Бюджетное учреждение профессионального образования

Ханты–Мансийского автономного округа–Югры

«Нижневартовский социально–гуманитарный колледж»

БУ «Нижневартовский социально–гуманитарный колледж»

**ПРОГРАММА**

**повышения квалификации**

**«Обеспечение безопасности персональных данных в соответствии**

**с 152-ФЗ «О персональных данных»**

**Автор программы:** Астахов Михаил Сергеевич – начальник отдела технической защиты информации ООО «СЦСО «Надежда» г. Нижневартовска.

**Категория слушателей:** лица, назначенные ответственными за организацию обработки персональных данных в организации, сотрудники отдела кадров, сотрудники бухгалтерии, лица, назначенные администраторами безопасности в организации, лица, осуществляющие свою трудовую деятельность на аттестованных по требованиям безопасности ПЭВМ.

**Форма обучения:** *очно-заочная с применением дистанционных образовательных технологий и электронного обучения.*

**Программа одобрена на заседании** педагогического совета

БУ «Нижневартовский социально-гуманитарный колледж»

(протокол № 29 от 04 февраля 2021)

**Трудоемкость программы -** 72 часа

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Общий объём, час** | **Аудиторные занятия, час** | **Практические занятия, час** | **СРС (дистанционно), час** | **Форма итоговой аттестации, час** |
| 72 | 36 | 17 | 17 | 2 часа  Тестирование |

Нижневартовск, 2021

**ОГЛАВЛЕНИЕ**

[АННОТАЦИЯ 3](#_Toc59710903)

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4](#_Toc59710904)

[1. ЦЕЛЬ ПРОГРАММЫ. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ 5](#_Toc59710905)

[2. УЧЕБНЫЙ ПЛАН 8](#_Toc59710906)

[3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК 9](#_Toc59710907)

[4. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ 10](#_Toc59710908)

[5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ 17](#_Toc59710909)

[6. ФОРМЫ АТТЕСТАЦИИ 19](#_Toc59710910)

[7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И ИНЫЕ КОМПОНЕНТЫ 20](#_Toc59710911)

АННОТАЦИЯ

Программа повышения квалификации «Обеспечение безопасности персональных данных в соответствии с 152-ФЗ «О персональных данных» разработана с учётом требований Федерального закона от 28 декабря 2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Основой для разработки программы являются Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», а также документы, регламентирующие вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18 февраля 2013 № 21.

Программа включает пояснительную записку, основные требования к уровню освоения содержания дисциплины, учебный и учебно-тематический план, содержание разделов программы по модулям с кратким содержанием тематики, организационно-педагогические условия реализации программы, формы аттестации и оценочные материалы для обучения слушателей по программе, рассчитанной на 72 учебных часа.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа курсов повышения квалификации является актуализацией знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и образовательных организациях, организующих и (или) осуществляющих обработку персональных данных.

Нормативный срок освоения программы составляет 72 часа, в том числе: теоретическое обучение - 32 часов, практические занятия – 17 часов, самостоятельная работа - 17 часов, зачет – 2 часа.

Форма обучения: очно-заочная с применением дистанционных образовательных технологий.

1. ЦЕЛЬ ПРОГРАММЫ. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

**Цель программы**: освоение специалистами актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Поставленная цель достигается решением следующих задач:

- изучением нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;

- изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;

- практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

**ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

Имеющаяся квалификация (требования к слушателям):

* + 1. Предшествующий уровень образования слушателя – среднее профессиональное, высшее образование.
    2. Слушатель должен иметь документ государственного образца о среднем профессиональном, высшем образовании.

**Вид деятельности:** работа по защите персональных данных.

|  |  |  |  |
| --- | --- | --- | --- |
| **Профессиональные компетенции** | **Практический опыт** | **Умения** | **Знания** |
| * способности использовать нормативные правовые акты и методические документы в своей профессиональной деятельности (ПК-1); * способности формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-2); * способности определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-3); * способности применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-4); * способности организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-5); * способности применять программные средства системного, прикладного и специального назначения (ПК-6). | * правильно определять цели обработки персональных данных, категории субъектов, чьи данные обрабатываются на предприятии (в организации), и состав обрабатываемых персональных данных; * разрабатывать внутренние нормативные документы, регламентирующие организацию обработки и защиту персональных данных в соответствии с требованиями Федеральных законов и Постановлений Правительства Российской Федерации по защите персональных данных; * оценивать типы актуальных угроз безопасности персональных данных и уровни их защищенности, формировать частную актуальную модель угроз персональным данным; * оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации; * представлять интересы предприятия (организации) при проведении мероприятий государственного контроля и надзора; * готовить уведомления в уполномоченный орган по защите прав субъектов персональных данных | * создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных; * планировать мероприятия по обеспечению безопасности персональных данных; * обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных; * проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных; * определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных. | * основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; * основные виды угроз безопасности персональных данных в информационных системах персональных данных; * содержание и порядок организации работ по выявлению угроз безопасности персональных данных; * процедуры задания и реализации требований по защите информации в информационных системах персональных данных; * меры обеспечения безопасности персональных данных; * требования по обеспечению безопасности персональных данных; * порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. |

В рамках имеющейся квалификации слушатели осваивают следующие общие компетенции:

Слушатель в результате освоения программы усовершенствует следующие профессиональные компетенции:

* способности использовать нормативные правовые акты и методические документы в своей профессиональной деятельности (ПК-1);
* способности формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-2);
* способности определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-3);
* способности применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-4);
* способности организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю (ПК-5);
* способности применять программные средства системного, прикладного и специального назначения (ПК-6).

2. УЧЕБНЫЙ ПЛАН

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Раздел, тема** | **Виды учебной работы, включая самостоятельную работу слушателей и трудоемкость (в часах)** | | | | **Форма аттестации** |
| **Всего** | **Лекции**  (вебинар) | **Практические занятия** | **Самостоятельная**  **работа** |
| **1** | **Модуль 1. Общие вопросы технической защиты информации** | **22** | **14** | **4** | **4** | **тестирование** |
| 1.1. | Правовые и организационные основы технической защиты информации ограниченного доступа | 9 | 6 | 1 | 2 |  |
| 1.2. | Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа | 13 | 8 | 3 | 2 |  |
| **2.** | **Модуль 2. Организация обеспечении безопасности персональных данных в информационных системах персональных данных** | **46** | **22** | **13** | **13** | **тестирование** |
| 2.1 | Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 21 | 10 | 4 | 7 |  |
| 2.2. | Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 20 | 10 | 5 | 5 |  |
| 2.3. | Практические реализации типовых моделей защищённых информационных систем обработки персональных данных | 7 | 2 | 4 | 1 |  |
|  | Итоговая аттестация | 2 |  |  |  | Теститро  вание, |
|  | **Итого** | **72** | **36** | **17** | **17** | **2** |

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный план составляется при сформированной группе с учетом уровня их подготовки.

Календарный учебный график отражает периоды теоретических занятий, практик, процедур промежуточной и итоговой аттестаций и т.д.

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Учебные недели** | 1 | 2 | 3 | 4 |
| **Учебные занятия (Т)** | T | T | T | T |
| **Выездные занятия (В)** | – | – | – | – |
| **Стажировка (П)** | – | – | – | – |
| **Контроль**  **Зачет, экзамен (З, Э)** | – | З | З | – |
| **Итоговая аттестация (А)** | – | – | – | А |

4. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ

**Рабочая программа модуля 1. Общие вопросы технической защиты информации**

Количество часов: 22 ч., в т.ч. лекций - 14 ч., практическая работа – 4 ч., самостоятельная работа - 4 ч.

**Лекция (2ч.) Основные понятия в области технической защиты информации (ТЗИ).**

Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая харак­теристика ее основных составляющих.

**Лекция (2ч.) Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации**

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

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

**Лекция (2ч.) Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**

Федеральный Закон ФЗ-152 «О персональных данных», постановления Правительства РФ № 1119, № 684, приказы ФСТЭК России, ФСБ России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

**Лекция (2ч.) Основные понятия и область применения ФЗ-152 «О персональных данных».**

Содержание понятия «персональные данные». Сущность понятия обработки персональ­ных данных. Автоматизированная и неавтоматизированная обработка персональных данных. Смешанные информационные системы.

Условия обработки персональных данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных.

Специальные категории персональных данных и особенности их обработки. Особенности обработки биометрических данных.

Права субъектов персональных данных и их соблюдение при обработке.

Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Прекращение обработки.

Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

Контроль и надзор за обработкой персональных данных.

Ответственность за нарушение требований по обработке персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных

**Лекция (2ч.) Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы».**

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

**Лекция (2ч.) Классификация объектов информатизации**

Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз не­санкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов ТСР/IР.

**Лекция (2ч.) Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники**

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

**Практическая работа (2ч.)**

Подготовить образец уведомления об обработке персональных данных, для отправки в Роскомнадзор.

**Практическая работа (2ч.)**

Провести классификацию объекта информатизации.

**Самостоятельная работа (2ч.)**

Самостоятельно изучить документы:

* Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.
* Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
* Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗю

**Самостоятельная работа (2ч.)**

Самостоятельно изучить документы:

* Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ.
* Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 30.11.2020) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации").
* Постановление Правительства Российской Федерации от 16 апреля 2012 г. N 313 г. Москва "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)".

**Рабочая программа модуля 2. Организация обеспечении безопасности персональных данных в информационных системах персональных данных**

Количество часов: 46 ч., в т.ч. лекционных – 22 ч., практических – 13 ч., самостоятельная работа – 13 ч.

**Лекция (2 ч.).** **Подготовка к** **определению актуальных угроз безопасности.**

Сбор и анализ исходных данных по ИСПДн. Описание технологического процесса обработки информации.

**Лекция (2 ч.).**  **Определение актуальных угроз безопасности персональных данных.**

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

Каналы утечки информации при ее обработке в ИСПДн, определение типов актуальных угроз безопасности персональных данных.

**Лекция (2 ч.).**  **Методика формирования модели угроз безопасности ПДн.**

Подготовка модели угроз безопасности ПДн, уточнение модели угроз ПДн и модели нарушителей.

**Лекция (2 ч.).**  **Основные принципы обеспечения безопасности персональных данных при их обработке.**

Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах пер­сональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.

**Лекция (2 ч.).**  **Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.**

Классификация информационных систем персональных данных по уровням защищенности.

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

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

**Лекция (2 ч.).**  **Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.**

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

**Лекция (2 ч.).**  **Организация обеспечения безопасности персональных данных в организациях и учреждениях.**

Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.

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

**Лекция (2 ч.).**  **Общая структура внутренней нормативной документации организации по защите ПДн.**

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

**Лекция (2 ч.).**  **Обязанности оператора, осуществляющего обработку персональных данных.**

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

**Лекция (2 ч.).**  **Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации.**

Основное содержание этапов организации обеспечения безопасности персональных данных.

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

**Лекция (2 ч.).**  **Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных.**

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

**Практическая работа (6 ч.)**

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

**Практическая работа (4 ч.)**

Практические реализации типовых моделей защищённых информационных систем обработки персональных данных.

**Практическая работа (3 ч.)**

Проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

**Самостоятельная работа (3 ч.)**

Самостоятельно изучить документы:

* Приказ ФСТЭК России от 18 февраля 2013 г. N 21
* Приказ ФСТЭК России от 11 февраля 2013 г. N 17

**Самостоятельная работа (3 ч.)**

* Самостоятельно изучить документ Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

**Самостоятельная работа (3 ч.)**

Самостоятельно изучить документы:

* Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».
* Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014) «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».

**Самостоятельная работа (4 ч.)**

Самостоятельно изучить документы:

* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением заместителя директора ФСТЭК России от 14 февраля 2008 г.
* Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 06.09.2014) «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».
* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением заместителя директора ФСТЭК России от 14 февраля 2008 г.
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением заместителя директора ФСТЭК России от 15 февраля 2008 г
* Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

**5.1. Материально-техническое оснащение курса**

При организации образовательного процесса по программе профессионального обучения в целях реализации компетентностного подхода используются интерактивные технологии, ориентированные на овладение слушателями способов самостоятельной деятельности, личностно-ориентированные технологи, способствующие развитию активности личности обучающегося в учебном процессе.

Слушатели, планирующие обучение с применением дистанционных технологий, должны иметь в своем распоряжении персональный компьютер, доступ в интернет, персональный адрес электронной почты и соответствующие навыки компьютерной грамотности.

Все взаимодействие со слушателями рассылка новостей, информационные материалы, техническая поддержка и пр. осуществляется только по электронной почте.

Одновременно с этим, слушатели получают по электронной почте регистрационный идентификатор логин и пароль доступа к своей персональной странице в системе дистанционного обучения, на которой расположены календарный план обучения, электронные образовательные материалы, методические указания, тестовые контрольные ресурсы и др.

Рекомендуемое программное обеспечение: установленная программа просмотра PDF файлов: AdobeAcrobatReader или аналогичный. Минимальные версии веб-браузеров: Coogle Chrome 11, Opera 9. Архиватор 7zip или аналогичные. Офисные пакеты: OpenOffice, MS Office или другой.

5.2. Учебно-методическое и информационное обеспечение курса

5.2.1. Программное обеспечение и интернет ресурсы:

а) программное обеспечение и Интернет-ресурсы;

б) наглядные средства обучения (презентации, схемы, таблицы, графики и т.д.).

5.2.2. Литература

5.2.2.1. Нормативные правовые акты

1. Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».
3. Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации».
4. Указ Президента РФ от 31.12.2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации».
5. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 № Пр- 1753).
6. Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
7. Указ Президента РФ от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Постановление Правительства РФ от 03.11.1994 г. №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
9. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
10. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
11. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
12. Приказ Роскомнадзора от 05.09.2013г №996 "Об утверждении требований и методов по обезличиванию персональных данных" (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»).
13. Приказ Роскомнадзора от 30 мая 2017 года №94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».
14. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в ИСПДн» (утв. Приказом ФСТЭК от 18.02.2013 №21)

5.2.2.2. Основная литература.

* + - 1. Аверченков, В. И. Защита персональных данных в организациях / В.И. Аверченков. - М.: Флинта, 2011. - 486 с.
      2. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А.В. Благодаров и др. - М.: Горячая линия - Телеком, 2013. -116 с.
      3. Бойкова, Ольга Феоктистовна Защита персональных данных: касается всех! Практическое пособие. Выпуск № 142 / Бойкова О.Ф. - М.: Либерея, 2012. - 663 с.
      4. Кин, Эндрю Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные для собственной выгоды / Эндрю Кин. - М.: Альпина Паблишер, 2016. - 224 с.
      5. Мещеряков, Роман Валерьевич Защита персональных данных в организациях здравоохранения / Мещеряков Роман Валерьевич. - М.: Горячая линия - Телеком, 2012. - 419 с.
      6. Новая парадигма защиты и управления персональными данными. - Москва: СПб. [и др.]: Питер, 2016. - 512 с.

6. ФОРМЫ АТТЕСТАЦИИ

**Промежуточная аттестация**

Промежуточная аттестация проводится по итогам каждого учебного модуля программы в соответствии с учебным планом и календарным учебным графиком образовательной программы. Формы промежуточной аттестации – итоговая практическая работа, тестирование.

**Итоговая аттестация**

Итоговая аттестация позволяет выявлять уровень теоретической и практической подготовки слушателей в соответствии с требованиями программы. Итоговая аттестация проводится в форме тестирования. Тестирование позволяет проверять у слушателей не только сформированность профессиональных компетенций, но и развитие общих компетенций.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И ИНЫЕ КОМПОНЕНТЫ

|  |  |  |
| --- | --- | --- |
| **Вид работы** | **Тема работы** | **Ожидаемые результаты, демонстрируемые слушателем при выполнении данного вида работы** |
| Тестирование | Общие вопросы технической защиты информации | Знать:   * Правовые и организационные основы технической защиты информации ограниченного доступа * Методические документы описывающие способы выявления угроз безопасности информации на объектах информатизации * Основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа |
| Тестирование | Организация обеспечении безопасности персональных данных в информационных системах персональных данных | Знать:   * Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных * Практические реализации типовых моделей защищённых информационных систем обработки персональных данных * технические меры защиты информации в информационных системах персональных данных |
| Итоговое тестирование |  | Знать:   * Общие вопросы технической защиты информации * Методы организации обеспечении безопасности персональных данных в информационных системах персональных данных |