1. **Паспорт Образовательной программы**

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 14**.**10**.**2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Учебный центр ООО "Сплайнер" |
| 1.2 | Логотип образовательной организации | D:\YandexDisk\КУРСЫ ДПО\ДПО СПЛАЙНЕР\Bezymyanny-2.jpg |
| 1.3 | Провайдер ИНН | 0257011283 |
| 1.4 | Ответственный за программу ФИО | Соколов Геннадий Александрович |
| 1.5 | Ответственный должность | Старший преподаватель |
| 1.6 | Ответственный Телефон | 89093491822 |
| 1.7 | Ответственный Е-mail | 2991822@mail.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных |
| 2.2 | Ссылка на страницу программы | http://дпоплатформа.рф/glavnaya |
| 2.3 | Формат обучения | Онлайн |
| 2.4 | 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 | подтверждаем |
| 2.5 | Уровень сложности | Базовый |
| 2.6 | Количество академических часов | **72** |
| 2.7 | 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) | 38 |
| 2.8 | 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 30 000 руб,  Ссылка №1: <https://www.academyit.ru/courses/%D0%A2%D0%97%D0%9A%D0%98001/>  Ссылка №2: <https://www.infosystems.ru/courses/kursy_soglasovannye_s_federalnymi_organami/obespechenie_bezopasnosti_personalnykh_dannykh_pri_ikh_obrabotke_v_informatsionnykh_sistemax_persona/>  Ссылка №3: <https://itsecurity.ru/catalog/pk123/> |
| 2.9 | Минимальное количество человек на курсе | 3 |
| 2.10 | Максимальное количество человек на курсе | 2000 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 3 слушателя в 2020 г. |
| 2.12 | Формы аттестации | Тестирование по каждому модулю, Итоговая аттестация в форме тестирования |
| 2.13 | 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**

Курс по обеспечению безопасности персональных данных ориентирован на подготовку специалистов различных категорий, от руководителей предприятий и их структурных подразделений до лиц, ответственных за организацию обработки персональных данных.

Курс по обеспечению безопасности персональных данных позволяет получить знания, необходимые для обработки персональных данных в соответствии с требованиями российских законов. Особое внимание уделяется вопросам технической реализации требований законодательства по защите персональных данных.

Характеристика новой квалификации и связанных с ней видов профессиональной деятельности: область профессиональной деятельности слушателя, прошедшего обучение по программе повышения квалификации – организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Программа повышения квалификации составлена с учетом требований профессионального стандарта «Специалист по защите информации в автоматизированных системах». Регистрационный номер 843. Утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. №522н.

Уровень квалификации: 5 (для лиц, имеющих среднее профессиональное образование либо высшее непрофильное образование), 6 (для лиц, имеющих высшее профильное образование).

В результате обучения слушатель будет иметь способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности, а также определять виды и формы информации в информационных системах персональных данных, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия.

1. ШАБЛОН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ДПО)

Титульный лист программы

Название организации

Дополнительная профессиональная программа повышения квалификации

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных »

72 час.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Целью освоения программы «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» является освоение актуальных изменений в вопросах профессиональной деятельности, обновление 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.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

2.1.2 основные виды угроз безопасности персональных данных в информационных системах персональных данных

2.2. Умение (способность к деятельности)

2.2.1. уметь планировать мероприятия по обеспечению безопасности персональных данных;

2.2.2 уметь разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных

2.3.Навыки (использование конкретных инструментов)

2.3.1 владеть навыками определения уровня защиты персональных данных;

2.3.2 владеть навыками выявления угроз безопасности персональных данных в информационных системах персональных данных.

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

* 1. К освоению программы допускаются лица, имеющие среднее профессиональное или высшее образование.
  2. Квалификация
  3. Наличие опыта профессиональной деятельности
  4. Предварительное освоение иных дисциплин/курсов /модулей

**4.Учебный план программы «**Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных**»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Модуль 1. Общие вопросы технической зашиты информации | 16 | 8 | - | 8 |
| 2 | Модуль 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных | 16 | 8 | - | 8 |
| 3 | Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 16 | 8 | - | 8 |
| 4 | Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 16 | 6 | - | 10 |
| 5 | Модуль 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных | 6 | 2 | - | 4 |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачёт, реферат и т.д.)** | | |
| 2 | | 72 | Зачет | | |

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

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Модуль 1. Общие вопросы технической зашиты информации | 16 | 1.11.2020 - 3.11.2020 |
| **2** | Модуль 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных | 16 | 4.11.2020 - 5.11.2020 |
| 3 | Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 16 | 6.11.2020 - 8.11.2020 |
| 4 | Модуль 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 16 | 9.11.2020 - 11.11.2020 |
| 5 | Модуль 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных | 6 | 12.11.2020- 14.11.2020 |
| 6 | Итоговая аттестация | 2 | 14.11.2020 |
| **Всего:** | | 72 | 14 дней |

**6.Учебно-тематический план программы «**  Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Модуль 1. Общие вопросы технической зашиты информации | 16 | 8 | - | 8 | тестирование |
| 1.1 | Актуальность проблемы обеспечения безопасности персональных данных в информационных системах и сети интернет. | 6 | 4 | - | 2 | тестирование |
| 1.2 | Правовое регулирование в области защиты персональных данных. Нормативные правовые акты в области персональных данных. | 10 | 4 | - | 6 | тестирование |
| 2 | Организация обеспечения безопасности персональных данных в информационных системах персональных данных | 16 | 8 | - | 8 | тестирование |
| 2.1 | Разъяснения о вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки. | 8 | 4 | - | 4 | тестирование |
| 2.2 | Основные положения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных». | 8 | 4 | - | 4 | тестирование |
| 3 | Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | 16 | 8 | - | 8 | тестирование |
| 3.1 | Основные организационно-технические меры защиты информации. Угрозы безопасности персональных данных. | 8 | 4 | - | 4 | тестирование |
| 3.2 | Определение уровня защищённости информационных систем персональных данных. | 8 | 4 | - | 4 | тестирование |
| 4 | Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | 16 | 6 | - | 10 | тестирование |
| 4.1 | Перечень мер по обеспечению безопасности персональных данных при их обработке. | 8 | 4 | - | 4 | тестирование |
| 4.2 | Государственные регуляторы в области защиты персональных данных. Рекомендуемый перечень мер по защите персональных данных. | 8 | 2 | - | 6 | тестирование |
| 5 | Практические реализации типовых моделей защищенных информационных систем обработки персональных данных | 6 | 2 | - | 4 | тестирование |
| 5.1 | Разработка пакета внутренних документов по защите персональных данных. Виды ответственности за нарушения законодательства Российской Федерации о персональных данных. Штрафы за нарушения законодательства РФ в области персональных данных. | 4 | 2 | - | 2 | тестирование |
| 5.2 | Разработка комплекта документов по персональным данным. Бланк приказа о назначении ответственного. Образец Должностной инструкции. | 2 | - | - | 2 | тестирование |
| 6 | Итоговая аттестация | 2 | - | - | - | тестирование |

**7. Учебная (рабочая) программа повышения квалификации «**  Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных  **»**

**Модуль 1.** Общие вопросы технической зашиты информации **(**16 **час.)**

**Тема 1.1** Актуальность проблемы обеспечения безопасности персональных данных в информационных системах и сети интернет **(** 6 **час)**

Приводится информация об актуальности проблемы обеспечения безопасности персональных данных в информационных системах и сети интернет

**Тема 1.2** Правовое регулирование в области защиты персональных данных. Нормативные правовые акты в области персональных данных. (10 час)

Приводится информация о правовом регулирование в области защиты персональных данных, а также перечень нормативных правовых актов в области персональных данных (ФЗ, Приказы, постановления и т.п.)

**Модуль 2.** Организация обеспечения безопасности персональных данных в информационных системах персональных данных **(**16 **час.)**

**Тема 2.1.** Разъяснения о вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки.

Приводится информация о вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки

Тема 2.2. Основные положения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

В этом модуле приводятся основные положения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»

Модуль 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных (16 час)

Тема 3.1 Основные организационно-технические меры защиты информации. Угрозы безопасности персональных данных.

Приводится информация об основных организационно-технические мерах защиты информации, а также о возможных угрозах безопасности персональных данных.

Тема 3.2 Определение уровня защищённости информационных систем персональных данных.

Приводится информация об уровне защищённости информационных систем персональных данных.

Модуль 4 Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (16 час)

Тема 4.1 Перечень мер по обеспечению безопасности персональных данных при их обработке.

Приводятся перечни мер по обеспечению безопасности персональных данных при их обработке.

Тема 4.2 Государственные регуляторы в области защиты персональных данных. Рекомендуемый перечень мер по защите персональных данных.

Приводятся государственные регуляторы в области защиты персональных данных, а также рекомендуемый перечень мер по защите персональных данных.

Модуль 5 Практические реализации типовых моделей защищенных информационных систем обработки персональных данных

5.1 Разработка пакета внутренних документов по защите персональных данных. Виды ответственности за нарушения законодательства Российской Федерации о персональных данных. Штрафы за нарушения законодательства РФ в области персональных данных.

Приводятся примеры разработанных документов по защите персональных данных, виды ответственности за нарушения законодательства Российской Федерации о персональных данных, а также штрафы за нарушения законодательства РФ в области персональных данных.

5.2 Разработка комплекта документов по персональным данным. Бланк приказа о назначении ответственного. Образец Должностной инструкции.

Приводятся пример разработки комплекта документов по персональным данным, бланк приказа о назначении ответственного и образец Должностной инструкции.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1** | Модуль 1. Тема 1.2 | Правовое регулирование в области защиты персональных данных. Нормативные правовые акты в области персональных данных. | Самостоятельно составьте список в порядке значимости (от большей к меньшой) нормативных правовых актов в области персональных данных |
| 2 | Модуль 2. Тема 2.2 | Основные положения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных». | Самостоятельно составьте документ под названием «Согласие на обработку персональных данных» для работников коммерческой организации ООО «Ромашка». |
| 3 | Модуль 3. Тема 3.2 | Определение уровня защищённости информационных систем персональных данных. | Перед тем, как начать собирать персональные данные, оператору необходимо уведомить об этом Роскомнадзор в соответствии [ч. 1 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_61801/d996966e22e1320c9de1ab82d9f6be12c3d9d765/) «О персональных данных». Внимательно изучив Приказ Роскомнадзора от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения", найдите ошибки в представленном варианте уведомления публичным акционерным обществом «Сувенир». |
| 4 | Модуль 4. Тема 4.1 | Перечень мер по обеспечению безопасности персональных данных при их обработке. | Перед Вами стоит задача по формированию приказа о назначении ответственного за организацию обработки персональных данных работников. Вам поможет представленный далее образец и комментарии к нему. |
| 5 | Модуль 5. Тема 5.1 | Разработка пакета внутренних документов по защите персональных данных. Виды ответственности за нарушения законодательства Российской Федерации о персональных данных. Штрафы за нарушения законодательства РФ в области персональных данных. | Перед Вами представлены следующие документы:  -инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.  -приказ о назначении ответственного за обеспечение безопасности персональных данных в информационной системе.  Вам нужно переделать эти документы, чтобы они конкретно подходили под Вашу организацию. Укажите полное наименование, а также организационно-правовую форму Вашей организации. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1.1** | **Тип законодательного акта, которая носит обязательный характер и имеет верховенство над национальным правом:**  **-директива**  **-закон**  **- регламент** | Масштабы компьютерной преступности в РФ:  - Возрастают  - Снижаются  - Остаются неизменными | В каком году принят Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR:  - 2016  - 2018  - 2001 |
| **1.2** | Какой закон является основным в области обеспечения безопасности персональных данных?  - Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"  - Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»  - Закон Российской Федерации от 27.12.1991 года № 2124-1 «О средствах массовой информации» | Обладателем информации может быть:  - гражданин (физическое лицо),  - юридическое лицо  Российская Федерация,  -муниципальное образование  все вышеперечисленное | Отношения, связанные с обработкой персональных данных, регулируются  - Федеральным законом «О персональных данных»  - Федеральным законом «О защите информации»  - Федеральным законом «О конфиденциальной информации» |
| 2.1 | **Субъект персональных данных – это**  **-**физическое лицо  -государство  -различные учреждения | В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет:  -оператор  - лицо, осуществляющее обработку персональных данных по поручению оператора  - оба несут ответственность солидарно | Специальные категории персональных данных – это:  - персональные данные, касающиеся расовой, национальной принадлежности,  - политических взглядов, религиозных или философских убеждений,  - состояния здоровья, интимной жизни |
| 2.2 | К принципам обработки персональных данных относится  - ограничение достижений конкретных, заранее определенных и законных целей.  - объединение баз данных, содержащих персональные данные.  - обработка персональных данных, несовместимая с целями сбора персональных данных. | Автоматизированная обработка персональных данных – это:  - обработка персональных данных с помощью средств вычислительной техники;  - обработка персональных данных пользователя с применением компьютера;  - обработка персональных данных с использованием средств автоматизации; | **ЭЦП – это:**  - электронно-цифровая подпись  - электронно-цифровой преобразователь  - электронно-цифровой процессор |
| 3.1 | Информационная система, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных является:  - информационной системой, обрабатывающей специальные персональные данные  - информационной системой, обрабатывающей биометрические персональные данные  - информационной системой, обрабатывающей общедоступные персональные данные | Действие Приказа ФСТЭК №17 распространяется на:  - операторов государственных информационных систем  - всех операторов персональных данных  - операторов информационных систем, содержащих информацию, составляющую государственную тайну | Что мы получаем по итогу разработки модели угроз?  - перечень актуальных угроз  - перечень наиболее опасных угроз  - перечень наиболее вероятных угроз |
| 3.2 | Нарушитель безопасности персональных данных – это  - Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;  - Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;  - Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных. | Для того чтобы снизить вероятность утраты информации необходимо:  - регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)  - регулярно производить антивирусную проверку компьютера  - регулярно выполнять проверку жестких дисков компьютера на наличие ошибок | Какое из свойств защищаемой информации не является основным?  - регистрируемость  - доступность  - целостность |
| 4.1 | В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор:  - вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований  - обязан перекатить обработку персональных данных - вправе продолжить обработку персональных данных | Сколько существует уровней защищенности, которые необходимо обеспечить персональным данным в соответствии с постановлением Правительства №1119?  - 4  - 2  - 3 | Какой орган разработал методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных?  - ФСТЭК - ФСБ - Роскомнадзор |
| 4.2 | Какой орган осуществляет надзор в сфере криптографической защиты информации? - ФСБ - ФСТЭК - Роскомнадзор | Оператор обязан опубликовать на сайте документ, определяющий его политику в отношении обработки персональных данных в случае, если:  - оператор –государственный или муниципальный орган  - оператор – юридическое лицо или физическое лицо   - в любом случае | Сколько существует уровней защищенности, которые необходимо обеспечить персональным данным в соответствии с постановлением Правительства №1119?  - 4  - 2  - 3 |
| 5.1 | Что обязательно нужно разместить на официальном сайте муниципального органа?  - документы, определяющие политику в отношении обработки персональных данных  - форму согласия на обработку персональных данных  - положение о защите персональных данных | В какой орган нужно отправить Уведомление об обработке персональных данных?  - территориальный орган Управления Роскомнадзора  - администрация района  - департамент информационных технологий | Какая ответственность предусмотрена за нарушение трудового  кодекса Российской Федерации в части персональных данных?  - дисциплинарная и материальная  - административная,  - гражданско-правовая  уголовная |
| 5.2 | Перед кем оператор персональных данных несет ответственность?  - перед субъектом персональных данных  - перед Роскомнадзором  - не перед кем не несет ответственности | В статье 272 уголовного кодекса говорится…  - о неправомерном доступе к компьютерной информации  - о создании, исполнении и распространении вредоносных программ для ЭВМ  - о преступлениях в сфере компьютерной информации | Если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок не превышающий:  - 30 рабочих дней.  - 7 рабочих дней;  - 10 рабочих дней; |

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

Критерии оценки по 4-х балльной шкале

|  |  |
| --- | --- |
| Оценка  экзаменатора,  уровень | Критерии (дописать критерии в соответствии с компетенциями) |
| «отлично»,  высокий уровень | Слушатель показал прочные знания основных положений учебной программы (дисциплины), умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов расчетов или экспериментов |
| «хорошо», повышенный уровень | Слушатель показал прочные знания основных положений учебной программы (дисциплины), умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты расчетов или эксперимента |
| «удовлетворительно»,  пороговый уровень | Слушатель показал знание основных положений учебной программы (дисциплины), умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой |
| «неудовлетворительно», ниже порогового уровня | При ответе обучающегося выявились существенные пробелы в знаниях основных положений учебной программы (дисциплины), неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой |

2.4 Критерии оценки по 2-х балльной шкале

|  |  |
| --- | --- |
| Результат зачета | Критерии (дописать критерии в соответствии с компетенциями) |
| «зачтено» | Слушатель показал знания основных положений учебной программы (дисциплины), умение решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты расчетов или эксперимента |
| «не зачтено» | При ответе обучающегося выявились существенные пробелы в знаниях основных положений учебной программы (дисциплины), неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины |

Шкала оценивания компетенций

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Виды оценок | Оценки | | | |
| Академическая оценка по 4-х балльной шкале | неудовлетворительно  (менее 60% правильных ответов) | удовлетворительно  (60%-70% правильных ответов) | хорошо  (70%-85% правильных ответов) | отлично  (85%-100% правильных ответов) |
| Академическая оценка по 2-х балльной шкале | Не зачтено  (менее 60% правильных ответов) | Зачтено  (более 60% правильных ответов) | | |

**.**

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

Пример задание 3. (Модуль 3)

Перед тем, как начать собирать персональные данные, оператору необходимо уведомить об этом Роскомнадзор в соответствии [ч. 1 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_61801/d996966e22e1320c9de1ab82d9f6be12c3d9d765/) «О персональных данных». Внимательно изучив Приказ Роскомнадзора от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения", найдите ошибки в представленном варианте уведомления публичным акционерным обществом «Сувенир».

( Бланк организации)

Руководителю Управления Федеральной  службы

по надзору в сфере связи, информационных

технологий  и массовых коммуникаций

по Московской области

 УВЕДОМЛЕНИЕ

об обработке (о намерении осуществлять обработку) персональных данных

 Наименование, адрес оператора: Публичное акционерное общество «Сувенир» (ПАО «Сувенир» ), 100000, г. Москва, ул. Сувенирная, д.1, тел 8 (495) 111-11-11.

ИНН 5011111111, КПП 501101001, ОГРН 1055011111111.

Правовое основание обработки персональных данных: руководствуясь Уставом ПАО «Сувенир», Трудовым кодексом РФ; Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»; гл.4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон «Об акционерных обществах» от 26.12.1995 № 208-ФЗ,  лицензия № 00022 от 01.0.2020.  на оказание услуг

с целью (обработки персональных данных) учета сотрудников ПАО и иных физических лиц, оказание услуг.

осуществляет обработку следующих категорий персональных данных: ФИО, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы, контактный телефон принадлежащих следующим категориям субъектов персональных данных: сотрудникам, состоящим в трудовых отношениях, и  физическим лицам, находящимся в договорных и иных гражданско-правовых отношениях с ПАО.

 Обработка вышеуказанных персональных данных: осуществляется смешанно путем сбора, систематизации, накопления, хранения, уточнения, использования, передачи, удаления, уничтожения. Электронная обработка ведется на компьютерах, объединенных в локальную сеть, с передачей по внутренней сети, без передачи по сети Интернет.

Для обеспечения безопасности персональных данных принимаются следующие меры: Организационные и технические меры. Изданы приказы и разработаны и утверждены документы по организации работы по защите персональных данных,  приказом от 01.01.2020г.назначен Попов Семен Семенович ответственным лицом за организацию обработки персональных данных (тел. 8(495) 111-11-10, 100000, г. Москва, ул. Сувенирная, д. 1, souvеnirа@vail.ru Шифрование информации и не производится. Информационная система не классифицирована.

Сведения о наличии или об отсутствии трансграничной передачи персональных данных: трансграничная передача персональных данных не осуществляется

Сведения об обеспечении безопасности персональных данных: Информация доступна для строго определенных сотрудников, хранится на бумажных носителях в сейфе, а в персональных компьютерах хранится с доступом через пароль. Помещения, в которых находятся (бумажные и электронные) носители информации, относящейся к персональным данным,  запираются под ключ и сдаются под охранную сигнализацию.

Дата начала обработки персональных данных: 01.12.2019 г.

Срок или условие прекращения обработки персональных данных: изъятие полномочий по обработке персональных данных, ликвидация.

 Руководитель                                                            В.В.Иванов

10.01.2020 г.

         М.П.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В рассматриваемом варианте оператор, в нарушение требований законодательства, указал неполный перечень обрабатываемых персональных данных: ИНН, СНИЛС, сведения о воинском учете.

Указание неполного перечня обрабатываемых персональных данных – одно из типовых нарушений в сфере обработки персональных данных.

**.**

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

Обучающие задачи для самостоятельной работы:

Задание 1. (Модуль 1)

Самостоятельно составьте список в порядке значимости (от большей к меньшой) нормативных правовых актов в области персональных данных

Задание 2. (Модуль 2)

Самостоятельно составьте документ под названием «Согласие на обработку персональных данных» для работников коммерческой организации ООО «Ромашка».

Важно! Перечень основных моментов, которые должны быть отражены в документе, закрепляющем согласие на обработку персональных данных, содержится в п. 4 ст. 9 закона № 152-ФЗ. Бланк согласия на обработку персональных данных не имеет законодательно утвержденной формы. Каждый получатель персональной информации может разработать форму согласия самостоятельно, отразив в ней необходимый ему перечень сведений и особенности их обработки.

Задание 3. (Модуль 3)

Перед тем, как начать собирать персональные данные, оператору необходимо уведомить об этом Роскомнадзор в соответствии [ч. 1 ст. 22 Федерального закона от 27.07.2006 г. № 152-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_61801/d996966e22e1320c9de1ab82d9f6be12c3d9d765/) «О персональных данных». Внимательно изучив Приказ Роскомнадзора от 30.05.2017 № 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения", найдите ошибки в представленном варианте уведомления публичным акционерным обществом «Сувенир».

( Бланк организации)

Задание 4. (Модуль 4)

Перед Вами стоит задача по формированию приказа о назначении ответственного за организацию обработки персональных данных работников. Вам поможет представленный ниже образец и комментарии к нему.

В самом начале приказа напишите название компании, наименование распоряжения, его номер и дату составления. Затем переходите к основной части.

Обязательно укажите в связи с какими обстоятельствами создается приказ (это будет его обоснование) и поставьте ссылку на норму закона или внутренний документ компании, имеющий непосредственное отношение к формированию распоряжения (это будет основание).

Потом внесите собственно указание о назначении ответственного лица, обозначив его должность и ФИО.

Коротко отметьте его основные функции и обязанности (полный их перечень лучше привести в соответствующей должностной инструкции), а также впишите сведения о работнике (также должность и ФИО), который будет замещать ответственного сотрудника в период его отсутствия на работе по уважительным причинам.

В завершение не забудьте возложить контроль за исполнение данного распоряжение на кого-либо из руководящего состава предприятия (следует отметить, что контролировать выполнение приказа может и сам директор), а также собрать все необходимые подписи.

Образец

Задание 5. (Модуль 5)

Перед Вами представлены следующие документы:

-инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

-приказ о назначении ответственного за обеспечение безопасности персональных данных в информационной системе.

Вам нужно переделать эти документы, чтобы они конкретно подходили под Вашу организацию. Укажите полное наименование, а также организационно-правовую форму Вашей организации.

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

1 Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные

(конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2 Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

− Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

− Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

− Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

− Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

− Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

− Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

− Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

− Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

− Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

− Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

− Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

− Обязан проводить мероприятия по организации антивирусной защиты;

− Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

− Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

− Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

− Установить причины, по которым стал возможным НСД;

− Установить последствия, к которым привел НСД;

− Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

− Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при

необходимости провести настройку;

− Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3 Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

− Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

Примеры тестовых заданий:

Что такое персональные данные?

любая информация, относящаяся к прямо определенному или определяемому физическому лицу (субъекту персональных данных)

любая информация, относящаяся к косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

все перечисленное

2. Что такое GDPR?

общий регламент по защите персональных данных Европейского союза

общий регламент по защите персональных данных Российской федерации

общий регламент по защите персональных данных в мире

3. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц – это…

предоставление персональных данных

распространение персональных данных

обезличивание персональных данных

4. Что относится к специальным персональным данным?

политические взгляды

телефон

адрес электронной почты

5. Какой орган осуществляет и организует в соответствии с федеральным законодательством сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств?

ФСБ

ФСТЭК

Роскомнадзор

6. Какой штраф предусмотрен для юридического лица за невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных?

20-40 тыс. руб

не предусмотрен

10-20 тыс. руб

7. Какой орган осуществляет нормативно-правовое регулирование вопросов технической защиты информации?

1. ФСТЭК

2. Роскомнадзор

3. ФСБ

8. Какие угрозы связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в ИСПДн?

угрозы 1-го типа

угрозы 2-го типа

угрозы 3-го типа

9. Сколько существует уровней защищенности персональных данных?

4

3

10

10. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на:

1. оператора персональных данных

2. субъекта персональных данных

3. все вышеперечисленное

11. К принципам обработки персональных данных относится

ограничение достижений конкретных, заранее определенных и законных целей.

объединение баз данных, содержащих персональные данные.

обработка персональных данных, несовместимая с целями сбора персональных данных.

**12. Субъект персональных данных – это**

физическое лицо

государство

различные учреждения

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

оператор

лицо, осуществляющее обработку персональных данных по поручению оператора

оба несут ответственность солидарно

**14.** Автоматизированная обработка персональных данных – это

обработка персональных данных с помощью средств вычислительной техники;

обработка персональных данных пользователя с применением компьютера;

обработка персональных данных с использованием средств автоматизации;

**15.** Специальные категории персональных данных – это

персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни

персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни жизни

персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни

16. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность это-

Биометрические персональные данные

Специальные персональные данные

Общедоступные персональные данные

17. Информационная система (ИС) -

совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

программное обеспечение, предназначенное для работы с базами данных

упорядоченные наборы данных

**18. ЭЦП – это:**

электронно-цифровая подпись

электронно-цифровой преобразователь

электронно-цифровой процессор

**19.** Обработка специальных категорий персональных данных допускается, если:

субъект персональных данных дал согласие в письменной форме

персональные данные сделаны общедоступными оператором персональных данных

субъект персональных данных дал согласие в устной или письменной форме

**20.** На какие отношения распространяется действие Федерального закона «О персональных данных»?

на отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами

на отношения, возникающие при обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных

на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну

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

Контроль результатов обучения обучающимися, этапов и уровня формирования компетенций по дисциплине осуществляется через проведение входного, текущего, итогового контролей.

Изучаемы курс состоит из набора модулей. Объем учебного материала модуля раскрывает отдельную тему (раздел) изучаемого курса. После каждого модуля проводится тестирование. По каждому тесту модулей, а также по итоговому тестированию необходимо набрать более 60% правильных ответов для получения зачета.

Измерительные мероприятия в начале обучения для определения уровня владения обучающимся развиваемыми компетенциями – входное компьютерное тестирование.

Итоговая аттестация проводится в соответствии с Положением по организации итоговой аттестации слушателей по дополнительным профессиональным программам, принятым на заседании методического совета (от 2.09.2020 г.). Формой итоговой аттестации слушателей установлен итоговый зачет в виде компьютерного тестирования. **.**

**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** | Соколов Геннадий Александрович | кандидат технических наук, старший преподаватель учебного центра «Сплайнер»; | <http://splainer.ru/pedagog> |  | согласен |
| **2** | Гайнаншина Альфия Габдинуровна | ассистент учебного центра «Сплайнер». | <http://splainer.ru/pedagog> |  | согласна |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Самостоятельная работа слушателя | Соколов Г.А., Гайнаншина А.Г. Методические указания к самостоятельной работе слушателя, Сплайнер, г. Бирск - 2020 г. |
|  |  |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| https://e.lanbook.com/ | https://zpd-forum.com/ |
| https://znanium.com/ |  |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Видеолекции | Персональный компьютер или ноутбук |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.)

Данная программа не участвовала на конкурсах образовательных программ.

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

2 письма прилагаются

**VI.Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы (в соответствии с приложением)

Развитие компетенций в текущей сфере занятости.

Текущий статус: работающий по найму в организации, на предприятии

Цель: развитие профессиональных качеств

**VII.Дополнительная информация**

Программа предполагает работу с интернет ресурсами.

**VIII.Приложенные Скан-копии**

На платформу загружено:

- скан вариант утвержденного паспорта образовательной программы;

- скан вариант утвержденного паспорта компетенций (ПК-1);

- скан вариант утвержденного паспорта компетенций (ПК-2);

- скан вариант двух писем работодателей.