой аттестационной комиссии (в случае отсутствия председателя – его заместителем), членами и секретарем итоговой аттестационной комиссии и хранятся в архиве согласно номенклатуре дел.

Лицам, завершившим освоение дополнительной профессиональной программы повышения квалификации, но не подтвердившим соответствие подготовки требованиям, предъявляемым к слушателям, при прохождении одного или нескольких итоговых аттестационных испытаний, при восстановлении назначаются повторные итоговые аттестационные испытания в порядке, определяемом ООО «Агентство инновационного развития», но не более двух раз. Слушатели, не прошедшие итоговую аттестацию или получившие неудовлетворительные результаты, вправе пройти итоговую аттестацию в сроки, определенные ООО «Агентство инновационного развития», но не позднее чем через три месяца после прохождения итоговой аттестации впервые. Лицам, не проходившим итоговых аттестационных испытаний по уважительной причине (по медицинским показаниям или в других исключительных случаях, документально подтвержденных), предоставляется возможность пройти итоговые аттестационные испытания без отчисления из ООО «Агентство инновационного развития».

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| **1** | **Тагаев**  **Алексей Васильевич** | директор ООО «Агентство инновационного развития» |  |  | **да** |
| **2** | **Щерба**  **Алексей Сергеевич** | Инженер по безопасности, старший менеджер по работе с ключевыми клиентами ООО «ЭнигмаДон» |  |  | **да** |
| **3** | **Ганеева**  **Валерия Маратовна** | заместитель директор аООО «Агентство инновационного развития» |  |  | **да** |
| **4** | **Артамонов Алексей Викторович** | Заместитель начальника - начальник отдела информационных технологий  МФЦ города Ростова-на-Дону |  |  | **да** |
| **5** | **Яковенко Светлана Николаевна** | начальник отдела организационно-методического обеспечения МФЦ города Ростова-на-Дону |  |  | **да** |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Формы обучения:  - лекционные занятия - практические занятия  - самостоятельная работа  Методы обучения:  - наглядные, практические;  - объяснительно- поисковые,  - исследовательские, проблемные;  - индуктивные и дедуктивные  Технологии обучения:  - Технология развития критического мышления  - Проектная технология  - Модульная технология  - Информационно – коммуникационная технология | Методические разработки,  материалы курса, учебная литература |

**Нормативно-правовые документы**

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
2. «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7)
3. «Паспорт федерального проекта «Цифровое государственное управление» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 N 9)
4. ФЗ РФ «О безопасности» от 05.03.1992г. № 2446-1
5. ФЗ РФ «О государственной тайне» от 21.07.1993г. №5485-1 (с изм. и доп., вступающими в силу с 15.12.2007)
6. ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. №149-ФЗ
7. ФЗ РФ «О коммерческой тайне» от 29 июля 2004 г. №98-ФЗ
8. ФЗ РФ «О персональных данных» от 27 июля 2006 г. №152-ФЗ
9. ФЗ «О техническом регулировании» от 27 декабря 2002 г. №184-ФЗ
10. ФЗ РФ «Электронной цифровой подписи» от 10 января 2002 г. №1-ФЗ
11. ФЗ РФ «Об электронной подписи» от 6 апреля 2011 г. №63-ФЗ
12. ФЗ РФ «О связи» 7 июля 2003 г. №126-ФЗ
13. ФЗ «О лицензировании отдельных видов деятельности» от 8 августа 2001 года, №128-ФЗ
14. Приказ ФСТЭК №58 от 5.02.2010г. «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
15. Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
16. ФЗ от 4 мая 2011 г. №99-ФЗ «О лицензировании отдельных видов деятельности»
17. Постановление Совета Министров — Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам»
18. Постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. № 333
19. Положение о сертификации средств защиты информации Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 29 марта 1999 г. № 342; от 17 декабря 2004 г. № 808)
20. Постановление Правительства РФ «Об организации лицензирования отдельных видов деятельности» от 26.01.2006г. № 45
21. Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
22. Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации» от 15.08.06 № 504
23. Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532
24. Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
25. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008г. №687
26. Постановление Правительства РФ №211 от 21.03.12 «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»
27. Постановление Правительства РФ от 1 ноября 2012 г. № 1119  «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
28. Постановление Правительства РФ от 3 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации»

**Основная литература**

1. Кожевников А.Ю., Тутубалин П.И., Кирпичников А.П., Мокшин В.В. О построении подсистемы удаленного мобильного доступа к информационным ресурсам некоторой организации // Вестник Технологического университета. 2018. Т. 21. № 2. С. 139-147.
2. Пиков В.А., Вергасова А.Е. Способ реализации требований 152-ФЗ «О персональных данных» в российской части информационно-телекоммуникационной сети «Интернет» // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2018. № 4. С. 139-154.
3. Дерябина О.С. Основные задачи развития системы информационной безопасности // Молодой ученый. 2019. № 25 (263). С. 19-21.
4. Антошечкин А.В. Анализ возможностей применения биометрических технологий для реализации процедур обезличивания персональных данных // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2018. № 1. С. 27-36.
5. Дадалко В.А., Тимофеев Е.А. Основы формирования комплаенс-контроля в области системы обеспечения безопасности персональных данных // Национальные интересы: приоритеты и безопасность. 2020. Т. 16. № 2 (383). С. 339-350.
6. Симонова С.В. Обеспечение прав человека при эксплуатации информационных систем персональных данных: вызовы цифровой среды // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2020. № 1 (51). С. 72-77.
7. Мошуров Н.П., Щудро И.А., Фот Ю.Д. Защита персональных данных в локальных и глобальных сетях // Научно-технический вестник Поволжья. 2019. № 4. С. 150-155.
8. Епрынцева Н.А., Соколова А.В., Руднева А.А. О необходимости защиты персональных данных // Информационные технологии в строительных, социальных и экономических системах. 2019. № 1 (15). С. 120-123.
9. Кузнецов Е.С. Обеспечение безопасности данных пользователей интернет-банкинга с помощью систем искусственного интеллекта // В сборнике: Наука и технологии: стратегия развития Сборник научных статей. Под общей редакцией В.А. Козловой, И.В. Кожан. Ростов-на-Дону, 2019. С. 82-87.
10. Гильманшина А.Л. Анализ литературы и нормативно-правовой базы в области защиты персональных данных // Вестник науки. 2019. Т. 2. № 3 (12). С. 13-16.
11. Жук Роман Владимирович, Дзьобан Павел Игоревич, Власенко Александра Владимировна Построение взаимосвязи между нарушителем информационной безопасности и уязвимостями информационных активов в информационных системах обработки персональных данных // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 162-169.
12. Левинский А.Т. Система анализа и предупреждения угроз безопасности персональных данных на предприятии // Политехнический молодежный журнал. 2019. № 5 (34). С. 5.
13. Басан А.С., Некрасов А.В., Макаревич О.Б. Безопасность персональных данных // Ростов-на-Дону; Таганрог, 2018. Том Часть 1 Обеспечение безопасности персональных данных
14. Комаров С.А., Мицкая Е.В. Правовое регулирование обеспечения информационной безопасности и защиты персональных данных // Санкт-Петербург, 2018.
15. Полякова Т.А., Минбалеев А.В., Бойченко И.С. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде // Вестник Академии права и управления. 2018. № 3 (52). С. 32-36.
16. Чубукова С.Г., Стрельцов А.А., Ниесов В.А., Полякова Т.А. Организационное и правовое обеспечение информационной безопасности // Учебник и практикум / Москва, 2019. Сер. 68 Профессиональное образование (1-е изд.)
17. Карцхия А.А., Севостьянов В.Л. Информационная безопасность: правовые аспекты // Правовая информатика. 2018. № 4. С. 43-49.
18. Калабина В.Э., Егорова Н.Е. Кодирование информации, как средство защиты информации от несанкционированного доступа // В сборнике: Современные инновации в науке и технике Сборник научных трудов 8-й Всероссийской научно-технической конференции с международным участием. Ответственный редактор А.А. Горохов. 2018. С. 88-92.
19. Малиничев Д.М., Ермашов А.В. Обеспечение защиты информации в компании от несанкционированного доступа с помощью отечественных продуктов средств защиты информации // Colloquium-journal. 2019. № 11-1 (35). С. 101-103.
20. Казыханов А.А., Байрушин Ф.Т. Необходимость использования аппаратных модулей для защиты информации от НСД // Территория инноваций. 2018. № 1 (17). С. 43-45.
21. Михайлова Ю.Н., Ямщикова С.Л. Защита конфиденциальной информации // Аллея науки. 2018. Т. 1. № 1 (17). С. 431-434.
22. Богатко М.П., Фисунов А.В., Щеголев В.В. Анализ комплексных систем защиты информации от несанкционированного доступа // Вестник современных исследований. 2018. № 1.1 (16). С. 101-103.
23. Мухамадиева З.Б. Защита информации в информационных системах // Молодой ученый. 2018. № 9 (195). С. 34-36.
24. Яцук К.В., Смирнов Д.К., Цымбалий А.О. Защита информации в сети // Молодой ученый. 2018. № 10 (196). С. 29-32.
25. Чапайкин В.П., Ященко В.А., Яцук К.В. Технические средства защиты информации // Наука, техника и образование. 2018. № 4 (45). С. 31-35.
26. Криворотенко С.Н., Шестаков Н.Р. Информационная безопасность в контексте федерального закона «Об информации, информационных технологиях и о защите информации» // Вестник Краснодарского государственного института культуры. 2018. № 1 (14). С. 13.
27. Аншин И.А., Мусин А.А., Девяткин Д.Е. Средства защиты информации от несанкционированного доступа // Интернаука. 2018. № 19-1 (53). С. 48-50.
28. Карпов В.С., Скварник Е.В., Яцук К.В. Способы и средства технической защиты информации от утечки по техническим каналам // Точная наука. 2018. № 23. С. 26-30.
29. Ахмедова А.Г. Защита информации от внутренних угроз // European Science. 2018. № 5 (37). С. 41-42.
30. Колесников В.А., Несговоров А.Г. Перспективы использования технических средств защиты информации в России // Академия педагогических идей Новация. Серия: Студенческий научный вестник. 2018. № 6. С. 53-57.
31. Кулешов Ю.Е., Сергиенко В.А., Паскробка С.И. Методический подход к оценке эффективности защиты информации // Проблемы инфокоммуникаций. 2018. № 1 (7). С. 45-53.
32. Рафикова В.М., Фатеева Н.И. Применение методов защиты информации // Аллея науки. 2018. Т. 6. № 5 (21). С. 137-140.
33. Баранкова И.И., Михайлова У.В., Лукьянов Г.И., Калугина О.Б. Обеспечение защиты информации от утечки по техническим каналам // ЛАБОРАТОРНЫЙ ПРАКТИКУМ / Магнитогорск, 2018.
34. Попов Г.А., Попова Е.А. Системный подход к формированию состава функций управления в системах защиты информации // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2018. № 1. С. 71-80.

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| http://cyberrus.com/ | http://www.securitylab.ru/ |
| http://www.itsec.ru/articles2/allpubliks | https://threatpos |
| http://wiki.informationsecurity.club/doku.php/main | ttps://www.anti-malware.ru/ |
| http://www.iso27000.ru/ | https://geektimes.ru/hub/infosecurity/ |
| https://www.youtube.com/channel/UCinmAF3guG-A5u81cWiVrRg | http://safe.cnews.ru/ |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| **Вид занятий** | **Наименование оборудования,**  **программного обеспечения** |
| лекционные занятия | Компьютер с выходом в сеть Интернет, установленным пакетом стандартных программных продуктов (веб-браузер, средства работы с pdf документами, текстовые редакторы, видеопроигрыватель) |
| практические занятия | Компьютер с выходом в сеть Интернет, установленным пакетом стандартных программных продуктов (веб-браузер, средства работы с pdf документами, текстовые редакторы, видеопроигрыватель) |
| самостоятельная работа | Компьютер с выходом в сеть Интернет, установленным пакетом стандартных программных продуктов (веб-браузер, средства работы с pdf документами, текстовые редакторы, видеопроигрыватель) |

Приложение

к дополнительной профессиональной

программе повышения квалификации

**ПАСПОРТ КОМПЕТЕНЦИИ**

дополнительной профессиональной программы повышения квалификации

**«Комплексное обеспечение безопасности информации**

**и основы защиты персональных данных в образовательных учреждениях»**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **Наименование компетенции** | | способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации |
| **2** | **Указание типа компетенции** | | профессиональная |
| **3** | **Определение, содержание и основные сущностные характеристики компетенций** | | Под компетенцией понимается способность организовать техническую систему защиты информации, обслуживать ее и совершенствовать в соответствии с потребностями пользователей системы  **знать:**  - информационная безопасность: структура, состав, свойства, порядок организации безопасного информационного пространства в организации;  - основные виды угрозы безопасности информации и персональных данных; классификация нарушений безопасности, прямо или косвенно зависящих от операторов обработки персональных данных; основные виды и компоненты модели внешних угроз;  - основные программно-аппаратные, технические и криптографические средства защиты информации  **уметь**:  - определять внешних и внутренних нарушителей системы безопасности и их мотивы; определять актуальных информационные угрозы для организации;  - на основании исходных данных определять подходящий тип информационной системы защиты данных;  - выполнять обязанности оператора обработки и защиты информации в соответствии с требованиями законодательства и рекомендациями федеральных органов власти  **владеть**:  - навыками разработки модели угроз безопасности персональных данных для конкретной организации на основании требований ФСТЭК;  - навыками организации автоматизированной системы обработки информации, в том числе настройка аппаратных средств, программного обеспечения, хранения данных и организации обслуживающего персонала системы, ее пользователей;  - навыками практического управления системами программно-аппаратного, технического и криптографического свойства |
| **4** | **Дескриптор знаний, умений и навыков по уровням** | **Уровни формирования компетенций** | **Индикаторы** |
| **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать: основные компоненты системы защиты информации в организации  Уметь: определять внешние и внутренние информационные угрозы, подбирать технические средства способные противостоять угрозам безопасности  Владеть: навыками установки и настройки систем защиты информации под требования конкретной организации |
| **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать: порядок реализации модели информационной безопасности в организации, основные виды внешних и внутренних угроз  Уметь: подбирать походящие способы и системы защиты информации в зависимости от потребностей и масштабов организации  Владеть: навыками внедрения физических, аппаратных, программных средств защиты, исходя из потребностей организации |
| **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: классификация моделей защиты информации и основные программно-аппаратные, технические и криптографические средства используемые в каждом виде  Уметь: выполнять обязанности оператора обработки и защиты информации  Владеть: навыками установления требований к автоматизированным системам обработки информации в соответствии с критериями защищенности автоматизированных систем обработки информации от несанкционированного доступа |
| **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: типичные нарушения целостности системы информационной безопасности, основные виды криптографических способов защиты данных; классы безопасности информации  Уметь: предотвращать несанкционированное вторжение в системы защищенных данных, контролировать рабту и эффективность установленного программного комплекса  Владеть: навыками разработки модели угроз безопасности персональных данных для конкретной организации на основании требований ФСТЭК |
| **5** | **Характеристика взаимосвязи данной компетенции с другими компетенциями/необходимость владения другими компетенциями для формирования данной компетенции** | | способность ставить и решать прикладные задачи с использованием современных информационно-коммуникационных технологий |
| **6** | **Средства и технологии оценки** | | тестирование, решение контрольных и практических заданий |

**ПАСПОРТ КОМПЕТЕНЦИИ**

дополнительной профессиональной программы повышения квалификации

**«Комплексное обеспечение безопасности информации**

**и основы защиты персональных данных в образовательных учреждениях»**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **Наименование компетенции** | | способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности |
| **2** | **Указание типа компетенции** | | профессиональная |
| **3** | **Определение, содержание и основные сущностные характеристики компетенций** | | Под компетенцией понимается способность проводить анализ текущего состояния систем защиты информации и моментально реагировать на отклонение от нормы  **знать**:  - цели, задачи, принципы организации процесса защиты информации в организациях; основные угрозы безопасности, их виды и характеристики; несанкционированный доступ: виды, принципы защиты информации; возможные уровни защиты от несанкционированных доступов;  - уровни формирования режима информационной безопасности; девять классов защищенности автоматизированных систем от несанкционированного доступа, установленные документами ГКТ  - угрозы безопасности персональных данных; классификацию нарушений безопасности персональных данных, прямо или косвенно зависящий от операторов обработки персональных данных; основные виды и компоненты модели внешних угроз  **уметь**:  - подбирать эффективные способы защиты информационных систем в зависимости от существующих типов угроз; применять средства защиты информации;  - выполнять обязанности оператора обработки и защиты информации в соответствии с требованиями законодательства и рекомендациями федеральных органов власти  **владеть**:  - навыками проведения оценки эффективности и соответствия информационной системы организационно-техническим требованиям по защите персональных данных;  - навыками оформления заключения и составления предписания по устранению нарушений в области организации системы по защите персональных данных; навыками проведения аттестации объектов информатизации и персонала организации |
| **4** | **Дескриптор знаний, умений и навыков по уровням** | **Уровни формирования компетенций** | **Индикаторы** |
| **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать: способы и методы проведения анализа функционирования систем защиты информации  Уметь: оперативно реагировать на возникающие проблемы в функционировании систем безопасности данных  Владеть: навыками подготовки технической документации о функционировании систем защиты информации |
| **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать: основные угрозы безопасности, их виды и характеристики; несанкционированный доступ  Уметь: применять средства защиты информации и анализа их состояния в зависимости от текущей ситуации в организации  Владеть: навыками проведения первичного анализа функционирования систем защиты |
| **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: классификацию нарушений безопасности персональных данных, прямо или косвенно зависящий от операторов обработки персональных данных  Уметь: подбирать эффективные способы защиты информационных систем в зависимости от существующих типов угроз  Владеть: навыками проведения оценки эффективности и соответствия информационной системы организационно-техническим |
| **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: уровни формирования режима информационной безопасности, классы защищенности систем  Уметь: проводить комплексный анализ систем защиты информации, выявлять слабые зоны и искать пути их устранения  Владеть: навыками оформления заключения и составления предписания по устранению нарушений в системах защиты информации и порядку их качественного улучшения |
| **5** | **Характеристика взаимосвязи данной компетенции с другими компетенциями/необходимость владения другими компетенциями для формирования данной компетенции** | |  |
| **6** | **Средства и технологии оценки** | | тестирование, решение контрольных и практических заданий |

**ПАСПОРТ КОМПЕТЕНЦИИ**

дополнительной профессиональной программы повышения квалификации

**«Комплексное обеспечение безопасности информации**

**и основы защиты персональных данных в образовательных учреждениях»**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **Наименование компетенции** | | способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области защиты информации |
| **2** | **Указание типа компетенции** | | профессиональная |
| **3** | **Определение, содержание и основные сущностные характеристики компетенций** | | Под компетенцией понимается способность составлять локальную документацию и локальные нормативно-правовые акты в области защиты информации и конфиденциальных данных  **знать**:  - перечень основных законодательных актов, регулирующих вопросы защиты информации в Российской Федерации, а также дополнительные руководящие документы, приказы и стандарты, регламентирующие различные аспекты информационной безопасности и защиты персональных данных;  - основные виды ответственности за нарушение механизма обеспечения защиты информации и персональных данных в организации;  - основные задачи систем защиты информации в организациях; уровни формирования режима информационной безопасности.  **уметь**:  - применять нормы законодательства в процессе формирования систем и сервисов защиты информации и обеспечения конфиденциальности данных  - осуществлять документирование процессов по защите информации с построение системы уровневой иерархии  **владеть**:  - навыками разработки организационно-распорядительной и технической документации, отвечающей требованиям безопасности информации, регламентирующей процессы системы защиты информации на всех этапах её существования в организации;  - навыками инициализации, поддержки и контроля выполнения процессов при формировании и разработке организационно-распорядительной и технической документации по защите информации |
| **4** | **Дескриптор знаний, умений и навыков по уровням** | **Уровни формирования компетенций** | **Индикаторы** |
| **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать: законодательство Российской Федерации, регламентирующее основы обеспечения защиты информации и персональных данных в организациях  Уметь: применять нормы законодательства Российской Федерации в профессиональной деятельности  Владеть: навыками сбора и анализа существующей технической документации |
| **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать: основные задачи систем защиты информации в организациях; уровни формирования режима информационной безопасности  Уметь: осуществлять документирование процессов по защите информации  Владеть: навыками контроля выполнения норм законодательства и внутренних требований в организации |
| **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: основные положения и виды нормативно-правовых документов, закрепляющих основные вопросы защиты информации как на законодательном уровне, так и на уровне конкретной организации  Уметь: описывать трудовые процессы и функции, касающихся вопросов защиты информации в организации с построением уровневой иерархии  Владеть: навыками установления необходимого количества локальных нормативно-правовых актов, необходимых для успешной защиты информации в организации |
| **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: основные задачи систем защиты информации в организациях, применяемые нормы законодательства на каждом из уровней  Уметь: адаптировать деятельность организации, согласно требованиям законодательства, в области защиты информации  Владеть: навыками разработки локальных документов, регламентирующих вопросы защиты информации и обеспечения сохранности персональных данных |
| **5** | **Характеристика взаимосвязи данной компетенции с другими компетенциями/необходимость владения другими компетенциями для формирования данной компетенции** | |  |
| **6** | **Средства и технологии оценки** | | тестирование, решение контрольных и практических заданий |

**ПАСПОРТ КОМПЕТЕНЦИИ**

дополнительной профессиональной программы повышения квалификации

**«Комплексное обеспечение безопасности информации**

**и основы защиты персональных данных в образовательных учреждениях»**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **Наименование компетенции** | | способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации |
| **2** | **Указание типа компетенции** | | профессиональная |
| **3** | **Определение, содержание и основные сущностные характеристики компетенций** | | Под компетенцией понимается способность принимать участие и проводить аттестацию объектов информатизации по требованиям законодательства Российской Федерации в области защиты информации  **знать:**  - аттестация объектов информатизации и рабочего места сотрудников: порядок, положения, методы, виды  - основные виды оценки мер по обеспечению безопасности персональных данных; требования безопасности информации в системе сертификации ФСТЭК России; ГОСТ РО 0043-003-2012, ГОСТ РО 0043-004-2013;  - порядок и механизм идентификации и аутентификации пользователей в информационных системах  **уметь:**  - организовать систему обработки персональных данных обучающихся, подбирать функционал операторов и контролировать выполнение норм законодательства в области обработки данных граждан;  - на основании исходных данных определять подходящий тип информационной системы;  - определять класс защищенности автоматизированных систем, в зависимости от обрабатываемых данных; определять порядок и последовательность функций;  **владеть:**  - навыками проведения аттестации и рабочего места для работы в системе учета; контроля входа пользователей в систему и работа пользователей в системе; контроля вывода конфиденциальных данных на печать; контроля аппаратной конфигурации компьютера и подключаемых устройств; контроля сетевых интерфейсов; контроля целостности файлов, каталогов, элементов системного реестра;  - навыками установления требований к автоматизированным системам обработки информации в соответствии с критериями защищенности автоматизированных систем обработки информации от несанкционированного доступа; внедрять физические, аппаратные, программные средства защиты, исходя из потребностей организации |
| **4** | **Дескриптор знаний, умений и навыков по уровням** | **Уровни формирования компетенций** | **Индикаторы** |
| **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать: основные положения аттестации объектов безопасности и рабочего места сотрудника  Уметь: определять требования безопасности к рабочему месту сотрудника организации в зависимости от исполняемых обязанностей  Владеть: навыками внедрения физических, аппаратных, программных средств защиты, исходя из потребностей организации |
| **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать: общая культура безопасности данных в организации и контроль за функционирование данных  Уметь: осуществлять проверку соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных  Владеть: навыками организации полного внутреннего аудита информационных систем, организационных и физических мер обеспечения информационной безопасности |
| **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: порядок и механизм аттестации объектов в векторе защиты информации и данных  Уметь: проводить аттестацию рабочего места сотрудников организации и устанавливать требования к безопасности  Владеть: навыками контроля процесса аттестации и последующей эксплуатации |
| **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: основные виды оценки мер по обеспечению безопасности персональных данных; требования безопасности информации в системе сертификации ФСТЭК России; ГОСТ РО 0043-003-2012, ГОСТ РО 0043-004-2013  Уметь: на основании исходных данных определять подходящий тип информационной системы и проводить ее аттестацию в организации  Владеть: навыками установления требований к автоматизированным системам обработки информации в соответствии с критериями защищенности автоматизированных систем обработки информации от несанкционированного доступа |
| **5** | **Характеристика взаимосвязи данной компетенции с другими компетенциями/необходимость владения другими компетенциями для формирования данной компетенции** | |  |
| **6** | **Средства и технологии оценки** | | тестирование, решение контрольных и практических заданий |

**ПАСПОРТ КОМПЕТЕНЦИИ**

дополнительной профессиональной программы повышения квалификации

**«Комплексное обеспечение безопасности информации**

**и основы защиты персональных данных в образовательных учреждениях»**

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **Наименование компетенции** | | способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации, а также системы информационной безопасности в целом |
| **2** | **Указание типа компетенции** | | профессиональная |
| **3** | **Определение, содержание и основные сущностные характеристики компетенций** | | Под компетенцией понимается способность проводить контрольные проверки (внутренний и внешний аудит) функционирования систем защиты информации  **знать**:  - процесс проведения внутреннего и внешнего аудит;  - необходимый набор документов, необходимых для проверок различных уровней  **уметь**:  - организовать проверки различного уровня систем защиты информации и обработки персональных данных  **владеть**:  - навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации, а также системы информационной безопасности в целом |
| **4** | **Дескриптор знаний, умений и навыков по уровням** | **Уровни формирования компетенций** | **Индикаторы** |
| **Начальный уровень**  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать: системы защиты информации: индикаторы отклонения от нормы  Уметь: выявлять ошибки функционирования систем  Владеть: навыками обнаружения технических и организационных нарушений целостности системы защиты информации |
| **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать: порядок проведения внутреннего и внешнего аудита функционирования информационных систем  Уметь: проводить оценку и давать заключение о качестве работы систем  Владеть: навыками определения необходимых инструментов для организации качественной проверки |
| **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: необходимый набор документов, необходимых для проверок различных уровней  Уметь: проводить внутренний аудит информационных систем  Владеть: навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации |
| **Профессиональный**  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать: аудит безопасности персональных данных и конфиденциальной информации  Уметь: проводить внутренний аудит и оказывать содействие в проведении внешнего аудит систем защиты информации со стороны государственных органов  Владеть: навыками проведения контрольных проверок системы информационной безопасности в целом |
| **5** | **Характеристика взаимосвязи данной компетенции с другими компетенциями/необходимость владения другими компетенциями для формирования данной компетенции** | |  |
| **6** | **Средства и технологии оценки** | | тестирование, решение контрольных и практических заданий |