1. **Паспорт Образовательной программы**

**«Защита персональных данных в организации»**

|  |  |
| --- | --- |
| **Версия программы** | 1 |
| **Дата Версии** | 09.10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | **Финансовый университет при Правительстве Российской Федерации** |
| 1.2 | Логотип образовательной организации | http://www.fa.ru/org/div/cos/skp/Documents/logo_FU_RUS.png |
| 1.3 | Провайдер ИНН | **7714086422** |
| 1.4 | Ответственный за программу ФИО | **Резниченко Сергей Анатольевич** |
| 1.5 | Ответственный должность | **директор** |
| 1.6 | Ответственный Телефон | **8-499-277-28-70** |
| 1.7 | Ответственный Е-mail | **sareznichenko@fa.ru** |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | **Защита персональных данных в организации** |
| 2.2 | Ссылка на страницу программы | **https://dpofa.ru/programs/pk-protection** |
| 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 | Финансовый университет при Правительстве Российской Федерации имеет все необходимые технические, аппаратные и программные средства для возможности реализации программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа.  Имеется действующий учебный портал и электронная информационно-образовательная среда (ЭИОС) с идентификацией пользователей. |
| 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 | 83,7% трудоёмкости учебной деятельности отведено практическим занятиям и выполнению практических заданий в режиме самостоятельной работы: 60 часов из 72.  76% контактной работы с преподавателем отведено практическим занятиям: 38 часов из 50. |
| 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 | **Предлагаемая стоимость обучения: 30 000 руб.**  **Аналогичные программы:**  **1) Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (17 500 руб.)**  **https://www.academyit.ru/courses/%D0%A2%D0%97%D0%9A%D0%98001/**  **2) Защита персональных данных (15 000 руб.)**  **https://infobezopasnost.ru/zashchita-personalnyh-dannyh/**  **3) Обучение комплексной защите персональных данных от учебного центра «Патриот» (20 000 руб.)**  **http://granitsecurity.ru/protection-of-personal-information/** |
| 2.7 | Минимальное количество человек на курсе | **15** |
| 2.8 | Максимальное количество человек на курсе | **1000** |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | нет |
| 2.10 | Формы аттестации | **Промежуточная аттестация:**  **1 модуль – тестирование**  **2 модуль – тестирование**  **3 модуль - тестирование**  **Итоговая аттестация:**  **Зачёт 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**

**Требования к слушателям:**

- допускаются к обучению лица, имеющие среднее профессиональное и (или) высшее образование;

- владение навыками пользования персональным компьютером или мобильным устройством для выхода в сеть Интернет, информационно-коммуникационными технологиями для взаимодействия в Сети, в том числе офисными приложениями Microsoft Office (Word, Excel, Power Point), аналогичными интернет-ресурсами и сервисами для онлайн-работы.

**Адресная направленность программы**.

Программа повышения квалификации ориентирована на руководителей и сотрудников торговых и производственных организаций всех форм собственности, лиц, осуществляющих предпринимательскую деятельность (или планирующих её начать), а также на всех заинтересованных лиц с высшим и (или) средним специальным образованием, желающих получить знания и навыки в области информационной безопасности и обеспечения защищённости персональных данных в условиях современной цифровой экономики и информатизации общества. Освоение программы лицами, имеющими базовое образование в области информационной безопасности и защиты информации позволит расширить свой профессиональный кругозор и получить дополнительные знания и навыки. Освоение программы лицами, не имеющими базового образования в данной области, позволит освоить новую и востребованную профессию, получить новые знания и навыки, которые имеют высокую востребованность в современном обществе.

**Объём программы:** 72 ак. часа.

**Форма обучения:** онлайн, с применением электронного обучения и дистанционных образовательных технологий.

**Режим занятий:** не более 8 акад. часов в день.

**Цель программы:** Совершенствование профессиональных компетенций руководителей и сотрудников коммерческих предприятий всех форм собственности и различных видов деятельности в сфере обеспечения комплексной защиты персональных данных сотрудников и клиентов в условиях интенсивного развития цифровой экономики в соответствии с требованиями законодательства, нормативно-правовыми требованиями, обычаями делового оборота, условиями цифровой среды и информационного общества, сформировавшейся практикой и с учётом зарубежного и российского опыта; формирование теоретических знаний и практических умений воплотить полученные знания в конкретные формы и механизмы в действующем и организующемся бизнесе.

**Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения программы:**

Общепрофессиональная (ОПК-1): способность оценивать факторы, влияющие на безопасность обработки персональных данных в организации, анализировать требования нормативно-правовой базы в разрезе цифровой экономики и информационного общества в условиях постоянно изменяющей внешней среды;

Профессиональная (ПК-1): готовность применять различные методы и технологии защиты персональных данных, осуществлять планирование, организацию и контроль мероприятий по защите персональных данных в условиях развития цифровой экономики;

Профессиональная (ПК-2): способность оценивать риски при эксплуатации информационных систем персональных данных, эффективно организовывать процесс обработки персональных данных, оценивать эффективность защитных мероприятий, разрабатывать предложения по их совершенствованию, осуществлять управление информационной безопасностью организации с применением информационных технологий;

Профессиональная (ПК-3): способность проводить обследование (принимать участие в обследовании) информационных систем персональных данных, определять требования к построению систем защиты персональных данных в цифровой экономике, выявлять угрозы безопасности персональных данных в организации, выявлять и обрабатывать инциденты информационной безопасности персональных данных, определять требуемые уровни защищённости персональных данных, обрабатываемых в информационных системах персональных данных, осуществлять выбор и обосновывать необходимость применения средств защиты персональных данных, разрабатывать организационно-распорядительную документацию, руководить процессами обеспечения защищённости персональных данных на предприятии.

**Описание перечня профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется в процессе обучения**

Программа повышения квалификации основана на требованиях профессионального стандарта 06.033 Профессиональный стандарт "Специалист по защите информации в автоматизированных системах" (Утв. приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 года N 522н) в части обобщенных трудовых и трудовых функций:

- Обслуживание систем защиты информации в автоматизированных системах, код «А», уровень квалификации 5;

- Обеспечение защиты информации в автоматизированных системах, код «В», уровень квалификации 6;

- Внедрение систем защиты информации автоматизированных систем, код «С», уровень квалификации 6.

**Трудовые функции выпускника программы повышения квалификации, согласно профессионального стандарта:**

- А/02.5, Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем;

- А/03.5, Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем;

- В/03.6, Управление защитой информации в автоматизированных системах;

- С/02.6, Разработка организационно-распорядительных документов по защите информации в автоматизированных системах;

- С/04.6, Внедрение организационных мер по защите информации в автоматизированных системах.

Возможные наименования должностей, профессий лиц, окончивших программу повышения квалификации:

* Техник по защите информации I категории;
* Техник по защите информации II категории;
* Техник по защите информации;
* Инженер по защите информации;
* Специалист по защите информации.

**Результатами обучения по программе будут являться сформированные:**

а) знания:

- основных характеристик и тенденций развития современной цифровой экономики, механизмов общественных и корпоративных коммуникаций;

- форм представления, хранения и обработки персональных данных в цифровой среде;

- основных положений нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

- видов угроз безопасности персональных данных в информационных системах персональных данных;

- требований по обеспечению безопасности персональных данных;

- порядка применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

б) умения:

- создавать организационно-распорядительные документы по обеспечению безопасности персональных данных;

- планировать мероприятия по обеспечению безопасности 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.

в) владения:

- навыками анализа деловых процессов в цифровой экономике;

- навыками работы с правовыми базами данных;

- навыками определения уровней защищённости персональных данных;

- навыками выявления угроз безопасности персональных данных в информационных системах персональных данных;

- навыками применения сертифицированных средств защиты информации.

**В результате обучения слушатели смогут:**

- оценивать факторы, влияющие на безопасность обработки персональных данных в организациях;

- анализировать требования нормативно-правовой базы в разрезе цифровой экономики и информационного общества в условиях постоянно изменяющей внешней среды;

- применять различные методы и технологии защиты персональных данных, осуществлять планирование, организацию и контроль мероприятий по защите персональных данных в условиях развития цифровой экономики;

- оценивать риски при эксплуатации информационных систем персональных данных, эффективно организовывать процесс обработки персональных данных, оценивать эффективность защитных мероприятий, разрабатывать предложения по их совершенствованию, осуществлять управление информационной безопасностью организации с применением информационных технологий;

- принимать участие в обследовании информационных систем персональных данных, определять требования к построению систем защиты персональных данных в цифровой экономике;

- выявлять угрозы безопасности персональных данных в организации, выявлять и обрабатывать инциденты информационной безопасности;

- определять требуемые уровни защищённости персональных данных, разрабатывать организационно-распорядительную документацию, руководить процессами обеспечения защищённости персональных данных на предприятии.

Защита персональных данных при их обработке является обязательной в соответствии с требованиями действующего законодательства.

Поэтому являются востребованными специалисты, способные правильно организовать работу с персональными данными клиентов и сотрудников в фирме, организации и на предприятии.

**Выдаваемый документ:** удостоверение о повышении квалификации Финансового университета при Правительстве Российской Федерации.

**Ведущие спикеры программы:**

- Резниченко Сергей Анатольевич, к.т.н., доцент, директор института цифровых компетенций Финансового университета при Правительстве РФ;

- Сиротский Алексей Александрович, к.т.н., доцент, главный специалист института цифровых компетенций Финансового университета при Правительстве РФ

- Ибатулин Михаил Юрьевич, старший преподаватель МГТУ «СТАНКИН»

- Прус Юрий Витальевич, д.ф.-м.н., профессор, профессор Губкинского Университета

- Мельникова Елена Анатольевна, к.ф.-м.н., доцент ФГБОУ ВО РГСУ

1. **Цель программы**

Совершенствование профессиональных компетенций руководителей и сотрудников коммерческих предприятий всех форм собственности и различных видов деятельности в сфере обеспечения комплексной защиты персональных данных сотрудников и клиентов в условиях интенсивного развития цифровой экономики в соответствии с требованиями законодательства, нормативно-правовыми требованиями, обычаями делового оборота, условиями цифровой среды и информационного общества, сформировавшейся практикой и с учётом зарубежного и российского опыта; формирование теоретических знаний и практических умений воплотить полученные знания в конкретные формы и механизмы в действующем и организующемся бизнесе.

1. **Планируемые результаты обучения:**
   1. Знание (осведомленность в областях)
      1. основные характеристики и тенденции развития современной цифровой экономики, информационно-коммуникативные процессы и механизмы общественных и корпоративных коммуникаций;
      2. формы представления, хранения и средства обработки персональных данных в цифровой среде;
      3. основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
      4. основные виды угроз безопасности персональных данных в информационных системах персональных данных;
      5. содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
      6. процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
      7. меры обеспечения безопасности персональных данных;
      8. требования по обеспечению безопасности персональных данных;
      9. порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
   2. Умение (способность к деятельности)
      1. создавать организационно-распорядительные документы в интересах организации по обеспечению безопасности персональных данных;
      2. планировать мероприятия по обеспечению безопасности персональных данных;
      3. обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
      4. проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
      5. 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.
   3. Навык (использование конкретных инструментов)
      1. навыками анализа деловых процессов в цифровой экономике;
      2. навыками работы с правовыми базами данных;
      3. навыками определения уровней защищённости персональных данных;
      4. навыками выявления угроз безопасности персональных данных в информационных системах персональных данных;
      5. навыками разработки необходимых документов в интересах организации по обеспечению безопасности персональных данных;
      6. навыками применения сертифицированных средств защиты информации.
2. **Требования к слушателям** (возможно заполнение не всех полей)
   1. Образование: среднее профессиональное и (или) высшее образование
   2. Квалификация: 5-8 уровни квалификации
   3. Наличию опыта профессиональной деятельности: начальный опыт работы
   4. Предварительное освоение иных дисциплин/курсов /модулей: не требуется
3. **Описание состава / модулей программы**
   1. Модуль 1 «Организационно-правовые основы защиты персональных данных в информационных системах персональных данных»

Тема 1.1. Правовое, нормативное и методическое обеспечение безопасности персональных данных

Эволюция нормативно-правой базы в области информационной безопасности. Основные концепции защиты информации.

Актуальность проблемы обеспечения безопасности персональных данных, обрабатываемых в информационных системах организации. Основные понятия, термины и определения. Правовое, нормативное и методическое регулирование деятельности в области обеспечения безопасности персональных данных. Содержание и основные положения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Специальные нормативные документы по технической защите информации ограниченного доступа и обеспечению безопасности персональных данных. Правовое, нормативное и методическое регулирование использования средств криптографической защиты информации. Ответственность за нарушение требований по обеспечению безопасности персональных данных.

Тема 1.2. Угрозы безопасности персональных данных и уязвимости информационных систем персональных данных

Сущность угроз безопасности и основы подходов к оценке рисков.

Взаимосвязь цифровых технологий, электронной коммерции, электронного бизнеса, интернет-маркетинга, цифрового инструментария, использования информационно-телекоммуникационной сети «Интернет» с задачами обработки персональных данных и обеспечением их защищённости.

Информационные системы обработки персональных данных.

Общие положения и классификация угроз безопасности персональных данных. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации. Угрозы программно-математических воздействий и нетрадиционных информационных каналов.

Тема 1.3. Организация обработки персональных данных

Общий порядок организации обработки персональных данных. Классификация систем обработки персональных данных. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных. Разработка организационно-распорядительных документов, локальных нормативных актов по обработке и защите персональных данных.

Существенные требования нормативно-правовых документов в области защиты персональных данных.

Контрольные и регулирующие органы в области обеспечения информационной безопасности.

Взаимодействие компании с клиентами и сотрудниками.

* 1. Модуль 2 «Управление защитой персональных данных в цифровой экономике»

Тема 2.1. Обеспечение безопасности информационных систем персональных данных в цифровой экономике

Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Разработка Частной модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных организации.

Определение уровня защищённости персональных данных. Состав и содержание мер по обеспечению безопасности персональных данных. Создание системы защиты персональных данных; сертифицированные средства защиты персональных данных в информационных системах защиты персональных данных; аттестация информационных систем персональных данных. Особенности использования средств криптографической защиты информации в рамках построения системы защиты персональных данных в организации.

Особенности обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации. Требования к материальным носителям биометрических персональных данных и технологиям их хранения вне информационных систем персональных данных. Разработка организационно-распорядительной документации, необходимой для организации обработки персональных данных.

Тема 2.2. Компьютерное моделирование угроз и рисков информационной безопасности

Содержание моделей угроз.

Принципы анализа рисков информационной безопасности.

Метрические системы показателей мониторинга безопасности защитных механизмов.

Методы и инструменты анализа и контроля информационных рисков.

Преимущества и недостатки количественной оценки соотношения потерь от угроз безопасности и затрат на создание системы защиты.

Качественные оценки безопасности.

Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей.

Определение уровня рисков путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности на основе нормативно-правовых документов предприятия, касающихся вопросов информационной безопасности; требований действующего российского законодательства, руководящих документов ФСТЭК, требований ФСБ РФ, ГОСТов, рекомендаций международных стандартов.

Рекомендации компаний-производителей программного и аппаратного обеспечения.

Программный инструментарий оценки угроз и рисков безопасности персональных данных.

Оценка рисков информационной безопасности на определении вероятности реализации атак, а также уровней их ущерба.

Тема 2.3. Основы менеджмента информационной безопасности предприятий цифровой экономики

Основные направления управленческой (организационной) работы в сфере информационной безопасности на уровне отдельного предприятия. Общая структура политики информационной безопасности предприятия как основного организующего документа в этой области.

Разработка и анализ политик информационной безопасности.

Система стандартов менеджмента информационной безопасности.

Циклическая модель управления информационной безопасностью.

Организационно-управленческие аспекты внедрения систем менеджмента информационной безопасности на предприятии.

* 1. Модуль 3 «Практическая реализация механизмов защиты персональных данных в организации»

Тема 3.1. Документальное обеспечение защиты персональных данных

Общий порядок организации обеспечения документооборота в службе защиты информации. Разработка регламента и порядка обработки персональных данных. Оформление исходящей документации. Подготовка внешних обращений и заявлений. Работа с должностными лицами.

Тема 3.2. Взаимодействие с государственными, общественными и контрольными органами

Приобретение статуса оператора персональных данных.

Процедуры взаимодействия с внешней средой организации.

Общественный контроль.

Общественная аккредитация.

1. **Учебный план**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Модуль / Тема** | **Вид учебных занятий** | | | **Внеаудиторная работа** | **Формы аттестации, контроля** | **Трудоемкость** |
|  |  | Всего,  час. | Лекции | Практ. занятия | Сам. работа |  |  |
| **1** | **1/1.1** | 8 | 2 | 6 | 4 | тестирование | 12 |
| **2** | **1/1.2** | 8 | 2 | 6 | 4 | учебная дискуссия, опрос | 12 |
| **3** | **1/1.3** | 8 | 2 | 6 | 4 | групповой разбор мини-кейсов, опрос | 12 |
| **5** | **2/2.1** | 6 | 2 | 4 | 2 | тестирование | 8 |
| **6** | **2/2.2** | 6 | 2 | 4 | 2 | групповой разбор мини-кейсов | 8 |
| **7** | **2/2.3** | 6 | 2 | 4 | 2 | учебная дискуссия, опрос | 8 |
| **8** | **3/3.1** | 4 | - | 4 | 2 | опрос | 6 |
| **9** | **3/3.2** | 2 | - | 2 | 2 | опрос | 4 |

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

дата начала обучения – дата завершения обучения: **02-20 ноября 2020 г.**

периодичность набора групп - не менее 1 группы в месяц

1. **Вопросы входного тестирования**
   1. Что относится к персональным данным?

Варианты ответов (выберите один правильный ответ):

а) ФИО, возраст, домашний адрес и номер телефона

б) Группа крови, отпечатки пальцев, медицинские диагнозы

в) Сведения об образовании, фотографии

г) Все вышеперечисленное.

* 1. Имеете ли Вы право обратиться в адрес оператора, осуществляющего обработку Ваших персональных данных, с запросом о предоставлении сведений, касающихся обработки им Ваших персональных данных?

Варианты ответов (выберите один правильный ответ):

а) Да

б) Нет

в) Только если оператором является государственное учреждение

* 1. Куда следует обращаться за защитой персональных данных?

Варианты ответов (выберите один правильный ответ):

а) Роскомнадзор

б) Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

в) Роспотребнадзор

* 1. Имеет ли оператор право продолжить обработку Ваших персональных данных в случае отзыва согласия на обработку персональных данных?

Варианты ответов (выберите один правильный ответ):

а) Имеет

б) Имеет, при наличии оснований, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

в) Не имеет

* 1. Имеет ли право управляющая компания размещать персональные данные должников на сайте?

Варианты ответов (выберите один правильный ответ):

а) Имеет

б) Имеет в случае наличия согласия должника (субъекта персональных данных)

в) Не имеет

* 1. Должен ли интернет-ресурс, на котором Вы оставляете свои персональные данные, содержать документ, определяющий политику оператора в отношении обработки персональных данных?

Варианты ответов (выберите один правильный ответ):

а) Да

б) Нет

* 1. Информация – это

Варианты ответов (выберите один правильный ответ):

а) Любые данные, представленные на материальном носителе;

б) Сведения, принадлежащие кому-либо и защищаемые законом;

в) Сведения (сообщения, данные), независимо от формы их представления.

* 1. Безопасность персональных данных – это

Варианты ответов (выберите один правильный ответ):

а) Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

б) Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность персональных данных;

в) Состояние защищенности персональных данных, характеризуемое способностью технических средств обеспечить конфиденциальность персональных данных.

* 1. Доступ к информации – это

Варианты ответов (выберите один правильный ответ):

а) Возможность получения информации и ее использования;

б) Возможность использования информации;

в) Возможность доступа к информации;

г) Возможность доступа к информации, но не ее использования.

* 1. Целью Федерального закона от 27.07.2006 № 152-ФЗ является:

Варианты ответов (выберите один правильный ответ):

а) Контроль за обработкой персональных данных операторами персональных данных;

б) Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных;

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

* 1. Защищаемая информация – это

Варианты ответов (выберите один правильный ответ):

а) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

б) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации;

в) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов;

г) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации».

* 1. Что понимается под понятием «Конфиденциальность персональных данных»?

Варианты ответов (выберите один правильный ответ):

а) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных;

б) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом;

в) Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных или наличия иного законного основания.

* 1. Общедоступные персональные данные – это

Варианты ответов (выберите один правильный ответ):

а) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных;

б) Персональные данные, доступ неограниченного круга лиц к которым предоставлен в соответствии с федеральными законами;

в) Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

* 1. Специальные категории персональных данных – это

Варианты ответов (выберите один правильный ответ):

а) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни;

в) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни;

г) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости.

* 1. Что будет представлять собой цифровой профиль гражданина?

Варианты ответов (выберите один правильный ответ):

а) портретное изображение человека в электронном виде с фиксацией геометрических параметров тела

б) совокупность цифровых записей о гражданине, содержащихся в информационных системах государственных органов и организаций

в) электронный чип с записями о выданных гражданину документах и предоставленных услугах

1. **Вопросы промежуточного тестирования**
   1. Модуль 1
      1. Вся информация делится на:

* конфиденциальную
* общедоступную
* государственную тайну
* ограниченного доступа
  + 1. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
* уязвимость
* слабое место системы
* угроза
* атака
  + 1. В отношении информации, доступ к которой ограничен федеральными законами, необходимо соблюдать следующее требование:
* обеспечение доступности
* обеспечение неотказуемости
* обеспечение конфиденциальности
* обеспечение целостности
  + 1. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?
* специальные
* биометрические
* общедоступные
* дополнительные
  + 1. Как называется гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных?
* оператор информационной системы
* обладатель информации
* субъект информации
* обладатель информационной системы
  + 1. Информация, к которой нельзя ограничить доступ:
* информация о работе государственных органов
* информация об окружающей среде
* персональные данные субъекта
* информация о здоровье субъекта
  + 1. Как называется попытка реализации угрозы?
* нападение
* уязвимость
* атака
* слабое место системы
  + 1. Какой Федеральный закон устанавливает эквивалентность документа, подписанного собственноручно, и электронного сообщения с ЭЦП?
* о персональных данных
* о лицензировании отдельных видов деятельности
* об информации, информационных технологиях и о защите информации
* о безопасности
  + 1. На сколько групп подразделяются классы защищенности автоматизированной системы обработки информации?
* 10
* 9
* 3
* 5
  + 1. Каждый пользователь ЛВС должен иметь:
* уникальный идентификатор и пароль
* права доступа, позволяющие настраивать свое рабочее место
* свой съемный накопитель информации
* права доступа, позволяющие настраивать антивирусную защиту
  + 1. Персональные данные, над которыми были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПД, называются:
* общедоступными
* общеизвестными
* обезличенными
* специальными
  + 1. Кто должен своевременно обнаруживать факты несанкционироанного доступа к персональным данным?
* субъект персональных данных
* оператор персональных данных
* регулятор
* контролер
  + 1. Выдача одноразового бумажного пропуска на территорию оператора считается:
* неавтоматизированной обработкой персональных данных
* запрещенной обработкой персональных данных в соответствии с ФЗ “О персональных данных”
* автоматизированной обработкой персональных данных
* это неавтоматизированная обработка, если количество сотрудников оператора меньше 100 человек
  + 1. Слабое место в системном обеспечении ИСПД, которое может быть использовано для реализации угрозы безопасности персональных данных, называется:
* уязвимостью
* угрозой
* недостатком
* брешью
  + 1. Выдача бумажного талончика к врачу считается:
* запрещенной обработкой персональных данных в соответствии с ФЗ “О персональных данных”
* неавтоматизированной обработкой персональных данных
* автоматизированной обработкой персональных данных
* это неавтоматизированная обработка, если количество сотрудников больницы меньше 100 человек
  1. Модуль 2.
     1. Какой документ отражает полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПД – чтение, запись, корректировка, удаление?
* список лиц, допущенных к обработке ПД
* матрица доступа
* частная модель угроз
* положение по обеспечению безопасности персональных данных
  + 1. При построении сети и конфигурировании коммуникационного оборудования рекомендуется учитывать:
* количество пользователей сети
* разделение трафика по видам деятельности предприятия
* разделение трафика по производственной основе
* расположение межсетевых экранов
  + 1. К какому типу относится ИСПД, если в ней необходимо обеспечить целостность информации?
* специальная
* биометрическая
* типовая
* государственная
  + 1. К какому классу относится ИСПД, если в ней обрабатываются данные 1500 субъектов о состоянии их здоровья?
* 3 класс
* 2 класс
* 4 класс
* 1 класс
  + 1. Требования к средствам защиты и их выбор в каждом конкретном случае зависит от:
* категории персональных данных, обрабатываемых в ИСПД
* решения руководителя
* класса ИСПД
* ущерба, который может быть нанесен в результате атаки
  + 1. Ущерб, связанный с причинением физического, морального, финансового или материального вреда непосредственно субъекту ПД, называется:
* непосредственный ущерб
* косвенный ущерб
* явный ущерб
* опосредованный ущерб
  + 1. К какой категории относятся персональные данные, позволяющие идентифицировать субъекта?
* 2 категория
* 4 категория
* 3 категория
* 1 категория
  + 1. В ходе какого этапа построения системы защиты персональных данных определяются основные направления защиты персональных данных, и производится выбор способов защиты?
* формирование замысла защиты
* построение частной модели угроз
* оценка обстановки
* решение вопросов управления защитой
  + 1. К какому типу относится ИСПД, если в ней необходимо обеспечить доступность информации?
* биометрическая
* государственная
* специальная
* типовая
  + 1. Какое свойство информации требуется обеспечить в типовых информационных системах обработки персональных данных?
* целостность
* аутентичность
* конфиденциальность
* доступность
  + 1. Если злоумышленник получил доступ к почтовому ящику человека и рассылает письма от его имени, о каком виде ущерба идет речь?
* опосредованный ущерб
* непосредственный ущерб
* нематериальный ущерб
* неявный ущерб
  + 1. На каком этапе построения системы защиты происходит оценка возможного физического доступа к ПД?
* разработка замысла защиты
* реализация замысла защиты
* оценка обстановки
* решение вопросов управления защитой
  + 1. Требования по защите от НСД каких классов ИСПД в многопользовательском режиме при разных правах доступа совпадают?
* 1 и 2 классов
* 2 и 3 классов
* 1 и 3 классов
* 3 и 4 классов
  + 1. В каком законодательном документе определено понятие профиля защиты?
* ФЗ “О персональных данных”
* ГОСТ “Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий”
* ФЗ “Об информации, информационных технологиях и о защите информации”
* ФЗ “О безопасности”
  + 1. Наличие межсетевого экрана необходимо при:
* использовании изолированной локальной сети
* использовании сетей общего пользования
* использовании почтового ящика в сети Интернет
* использовании автономного автоматизированного рабочего места
  1. Модуль 3.
     1. Какой участник процесса сертификации оформляет экспертное заключение по сертификации средств защиты информации?
* органы по сертификации средств защиты информации
* заявитель
* федеральный орган по сертификации
* испытательные лаборатории
  + 1. На каком этапе создания системы защиты персональных данных разрабатывается частная модель угроз?
* ввод в действие
* эксплуатация
* стадия проектирования
* предпроектная стадия
  + 1. Сколько органов по сертификации действует в России?
* 3
* 4
* 5
* 2
  + 1. На каком этапе создания СЗПД производится закупка технических средств защиты?
* эксплуатация
* ввод в действие
* стадия проектирования
* предпроектная стадия
  + 1. Какой срок действия у сертификата средства защиты информации?
* 10 лет
* 3 года
* 5 лет
* 2 года
  + 1. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?
* создание СЗПД
* административное мероприятие
* организационное мероприятие
* техническое мероприятие
  + 1. На каком этапе создания СЗПД производится опытная эксплуатация средств защиты?
* эксплуатация
* предпроектная стадия
* стадия проектирования
* ввод в действие
  + 1. На каком этапе создания системы защиты персональных данных определяется состав персональных данных и необходимость их обработки?
* эксплуатация
* предпроектная стадия
* ввод в действие
* стадия проектирования
  + 1. Какие подсистемы в рамках СЗПД можно не использовать, если ИСПД является изолированной (локальной)?
* подсистема безопасности межсетевого взаимодействия
* подсистема криптографической защиты информации
* подсистема обнаружения вторжений
* подсистема обеспечения целостности
* подсистема анализа защищенности
* подсистема управления доступом, регистрации и учета
* подсистема антивирусной защиты
  + 1. Как называются меры защиты, которые создают маскирующие акустические и вибрационные помехи?
* криптографические меры защиты
* активные меры защиты от утечки по техническим каналам
* пассивные меры защиты от утечки по техническим каналам
* активные меры защиты от несанкционированного доступа
  + 1. Какая подсистема в рамках СЗПД предназначена для защиты информационной системы от вредоносных программ?
* подсистема обнаружения вторжений
* подсистема антивирусной защиты
* подсистема безопасности межсетевого взаимодействия
* подсистема анализа защищенности
  + 1. Что является основанием для включения оператора в ежегодный план проверок ФСТЭК?
* предписание Роскомнадзора
* заявления и обращения граждан
* истечение 3 лет со дня последней плановой проверки
* истечение 3 лет со дня государственной регистрации
  + 1. Выберите утверждения, характеризующие антивирусы с эвристическим методом обнаружения вирусов:
* не способны находить неизвестные вирусы
* способны находить неизвестные вирусы
* гарантированно находят известные вирусы
* имеют большое количество ложных срабатываний
  + 1. Процедура фильтрации в межсетевом экране представляет собой:
* анализ доменного имени источника сообщения на предмет совпадения определенным условиям
* помещение всех пакетов в буфер и ожидание решения администратора о легитимности трафика
* анализ заголовка пакета на предмет совпадения определенным условиям
  + 1. Какой орган является регулятором в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД?
* ФСТЭК
* Роспотребнадзор
* ФСБ
* Роскомнадзор

1. **Вопросы итогового тестирования**
   1. Трансграничная передача персональных данных – это:

Варианты ответов (выберите один правильный ответ):

а) Передача персональных данных на территорию иностранного государства;

б) Передача персональных данных на территорию другого субъекта РФ органу власти данного субъекта, физическому лицу или юридическому лицу данного субъекта РФ;

в) Передача персональных данных на территорию иностранного государства или органу власти иностранного государства;

г) Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

* 1. Оператор персональных данных - это:

Варианты ответов (выберите один правильный ответ):

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

б) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

в) Юридическое лицо, осуществляющее автоматизированную обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке;

г) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, но не определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

* 1. Обработка персональных данных – это:

Варианты ответов (выберите один правильный ответ):

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

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

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

* 1. Биометрические персональные данные – это:

Варианты ответов (выберите один правильный ответ):

а) Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных;

б) Сведения, которые характеризуют физиологические особенности человека, на основании которых можно установить его личность;

в) Сведения, которые характеризуют биологические особенности человека, на основании которых можно установить его личность.

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

Варианты ответов (выберите один правильный ответ):

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

б) На отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

в) На организацию хранения, комплектования, учета и использования архивных документов в соответствии с законодательством об архивном деле в РФ

г) Не распространяется на все перечисленных варианта.

* 1. Оператором персональных данных может являться:

Варианты ответов (отметьте все верные варианты):

а) Физическое лицо;

б) Юридическое лицо;

в) Муниципальный орган;

г) Государственный орган;

д) Гражданин;

е) Государственный служащий.

* 1. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий:

Варианты ответов (выберите один правильный ответ):

а) 10 дней;

б) 30 дней рабочих;

в) 30 дней;

г) 7 рабочих дней.

* 1. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные - это:

Варианты ответов (выберите один правильный ответ):

а) информационная система персональных данных;

б) база данных;

в) централизованное хранилище данных

* 1. Обеспечение безопасности персональных данных достигается:

Варианты ответов (выберите один правильный ответ):

а) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

б) обнаружением фактов доступа к персональным данным и принятием ответных мер;

в) реагированием на внешние угрозы персональным данным;

г) страхованием персональных данных

* 1. Идентификация – это:

Варианты ответов (выберите один правильный ответ):

а) Присвоение субъектам и объектам доступа идентификатора и сравнение предъявляемого идентификатора с вводимым идентификатором;

б) Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

в) Присвоение субъектам и объектам доступа идентификатора;

г) Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с вводимым идентификатором.

* 1. Нарушитель безопасности персональных данных – это:

Варианты ответов (выберите один правильный ответ):

а) Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;

б) Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;

в) Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

* 1. Недекларированные возможности технических и программных средств – это:

Варианты ответов (выберите один правильный ответ):

а) Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

б) Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых появляются новые возможности для работы;

в) Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

* 1. Что понимается под понятием «Контролируемая зона»?

Варианты ответов (выберите один правильный ответ):

а) Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств;

б) Пространство, в котором не исключается неконтролируемое пребывание сотрудников и посетителей оператора, но исключается неконтролируемое пребывание посторонних транспортных, технических и иных материальных средств;

в) Пространство, в котором не исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

* 1. Управление Роскомнадзора уведомляет оператора персональных данных о проведении плановой проверки:

Варианты ответов (выберите один правильный ответ):

а) не позднее, чем в течение 3-х рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом;

б) не позднее, чем в течение 7-ми рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Управления Роскомнадзора с уведомлением о вручении или иным доступным способом;

в) не менее чем за 24 часа до начала ее проведения любым доступным способом;

г) предварительное уведомление Оператора о начале проведения плановой проверки не требуется.

* 1. Кто должен осуществлять внутренний контроль за соблюдением оператором законодательства Российской Федерации о персональных данных?

Варианты ответов (выберите один правильный ответ):

а) Администратор безопасности;

б) Ответственный за организацию обработки персональных данных;

в) Ответственный за обеспечение безопасности персональных данных;

г) Руководитель организации

* 1. Требования по защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах устанавливает:

Варианты ответов (выберите один правильный ответ):

а) Приказ ФСТЭК №21;

б) Приказ ФСТЭК №17;

в) Приказ ФСТЭК №58;

* 1. От чего зависит базовый набор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, согласно приказу ФСТЭК №21:

Варианты ответов (выберите один правильный ответ):

а) уровня защищенности информационной системы персональных данных;

б) класса информационной системы персональных данных;

в) класса защищенности информационной системы персональных данных.

* 1. От чего зависит класс защищенности информационной системы персональных данных, согласно приказу ФСТЭК №17?

Варианты ответов (выберите один правильный ответ):

а) объем персональных данных, категория персональных данных;

б) уровень защищенности информации, масштаб системы;

в) уровень значимости информации, масштаб системы.

* 1. Для обеспечения какого уровня защищенности к оператору предъявляется наибольшее количество требований?

Варианты ответов (выберите один правильный ответ):

а) УЗ 1;

б) УЗ 2;

в) УЗ 3.

* 1. Какие средства защиты информации защищают информацию на компьютерах информационной системы персональных данных от сетевых угроз?

Варианты ответов (выберите один правильный ответ):

а) межсетевые экраны;

б) антивирусные средства;

в) средства анализа защищенности.

* 1. В каком нормативном правовом акте закреплены все виды конфиденциальной информации??

Варианты ответов (выберите один правильный ответ):

а) в ФЗ-152 «О персональных данных»;

б) в Указе Президента №188;

в) в Трудовом кодексе РФ.

* 1. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ??

Варианты ответов (выберите один правильный ответ):

а) Паспортные данные гражданина;

б) Информация, накапливаемая в открытых фондах библиотек, музеев, архивов;

в) Себестоимость продукта и объем сбыта;

г) Контактные данные клиентов.

* 1. Раскройте понятие "конфиденциальный документ":

Варианты ответов (выберите один правильный ответ):

а) это зафиксированная на материальном носителе конфиденциальная информация с реквизитами, позволяющими ее идентифицировать;

б) это зафиксированная на материальном носителе конфиденциальная информация с обязательным проставлением грифа конфиденциальности;

в) это любая информация имеющая конфиденциальный характер даже если она предоставлена в устном виде;

г) все ответы правильные.

* 1. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, называется:

Варианты ответов (выберите один правильный ответ):

а) источник информации;

б) носитель информации;

в) обладатель информации;

г) хранитель информации.

* 1. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:

Варианты ответов (выберите один правильный ответ):

а) база данных;

б) информационная система;

в) информационно-телекоммуникационная сеть;

г) информационная технология.

* 1. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

Варианты ответов (выберите один правильный ответ):

а) информационная система персональных данных;

б) база данных;

в) сервер;

г) централизованное хранилище данных.

* 1. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом, называется:

Варианты ответов (выберите один правильный ответ):

а) авторизация;

б) аутентификация;

в) идентификация;

г) самоидентичность.

* 1. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

Варианты ответов (выберите один правильный ответ):

а) идентификация;

б) авторизация;

в) шифрование;

г) обезличивание.

* 1. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа, называется:

Варианты ответов (выберите один правильный ответ):

а) антивирус;

б) криптография;

в) брандмауэр;

г) анализатор защищенности.

* 1. Карта, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации, называется:

Варианты ответов (выберите один правильный ответ):

а) межсетевой экран;

б) чип;

в) токен;

г) логин;

д) смарт-карта.

1. **Описание практико-ориентированных заданий и кейсов по модулям**
   1. Кейс №1

Недавно на форумах в сети «Интернет» обнаружили базы данных 600 тысяч клиентов сервисов «Avito» и «Юла», среди которых фигурируют реальные имена, адреса и номера телефонов пользователей. Множество недобросовестных предпринимателей и теневых элементов уже скачали эти базы с умыслом рассылать спам, назойливую рекламу, сомнительные предложения, или, что еще хуже, в целях выманивания данных платежных карт пользователей. Администрация форумов не удаляет базы, так как не видят в этой ситуации никакой проблемы, а тем более нарушения, и утверждает, что это не воровство персональных данных, а сбор открытых данных.

Следует проанализировать:

1. Кого и в какой степени могут винить пользователи сервисов «Авито» и «Юла»?

2. Дайте правовой анализ сбора персональных данных пользователей с сервисов «Авито» и «Юла» и размещение их в открытом доступе.

3. Имеются ли нарушения законодательства о персональных данных со стороны сервисов «Авито» и «Юла», и если да, то в чём они заключаются?

4. Является ли сайт оператором персональных данных?

5. Нужно ли сервисам типа «Авито» и «Юла» в обязательном порядке брать согласие на обработку данных и вступать в реестр операторов персональных данных?

6. Дайте рекомендации пользователям, не желающим получать нежелательные звонки и сомнительные предложения.

* 1. Практико-ориентированное задание №1

На основе исходных данных, предоставленных преподавателем, провести анализ информационной системы персональных данных и составить отчет, содержащий:

1. Основные характеристики информационной системы персональных данных.

2. Перечень обрабатываемых и подлежащих защите персональных данных.

3. Перечень должностей сотрудников, участвующих в обработке персональных данных.

4. Схему расположения информационной системы персональных данных относительно границ контролируемой зоны.

5. Схему локальной вычислительной сети (при её наличии), иллюстрирующей связи между конечными сетевыми устройствами, коммутаторами (концентраторами), маршрутизаторами, межсетевыми экранами и т.п.

6. Схему информационных потоков в информационной системе персональных данных.

7. Перечень программных средств, используемых в процессе обработки персональных данных.

8. Информацию о местах хранения носителей персональных данных, обрабатываемых без использования средств автоматизации.

9. Результат определения уровня защищенности информационной системы персональных данных.

* 1. Практико-ориентированное задание №2

На основе исходных данных, предоставленных преподавателем, методики определения актуальных угроз безопасности персональным данным и методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», провести анализ и построить модель угроз безопасности персональным данным. Составить отчёт, содержащий:

1. Описание процесса построения модели угроз безопасности персональным данным.

2. Перечень актуальных угроз безопасности персональным данным.

3. Описание последствий реализации актуальных угроз безопасности персональным данным.

* 1. Практико-ориентированное задание №3

На основе исходных данных, предоставленных преподавателем, составить «Политику безопасности организации при обработке персональных данных».

В Политике указать:

1. Порядок и процедуру обработки персональных данных.

2. Дать ключевые определения.

3. Сформулировать и указать цели обработки персональных данных.

4. Сформировать и указать принципы обработки персональных данных.

5. Указать права владельцев персональных данных и механизмы их соблюдения.

6. Перечислить реализуемые требования по защите персональных данных.

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

Задание 1. На основе исходных данных, предоставленных преподавателем, методики определения актуальных угроз безопасности персональным данным и методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», провести анализ и построить модель угроз безопасности персональным данным.

Задание 2. На основе исходных данных, предоставленных преподавателем, составить «Политику безопасности организации при обработке персональных данных».

1. **Оценочные материалы по образовательной программе:**

15.1 описание показателей и критериев оценивания, шкалы оценивания;

Для успешного прохождения промежуточного тестирования необходимо набрать не менее 65% от максимального количества баллов в любой попытке. Оценивание производится в форме промежуточного зачёта по модулю.

Для успешного прохождения итогового тестирования необходимо набрать не менее 65% от максимального количества баллов в любой попытке. Оценивание производится в форме зачёта с оценкой «зачтено» или «незачтено».

15.2 описание процедуры оценивания результатов обучения

Итоговая аттестация имеет целью определить сформированность спланированных к освоению профессиональных компетенций.

Итоговая аттестация представляет собой итоговое комплексное тестирование по всем разделам учебной программы.

Порядок проведения: тестирование проводится с личного компьютера, 20 -30 тестовых вопросов, количество попыток – 3.

1. **Паспорт компетенций**

Паспорт компетенций по форме – в виде отдельного файла.

1. **Организационно-педагогические условия (применяемые при реализации программы)**
   1. *Кадровое обеспечение (данные о преподавателях)*
      1. *Резниченко Сергей Анатольевич, директор института цифровых компетенций образовательного центра «Высшая школа финансовых технологий» Финансового Университета при Правительстве Российской Федерации, кандидат технических наук, доцент;*
      2. *Сиротский Алексей Александрович, главный специалист института цифровых компетенций образовательного центра «Высшая школа финансовых технологий» Финансового Университета при Правительстве Российской Федерации, кандидат технических наук, доцент*
      3. *Ибатулин Михаил Юрьевич, старший преподаватель МГТУ «СТАНКИН»*
      4. *Прус Юрий Витальевич, д.ф.-м.н., профессор, профессор Губкинского Университета*
      5. *Мельникова Елена Анатольевна, к.ф.-м.н., доцент ФГБОУ ВО РГСУ*
   2. *Методическое обеспечение*
      1. *В образовательном процессе используются разнообразные формы работы со слушателями. Лекции с мультимедийным сопровождением по наиболее сложным вопросам программы. Практикум – это вид практических занятий тренировочного характера, на котором осуществляется связь изучаемой теории и практики, а материал его часто служит иллюстрацией к лекции. Разработка презентации – самостоятельная работа с использованием информационных технологий и знаний, полученных на занятиях. Ттестирование – это стандартизированный метод оценки знаний, умений, навыков обучающихся.*
      2. *Программа осваивается с применением электронной информационно-образовательной среды (ЭИОС). Программа состоит из 3 модулей. В начале каждого модуля обучающиеся самостоятельно прослушивают установочную видеолекцию. После этого проводятся видеолекции или вебинары с применением вебинарной платформы. Затем слушатели выполняют практические задания. Промежуточная аттестация по модулю проводится в виде компьютерного тестирования.*
      3. *Образовательная программа рассчитана на 72 академических часа обучения и включает перечень модулей, темы, виды занятий, предназначенные для приобретения слушателями знаний, умений и навыков, необходимых для решения поставленных целей.*
      4. *В процессе преподавания программы повышения квалификации используются лекционные и практические занятия в дистанционном онлайн-формате, в виде вебинаров, видеолекций. Онлайн-лекции проводятся по сложным теоретическим вопросам курса. При проведении онлайн-лекционных занятий используются компьютерные и мультимедийные средства обучения.*
      5. *Практические занятия проводятся в интерактивной форме. На практических занятиях организуются индивидуальная, парная и групповая работа в онлайн-формате, осуществляется работа с различными источниками информации. На круглом столе в формате вебинаров организуется обсуждение актуальных проблем в предметной области.*
      6. *Продолжительность учебного дня – не более 8 академических часов.*
      7. *В процессе обучения слушатели получают доступ к электронной информационно-образовательной среде (ЭИОС) Финансового университета, через которую обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса, которые объединены в учебно-методический комплекс. Материалы учебно-методического комплекса доводятся до всех слушателей курса.*
   3. *Материально-техническое обеспечение*
      1. Для реализации образовательного процесса необходимы технические средства обучения: персональный компьютер (с выходом в интернет), с офисными приложениями Microsoft Office (Word, Excel, Power Point), Adobe Flash Player; Adobe Reader.
      2. Наименование специализированных учебных помещений: Учебный интерактивный тренажерный класс
      3. Наименование оборудования, программного обеспечения: Мультимедийное оборудование, компьютеры. Компьютер, подключенный к сети Интернет, интернет-браузер. Adobe Flash Player; Adobe Reader, и т.д.
   4. *Методы, формы и технологии*
      1. *Лекции*
      2. *Семинары*
      3. *Вебинары*
      4. *Практические занятия*
      5. *Кейсы*
      6. *Деловые игры*
      7. *Тестирование*
      8. *Опросы*
      9. *Дискуссии*
      10. *Групповые дискуссии*
      11. *Групповой разбор ситуаций*
      12. *Обучение на примерах*
      13. *Разбор примеров*
      14. *Изучение литературы*
      15. *Просмотр видеоматериалов*
      16. *Работа на учебном портале*
      17. *Консультации*
   5. *Перечень источников информационного сопровождения (учебная литература)*
      1. *Агапов А. Б. Основы государственного управления в сфере информатизации в Российской Федерации.- М.: Юристъ, 2012.-221с.*
      2. *Аудит информационной безопасности. Под ред. А.П.Курило. – М: БДЦ-Пресс, 2006 г – 304 с.*
      3. *Бабаш, А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. – 2-e изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 216 с. – Режим доступа: http://znanium.com/bookread.php?book=432654 (дата обращения 01.09.2020);*
      4. *Бачило И.Л. Информационное право. Роль и место в системе права Российской Федерации / И.Л. Бачило // Государство и право.- 2009. - № 2. - С. 14.*
      5. *Борисов М., Особенности защиты персональных данных в трудовых отношениях, Издательство Ленанд, 2017. – 224 стр.*
      6. *Бычков, А.И. Проблемы защиты персональных данных / Издательство «Инфотропик», 2020. – 116 с.*
      7. *Внуков А.А. Защита информации. 2-е изд. Учебное пособие для бакалавриата и магистратуры. Академический курс. М: Издательство Юрайт, 2019 г. – 240 с.*
      8. *Галатенко В.А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006 г. – 264 с.*
      9. *Декларация о правах и свободах человека и гражданина Российской Федерации от 22.11.91.*
      10. *Дубинин, Е.А. Оценка относительного ущерба безопасности информационной системы: Монография [электронный ресурс] / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 192 с. – Режим доступа: http://znanium.com/bookread.php?book=471787 (дата обращения 01.09.2020).*
      11. *Дупан (Гутникова), А.С., Жулин, А.Б., Жарова А.К. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет. М.: Издательский дом ВШЭ, 2016. – 344 с.*
      12. *Закон РФ “О средствах массовой информации” от 27.12.91 № 2124-1 (с изменениями и дополнениями, внесенными федеральными законами от 13.01.95 № 6-ФЗ; от 06.06.95 № 87-ФЗ; от 19.07.95 № 114-ФЗ; от 27.12.95 № 211-ФЗ).*
      13. *Конвенция Совета Европы “О защите личности в связи с автоматизированной обработкой персональных данных” от 28.01.81.*
      14. *Копылов В.А. О структуре и составе информационного законодательства // Государство и право. 2010. № 6. -С. 23-25.*
      15. *Минаев В.А., Фисун А.П. Правовое обеспечение информационной безопасности, Москва, 2008 г. – 368 с.*
      16. *Модельный закон МПА СНГ “О защите персональных данных” от 16.10.99. 23.09.92 № 3526-1.*
      17. *Окинавская Хартия глобального информационного общества от 22.07.00.*
      18. *Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2004. — 392 с.*
      19. *Петренко, В.И., Мандрица, И.В. Защита персональных данных в информационных системах. Практикум. Учебное пособие / СПб.: Издательство «Лань», 2019. – 108 с.*
      20. *Рассолов М.М. Информационное право. / М.М. Рассолов М.: Юрист, 2009. -198 с.*
      21. *Рекомендательный законодательный Акт “О принципах регулирования информационных отношений в государствах МПА СНГ” от 23.05.93.*
      22. *Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 с.*
      23. *Тихонов В., Райх В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. – М.: Гелиос АРВ, 2006 г. – 528 с.*
      24. *Указ Президента РФ “О дополнительных гарантиях прав граждан на информацию” от 31.12.93 № 2334.*
      25. *Указ Президента РФ “О перечне сведений конфиденциального характера” от 06.03.97 № 188.*
      26. *Федеральный закон РФ “О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания” от 14.06.94 № 5-ФЗ.*
      27. *Федеральный закон РФ “О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации” от 13.01.95 № 7-ФЗ.*
      28. *Федеральный закон РФ “О рекламе” от 18.07.95 № 108-ФЗ.Прикладная информатика (по отраслям)*
      29. *Федеральный закон РФ «О персональных данных», № 152, от 14 июля 2006 года.*
      30. *Федеральный закон РФ «Об информации, информационных технологиях и о защите информации», № 149, 27 июля 2006 года.*
   6. *Учебно-методические материалы*
      1. Публичные учебные материалы ВГУЭС http://abc.vvsu.ru/Books/dokumentoved\_hrestomat\_ch2/page0018.asp
      2. Всероссийский научно-исследовательский институт документоведения и архивного дела http://www.vniidad.ru
      3. Гильдия управляющих документацией http://www.gdm.ru
      4. Система управления персоналом организации http://www.top-personal.ru/page.html60
      5. Юридический навигатор http://www.delo-press.ru/documents-it/index.html
      6. Томский политехнический университет http://portal.tpu.ru
      7. Электронная библиотечная система «КнигаФонд»: http://www.knigafund.ru/
      8. Электронная библиотечная система издательства «Лань»: http://e.lanbook.com/
      9. Антивирусная защита компьютерных систем. Лаборатория Касперского. ИНТУИТ, 2008 // http://www.intuit.ru/department/security/antiviruskasp/.
      10. Базовый стандарт организации беспроводных локальных сетей IEEE 802.11 // http://standarts.ieee.org/reading/ieee/std/lanman/802.11-1999.pdf.
      11. Совет Безопасности Российской Федерации http://www.scrf.gov.ru/.
2. **Иная информация о качестве и востребованности образовательной программы**
3. **Рекомендаций к программе от работодателей**: рекомендательные письма прилагаются.
4. **Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы

|  |  |
| --- | --- |
| **Цели получения ПЦС** | |
| **текущий статус** | **цель** |
| **Развитие компетенций в текущей сфере занятости** | |
| работающий по найму в организации, на предприятии | развитие профессиональных качеств |

1. **Дополнительная информация**
2. **Приложение: утвержденная программа прилагается**