

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮ |
|  |  | Проректор по общим вопросам ДГТУ |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Мозговой А.В. / |
|  |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г. |

**Паспорт Образовательной программы**

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

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 11.10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет» (ДГТУ) |
| 1.2 | Логотип образовательной организации | лого ДГТУ вектор_варианты-07 |
| 1.3 | Провайдер ИНН | 6165033136 |
| 1.4 | Ответственный за программу ФИО | Газизов Андрей Равильевич |
| 1.5 | Ответственный должность | Доцент кафедры "Вычислительные системы и информационная безопасность" |
| 1.6 | Ответственный Телефон | **+79885888010** |
| 1.7 | Ответственный Е-mail | ds@donstu.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://fpk.skif.donstu.ru/enrol/index.php?id=31**2** |
| 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 | У ОО имеется собственная электронная платформа для реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа http://fpk.skif.donstu.ru |
| 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) | 45 |
| 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 | 20000 <https://edu.softline.com/vendors/softline/obespechenie-bezopasnosti-personalnyh-dannyh-pri-ih-obrabotke-v-informacionnyh-sistemah-personalnyh-dannyh/>, <https://fsb-fstec.ru/?yclid=6012094079785269732>, <https://fsb-fstec.ru/?yclid=6012094079785269732> |
| 2.9 | Минимальное количество человек на курсе | **5** |
| 2.10 | Максимальное количество человек на курсе | 15 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | Нет |
| 2.12 | Формы аттестации | Выполнение контрольного задания |
| 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**

Цель программы повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»:

совершенствование и (или) получение новых профессиональных компетенций, необходимых для осуществления профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации руководителей и специалистов (обучающихся), обеспечивающих безопасность персональных данных при их обработке в информационных системах персональных данных;

развитие у обучающихся личностных качеств, позволяющих реализовать сформированные компетенции в профессиональной деятельности;

формирование способности приобретать новые знания, психологической готовности к изменению вида и характера своей профессиональной деятельности;

обеспечение многообразия образовательных возможностей обучающихся.

Профессиональные компетенции (ПК) включают:

способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-l);

способность использовать нормативные право вые документы в своей профессиональной деятельности (ПК-3);

способность формировать комплекс мер по информационной безопасности с учетом его пра­вовой обоснованности, административно-управленческой и технической реализуемости и эконо­мической целесообразности (ПК-4);

способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организацион­ной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития техно­логий защиты информации (ПК-5);

способность организовать про ведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);

способность определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информаци­онных процессов предприятия, целей и задач деятельности предприятия (ПК-8);

способность выполнять работы по установке, настройке и обслуживанию технических и про­граммно-аппаратных средств защиты информации (ПК -11);

способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);

способность применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);

способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);

способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-23).

1.2 Планируемые результаты обучения.

Слушатели, прошедшие обучение, должны:

а) знать:

основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

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

содержание и порядок организации работ по выявлению угроз безопасности персональных данных;

процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

меры обеспечения безопасности персональных данных;

требования по обеспечению безопасности персональных данных;

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

б) уметь:

создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;

планировать мероприятия по обеспечению безопасности персональных данных;

обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

в) владеть:

навыками работы с правовыми базами данных;

навыками определения уровней защищённости персональных данных;

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

навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;

навыками применения сертифицированных средств защиты информации.

Перечень профессиональных стандартов, соответствующих профессиональной деятельности выпускников, осваивающих образовательную программу:

Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден Приказом Министерства труда и социальной защиты Российской Федерации № 522н от 15.09. 2016 г.

Партнеры образовательной программы:

«НПО Горизонт», ГУ МЧС России по Ростовской области, ГУФСИН России по Ростовской области, КБ «Центр-Инвест», ОАО «КБ «Связь»», ОАО «Комбайновый завод «Ростсельмаш», ОАО «Роствертол», ОАО «Энергосбыт Ростовэнерго», Управление ФСТЭК России по Южному и Северо-Кавказскому федеральным округам, ФГНУ «НИИ Спецвузавтоматика», ФГУП «РНИИРС», Штаб Южного военного округа.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | УТВЕРЖДАЮ |  |
|  |  | Проректор по общим вопросам ДГТУ |  |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Мозговой А.В. / |  |
|  |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г. |  |

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

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

72 часа

г. Ростов-на-Дону

2020 г.

**1. Цели дополнительной программы: совершенствование** и (или) получение новых профессиональных компетенций, необходимых для осуществления профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации руководителей и специалистов (обучающихся), обеспечивающих безопасность персональных данных при их обработке в информационных системах персональных данных;

развитие у обучающихся личностных качеств, позволяющих реализовать сформированные компетенции в профессиональной деятельности;

формирование способности приобретать новые знания, психологической готовности к изменению вида и характера своей профессиональной деятельности;

обеспечение многообразия образовательных возможностей обучающихся.

**2.Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях)

2.1.1. основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

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

2.1.3 содержание и порядок организации работ по выявлению угроз безопасности персональных данных;

2.1.4 процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

2.1.5 меры обеспечения безопасности персональных данных;

2.1.6 требования по обеспечению безопасности персональных данных;

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

2.2. Умение (способность к деятельности)

2.2.1. создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;

2.2.2 планировать мероприятия по обеспечению безопасности персональных данных;

2.2.3 обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

2.2.4 проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2.2.5 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

2.3. Навыки (использование конкретных инструментов)

2.3.1 работы с правовыми базами данных;

2.3.2 определения уровней защищённости персональных данных;

2.3.3 выявления угроз безопасности персональных данных в информационных системах персональных данных;

2.3.4 разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;

2.3.5 применения сертифицированных средств защиты информации.

**3.Категория слушателей**

1. Образование- высшее или среднее профессиональное образование;
2. Квалификация-необязательно;
3. Наличие опыта профессиональной деятельности- приветствуется, но необязательно;
4. Предварительное освоение иных дисциплин/курсов /модулей - не требуется.

**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 | Технические каналы утечки персональных данных | 12 | 3 | 6 | 3 |
| 2 | Способы и средства защиты персональных данных от утечки по техническим каналам | 8 | 2 | 4 | 2 |
| 3 | Методы и средства контроля эффективности технической защиты персональных данных | 12 | 3 | 6 | 3 |
| 4 | Организация технической защиты персональных данных | 12 | 3 | 6 | 3 |
| 5 | Организационное обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 2 | 4 | 2 |
| 6 | Правовое обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 2 | 4 | 2 |
| Итоговая аттестация | |  | Указывается вид (экзамен, зачёт, реферат и т.д.) | | |
| Зачет | | 72 | Контрольная работа | | |

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

Дата начала обучения: 02.11.2020

Дата окончания обучения: 16.11.2020

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование учебных модулей | Трудоёмкость (час) | Сроки обучения |
| 1 | Технические каналы утечки персональных данных | 12 | 2 дня |
| 2 | Способы и средства защиты персональных данных от утечки по техническим каналам | 8 | 1 день |
| 3 | Методы и средства контроля эффективности технической защиты персональных данных | 12 | 2 дня |
| 4 | Организация технической защиты персональных данных | 12 | 2 дня |
| 5 | Организационное обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 1 день |
| 6 | Правовое обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 1 день |
| Всего: | | 72 | 9 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 контро-ля** |
| **Лекции** | **Практи-ческие занятия** | **Самостоятельная работа** |
| 1 | Технические каналы утечки персональных данных | 12 | 3 | 6 | 3 | Нет |
| 1.1 | Цели и задачи защиты персональных данных от утечки по техниче­ским каналам (технической защиты персональных данных). | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 1.2 | Технические каналы утечки персональных данных при их обработке средствами информационных и коммуникационных технологий | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 1.3 | Технические каналы утечки акустической (речевой) информации при обработке персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 2 | Способы и средства защиты персональных данных от утечки по техническим каналам | 8 | 2 | 4 | 2 | Нет |
| 2.1 | Способы и средства защиты персональных данных при их обработке средствами информационных и коммуникационных технологий | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 2.2 | Способы и средства защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 3 | Методы и средства контроля эффективности технической защиты персональных данных | 12 | 3 | 3 | 3 | Нет |
| 3.1 | Методы и средства контроля эффективности технической защиты персональных данных при их обработке средствами информационных и коммуникационных технологий | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 3.2 | Методы и средства контроля эффективности защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 3.3 | Методы и средства выявления электронных устройств негласного получения персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 4 | Организация технической защиты персональных данных | 12 | 3 | 6 | 3 | Нет |
| 4.1 | Лицензирование деятельности в области технической защиты персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 4.2 | Сертификация средств технической защиты персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 4.3 | Аттестация объекта информатизации по требованиям безопасности персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 5 | Организационное обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 2 | 4 | 2 | Нет |
| 5.1 | Понятие организационной защиты персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 5.2 | Технологические меры и методы обеспечения физической безопасности объекта персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 6 | Правовое обеспечение безопасности персональных данных при их обработке в информационных системах | 8 | 2 | 4 | 2 | Нет |
| 6.1 | Персональные данные, как объект правового регулирования. Законодательство РФ в области защиты персональных данных. | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |
| 6.2 | Правовые режимы защиты персональных данных | 4 | 1 | 2 | 1 | Собеседование по вопросам темы |

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

**Модуль 1. Технические каналы утечки персональных данных (12 час.)**

**Тема 1.1**. Цели и задачи защиты персональных данных от утечки по техниче­ским каналам (технической защиты персональных данных). (4 час.)

Содержание темы: Термины и определения в области технической защиты персональных данных: объект информатизации, персональные данные, выделенное помещение, основные технические средства и системы, вспомогательные технические средства и системы, утечка персональных данных по техническому каналу, перехват персональных данных, средство разведки, специальное техническое средство негласного получения персональных данных, посторонние проводники, контролируемая зона, технический канал утечки персональных данных. Классификация технических каналов утечки персональных данных. Место технической защиты персональных данных в государственной системе защиты информации в Российской Федерации. Цели и задачи защиты персональных данных от утечки информации по техниче­ским каналам (технической защиты персональных данных). Нормативные документы по технической защите персональных данных.)

**Тема 1.2.** Технические каналы утечки персональных данных при их обработке средствами информационных и коммуникационных технологий (4 час.)

Содержание темы: Общая характеристика и классификация технических каналов утечки персональных данных при их обработке средствами информационных и коммуникационных технологий. Технические каналы утечки персональных данных, возникающие за счет побочных электромагнитных излучений. Технические каналы утечки персональных данных, возникающие за счет наводок побочных электромагнитных излучений. Технический канал утечки персональных данных, создаваемый путем «высокочастотного облу­чения» средств информационных и коммуникационных технологий. Технический канал утечки персональных данных, создаваемый путем внедрения в средства информационных и коммуникационных технологий электронных устройств негласного получения персональных данных.

**Тема 1.3.** Технические каналы утечки акустической (речевой) информации при обработке персональных данных (4 час.)

Содержание темы: Характери­стики речевого сигнала. Общая характеристика и классификация технических каналов утечки аку­стической информации при обработке персональных данных. Прямые акустические каналы утечки речевой информации при обработке персональных данных. Акустовибра­ционные каналы утечки речевой информации при обработке персональных данных. Акустооптический (оптикоэлектронный) канал утечки речевой информации при обработке персональных данных. Акустоэлектрические каналы утечки речевой информации при обработке персональных данных. Акустоэлектромагнитные каналы утечки речевой информации при обработке персональных данных. Средства акустической разведки и их технические характеристики.

**Модуль 2. Способы и средства защиты персональных данных от утечки по техническим каналам (8 час.)**

**Тема 2.1.** Способы и средства защиты персональных данных при их обработке средствами информационных и коммуникационных технологий (4 час.)

Содержание темы: Классификация способов и средств защиты объектов персональных данных. Экранирование технических средств их соединительных линий. Экранированные помещения. Заземление технических средств. Требования к системам электропитания и заземления основных технических средств и систем. Помехоподавляющие фильтры (принципы построения, основные характеристики, требования по установке). Системы пространственного и линейного электромагнитного зашумления (принципы построения, основные характеристики, требования по установке). Защищённые средства информационных и коммуникационных технологий.

**Тема 2.2**. Способы и средства защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных (4 час.)

Содержание темы: Классификация способов и средств защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных. Звукоизоляция выделенных помещений. Звукопоглощающие материалы. Системы и средства виброакустической маскировки (принципы построения, основные характеристики, требования по установке). Способы и средства защиты вспомогательных технических средств и систем. Специальные технические средства подавления электронных устройств перехвата утечки акустической (речевой) информации при обработке персональных данных (широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).

**Модуль 3. Методы и средства контроля эффективности технической защиты персональных данных (12 час.)**

**Тема 3.1**. Способы и средства защиты персональных данных при их обработке средствами информационных и коммуникационных технологий (4 час.)

Содержание темы: Показатели эффективности защиты персональных данных при их обработке средствами информационных и коммуникационных технологий. Требования к средствам измерения побочных электромагнитных излучений и наводок средств информационных и коммуникационных технологий и условиям проведения измерений; порядок проведения измерений. Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств информационных и коммуникационных технологий.

**Тема 3.2.** Методы и средства контроля эффективности защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных (4 час.)

Содержание темы: Показатели эффективности защиты речевой информации при обработке персональных данных. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции. Методика расчета словесной разборчивости речи. Ме­тодика оценки возможностей средств акустической разведки по перехвату речевой информации при обработке персональных данных. Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.

**Тема 3.3.** Методы и средства выявления электронных устройств негласного получения персональных данных (4 час.)

Содержание темы: Методы выявления электронных устройств негласного получения персональных данных, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения персональных данных: индикаторы электромагнитного поля, программно-аппаратные комплексы радиоконтроля, анализаторы проводных коммуникаций, нелинейные локаторы, рентгено-телевизионные комплексы. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения персональных данных.

**Модуль 4. Организация технической защиты персональных данных (8 час.)**

**Тема 4.1**. Лицензирование деятельности в области технической защиты персональных данных (4 час.)

Содержание темы: Общий порядок лицензирования деятельности в области защиты персональных данных: понятийный аппарат в области лицензирования, порядок получения лицензии, реестры лицензий на виды деятельности. Лицензирование деятельности в области защиты персональных данных: виды деятельности, подлежащие лицензированию; лицензирование деятельности в области защиты персональных данных контроль за соблюдением лицензиатом лицензионных требований и условий; соблюдение лицензиатом лицензионных требований и условий.

**Тема 4.2**. Сертификация средств технической защиты персональных данных (4 час.)

Содержание темы: Общий порядок сертификации средств технической защиты персональных данных: общие положения; система и процедура сертификации средств технической защиты персональных данных; приостановка или аннулирование сертификата; контроль и ответственность при сертификации. Порядок сертификации во ФСТЭК РФ: подача заявки на сертификацию во ФСТЭК РФ; решение на проведение сертификационных испытаний; заключение договора с испытательной лабораторией; подготовка исходных данных; сертификационные испытания; оформление результатов испытаний; заключение договора с органом по сертификации; экспертиза результатов сертификационных испытаний; решение о выдаче сертификата.

**Тема 4.3.** Аттестация объекта информатизации по требованиям безопасности персональных данных (4 час.)

Содержание темы: Объект информатизации. Аттестация объектов информатизации по требованиям безопасности персональных данных: аттестация и порядок её проведения; обязательная и добровольная аттестация; содержание и цель аттестации; перечень работ при аттестации; аккредитация органов по аттестации; структура системы аттестации; функции органов по аттестации; функции ФСТЭК в рамках системы аттестации; функции заявителей в рамках системы аттестации; функции испытательных центров в рамках системы аттестации; документы заявителя в орган по аттестации для проведения испытаний; документы заявителя в орган по аттестации в зависимости от особенностей аттестуемого объекта; порядок проведения аттестации объектов информатизации; содержание аттестационных испытаний; содержание протокола аттестационных испытаний; содержание аттестата соответствия.

**Модуль 5. Организационное обеспечение безопасности персональных данных при их обработке в информационных системах (8 час.)**

**Тема 5.1.** Понятие организационной защиты персональных данных (4 час.)

Содержание темы: Направления, принципы и условия организационной персональных данных. Подходы и требования к организации системы защиты персональных данных. Методы, силы и средства, используемые для организации защиты персональных данных.

**Тема 5.2** Технологические меры и методы обеспечения физической безопасности объекта персональных данных (4 час.)

Содержание темы: Средства и методы физической защиты объекта персональных данных. Структура системы физической защиты персональных данных. Процедурные меры обеспечения защиты персональных данных. Программно-технические методы обеспечения защиты персональных данных

**Модуль 6. Правовое обеспечение безопасности персональных данных при их обработке в информационных системах (8 час.)**

**Тема 6.1.** Персональные данные, как объект правового регулирования. Законодательство РФ в области защиты персональных данных (4 час.)

Содержание темы: Структура и состав законодательства РФ в области защиты персональных данных. Основные определения в области правового регулирования защиты персональных данных. Классификация и виды персональных данных.

**Тема 6.2** Правовые режимы защиты персональных данных (4 час.)

Содержание темы: Правовая защита персональных данных. Нормативно-правовое регулирование профессиональной и служебной тайны в сфере персональных данных.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 3.1 | Методы и средства контроля эффективности технической защиты персональных данных при их обработке средствами информационных и коммуникационных технологий | Разработка частной модели угроз безопасности персональных данных в информационной системе персональных данных (ИСПДн) | Исходная степень защищенности определяется следующим образом – (кол-во «+» делим на 7 и умножаем на 100 = %)  ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу).  ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.  ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.  При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Yx, а именно:  0 для высокой степени исходной защищенности;  5 для средней степени исходной защищенности;  10 для низкой степени исходной защищенности.  ИСПДн имеет \_\_\_\_\_\_\_\_уровень исходной защищенности, показатель исходной защищенности Y1 =\_\_\_\_. |
| 3.2 | Методы и средства контроля эффективности защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных | Определение класса защищенности информационной системы персональных данных (ИСПДн) | Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерный доступ, копирование, предоставление или распространение), целостности (уничтожение или модифицирование) или доступности (блокирование) информации.  УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],  где степень возможного ущерба определяется обладателем информации, заказчиком и (или) оператором самостоятельно экспертным или иными методами и может быть:  Высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции.  Средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций.  Низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.  Информация имеет высокий уровень значимости (УЗ1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности (конфиденциальности, целостности, доступности) определены низкие степени ущерба.  Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.  При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.  Информационная система имеет федеральный масштаб, если она функционирует в пределах Российской Федерации (федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.  Организация: ООО «…»  Персональные данные, обрабатываемые в ИСПДн:  Адрес;  данные об образовании;  ИНН;  паспортные данные;  ПСС;  сведения о трудовом стаже, метах работы;  состав семьи.  Масштаб информационной системы: объектовый.  Класс защищенности информационной системы определяется в соответствии с таблицей:   |  |  |  |  | | --- | --- | --- | --- | | Уровень значимости  информации | Масштаб информационной системы | | | | Федеральный | Региональный | Объектовый | | УЗ 1 | К1 | К1 | К1 | | УЗ 2 | К1 | К2 | К2 | | УЗ 3 | К2 | К3 | К3 | | УЗ 4 | К3 | К3 | К4 |   УЗ =\_\_\_\_\_\_.  На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_. |
| 3.3 | Методы и средства контроля эффективности технической защиты персональных данных при их обработке средствами информационных и коммуникационных технологий | Определение уровня защищенности информационной системы персональных данных (ИСПДн) | Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.  Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.  Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.  Организация: ООО «…».  Персональные данные, обрабатываемые в ИСПДн:  Сотрудники:  данные о родственниках (свидетельство о браке, свидетельство о рождении);  данные об образовании;  ИНН;  паспортные данные;  сведения о трудовом стаже;  сведения о составе семьи.  Внешние контрагенты:  должность;  ИНН;  паспортные данные;  сведения о доходах;  служебный телефон и адрес;  ФИО.  Объем обрабатываемых персональных данных: объектовый. до 100 000 субъектов ПДн.  Актуальны угрозы 2-типа.  На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности. |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1 | Проблема информационной безопасности общества.  Понятие – «информационная безопасность».  Понятие – «доступность информации».  Понятие – «целостность информации».  Понятие – «конфиденциальность информации».  Задачи информационной безопасности общества.  Уровни формирования режима информационной безопасности.  Правовые основы информационной безопасности общества.  Перечень законодательных актов РФ в области информационной безопасности и защиты информации.  Ответственность за нарушения в сфере информационной безопасности.  Требования безопасности к информационным системам (Стандарты информационной безопасности: «Общие критерии»).  Принцип иерархии: класс – семейство – компонент – элемент (Стандарты информационной безопасности: «Общие критерии»).  Функциональные требования (Стандарты информационной безопасности: «Общие критерии»).  Требования доверия требования (Стандарты информационной безопасности: «Общие критерии»).  Сервисы безопасности в вычислительных сетях.  Механизмы безопасности в вычислительных сетях.  Администрирование средств безопасности в вычислительных сетях.  ФСТЭК и ее роль в обеспечении информационной безопасности в РФ.  Документы по оценке защищенности автоматизированных систем в РФ.  Цели, задачи и содержание административного уровня информационной безопасности.  Разработка политики информационной безопасности.  Классы угроз информационной безопасности.  Каналы несанкционированного доступа к информации.  Особенности информационной безопасности в компьютерных сетях.  Специфика средств защиты в компьютерных сетях.  Понятие протокола передачи данных.  Принципы организации обмена данными в вычислительных сетях.  Транспортный протокол TCP и модель ТСР/IР.  Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO.  Характеристика уровней модели OSI/ISO.  Основы IP-протокола.  Классы адресов вычислительных сетей.  Система доменных имен.  Классы удаленных угроз и их характеристика.  Типовая удаленная атака – общая характеристика типовых удаленных атак.  Типовая удаленная атака – «анализ сетевого трафика».  Типовая удаленная атака – «подмена доверенного объекта».  Типовая удаленная атака – «ложный объект»  Типовая удаленная атака – «отказ в обслуживании».  Причины успешной реализации удаленных угроз в вычислительных сетях. | Объект информатизации.  Персональные данные.  Выделенное помещение.  Основные технические средства и системы,  Вспомогательные технические средства и системы.  Утечка персональных данных по техническому каналу,  Перехват персональных данных.  Средство разведки.  Специальное техническое средство негласного получения персональных данных.  Посторонние проводники.  Контролируемая зона.  Технический канал утечки персональных данных.  Классификация технических каналов утечки и персональных данных.  Место технической защиты персональных данных в государственной системе защиты информации в Российской Федерации.  Цели и задачи защиты персональных данных от утечки информации по техниче­ским каналам (технической защиты персональных данных).  Нормативные документы по технической защите персональных данных.  Общая характеристика и классификация технических каналов утечки персональных данных при их обработке средствами информационных и коммуникационных технологий.  Технические каналы утечки персональных данных, возникающие за счет побочных электромагнитных излучений.  Технические каналы утечки персональных данных, возникающие за счет наводок побочных электромагнитных излучений.  Технический канал утечки персональных данных, создаваемый путем «высокочастотного облу­чения» средств информационных и коммуникационных технологий.  Технический канал утечки информации, создаваемый путем внедрения в средства информационных и коммуникационных технологий электронных устройств негласного получения персональных данных.  Характери­стики речевого сигнала.  Общая характеристика и классификация технических каналов утечки аку­стической информации при обработке персональных данных.  Прямые акустические каналы утечки речевой информации при обработке персональных данных.  Акустовибра­ционные каналы утечки речевой информации при обработке персональных данных.  Акустооптический (оптикоэлектронный) канал утечки речевой информации при обработке персональных данных.  Акустоэлектрические каналы утечки речевой информации при обработке персональных данных.  Акустоэлектромагнитные каналы утечки речевой информации при обработке персональных данных. | Нет. |
| 2 | Классификация способов и средств защиты объектов персональных данных.  Экранирование тех­нических средств их соединительных линий.  Экранированные помещения.  Заземление техниче­ских средств.  Требования к системам электропитания и заземления основных технических средств и систем.  Помехоподавляющие фильтры − принципы построения, основные характеристики, требо­вания по установке.  Системы пространственного и линейного электромагнитного зашумления − принципы построения, основные характеристики, требования по установке.  Защищённые сред­ства информационных и коммуникационных технологий.  Классификация способов и средств защиты выделенных помещений от утечки акустической (речевой) информации при обработке персональных данных.  Звукоизоляция выделенных помещений.  Звукопоглощающие материалы.  Системы и средства виброакустической маскировки − принципы построения, основные характеристики, требования по установке.  Способы и средства защиты вспомогательных технических средств и систем.  Специальные технические средства подавления электронных устройств перехвата акустической (речевой) информации при обработке персональных данных − широкополосные генераторы шума.  Специальные технические средства подавления электронных устройств перехвата акустической (речевой) информации при обработке персональных данных − блокираторы средств сотовой связи,  Специальные технические средства подавления электронных устройств перехвата акустической (речевой) информации при обработке персональных данных − активные средства защиты телефонных линий связи. | Нет |
| 3 | Показатели эффективности защиты информации, обрабатываемой средствами информационных и коммуникационных технологий.  Требования к средствам измерения побочных электромагнитных излучений и наводок средств информационных и коммуникационных технологий и условиям проведения измерений.  Порядок проведения измерений побочных электромагнитных излучений и наводок средств информационных и коммуникационных технологий.  Методика оценки возможностей средств технической разведки по перехвату побочных электромагнитных излучений и наводок средств информационных и коммуникационных технологий.  Показатели эффективности защиты речевой информации при обработке персональных данных.  Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений; порядок проведения измерений уровня звуко- и виброизоляции.  Методика расчета словесной разборчивости речи.  Ме­тодика оценки возможностей средств акустической разведки по перехвату речевой информации при обработке персональных данных.  Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.  Тема 3.3. Методы и средства выявления электронных устройств негласного получения персональных данных.  Методы выявления электронных устройств негласного получения персональных данных, внедренных в выделенные помещения и технические средства.  Средства выявления электронных устройств негласного получения персональных данных: индикаторы электромагнитного поля.  Средства выявления электронных устройств негласного получения персональных данных: программно-аппаратные комплексы радиоконтроля.  Средства выявления электронных устройств негласного получения персональных данных: анализаторы проводных коммуникаций.  Средства выявления электронных устройств негласного получения персональных данных: нелинейные локаторы.  Средства выявления электронных устройств негласного получения персональных данных: рентгено-телевизионные комплексы.  Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения персональных данных. | Нет |
| 4 | персональных данных.  Основные понятия системы лицензирования деятельности в области технической защиты персональных данных.  Порядок получения лицензии в области технической защиты персональных данных.  Содержание заявления для получения лицензии в области технической защиты информации.  Перечень документов, прилагаемых к заявлению для получения лицензии в области технической защиты персональных данных.  Причины отказа в получении лицензии в области технической защиты персональных данных.  Содержание решения о предоставлении лицензии в области технической защиты персональных данных и документа, подтверждающего её наличие.  Приостановка действия или аннулирование лицензии в области технической защиты персональных данных.  Прекращение действия лицензии в области технической защиты персональных данных.  Реестры лицензий на виды деятельности в области технической защиты информации.  Виды деятельности, подлежащие лицензированию в области технической защиты информации.  Требования и условия к соискателю лицензии в области технической защиты персональных данных.  Перечень документов во ФСТЭК для соискателя лицензии в области технической защиты персональных данных.  Действия ФСТЭК при лицензировании деятельности в области технической защиты персональных данных.  Контроль за соблюдением лицензиатом лицензионных требований и условий − в области технической защиты персональных данных − плановая проверка лицензиата.  Контроль за соблюдением лицензиатом лицензионных требований и условий − в области технической защиты персональных данных − внеплановая проверка лицензиата.  Соблюдение лицензиатом лицензионных требований и условий − в области технической защиты персональных данных.  Аутсорсинг технической защиты персональных данных.  Сертификация средств технической защиты персональных данных − структура, система.  Сертификат соответствия средств технической защиты персональных данных.  Аккредитация сертификации средств технической защиты персональных данных.  Федеральный орган по сертификации средств технической защиты персональных данных.  Центральный орган по сертификации средств технической защиты персональных данных.  Органы по сертификации средств технической защиты персональных данных.  Испытательные лаборатории по сертификации средств технической защиты персональных данных.  Сертификация средств технической защиты персональных данных − изготовители средств технической защиты персональных данных.  Процедура сертификации средств технической защиты персональных данных.  Приостановка или аннулирование сертификата средств технической защиты персональных данных.  Контроль и ответственность при сертификации средств технической защиты персональных данных.  Порядок сертификации во ФСТЭК РФ − подача заявки на сертификацию во ФСТЭК РФ.  Порядок сертификации во ФСТЭК РФ − решение на проведение сертификационных испытаний.  Порядок сертификации во ФСТЭК РФ − заключение договора с испытательной лабораторией.  Порядок сертификации во ФСТЭК РФ − подготовка исходных данных.  Порядок сертификации во ФСТЭК РФ − сертификационные испытания.  Порядок сертификации во ФСТЭК РФ − оформление результатов испытаний.  Порядок сертификации во ФСТЭК РФ − заключение договора с органом по сертификации.  Порядок сертификации во ФСТЭК РФ − экспертиза результатов сертификационных испытаний.  Порядок сертификации во ФСТЭК РФ − решение о выдаче сертификата.  Аттестация объектов информатизации по требованиям безопасности персональных данных и порядок её проведения.  Обязательная и добровольная аттестация объектов информатизации по требованиям безопасности персональных данных.  Содержание и цель аттестации объектов информатизации по требованиям безопасности персональных данных.  Перечень работ при аттестации объектов информатизации по требованиям безопасности персональных данных.  Аккредитация органов по аттестации объектов информатизации по требованиям безопасности персональных данных.  Структура системы аттестации объектов информатизации по требованиям безопасности персональных данных.  Функции органов по аттестации объектов информатизации по требованиям безопасности персональных данных.  Функции ФСТЭК в рамках системы аттестации объектов информатизации по требованиям безопасности персональных данных.  Функции заявителей в рамках системы аттестации объектов информатизации.  Функции испытательных центров в рамках системы аттестации объектов информатизации по требованиям безопасности персональных данных.  Документы заявителя в орган по аттестации для проведения испытаний объектов информатизации по требованиям безопасности персональных данных.  Документы заявителя в орган по аттестации в зависимости от особенностей аттестуемого объекта информатизации по требованиям безопасности персональных данных.  Порядок проведения аттестации объекта информатизации.  Содержание аттестационных испытаний объекта информатизации по требованиям безопасности персональных данных.  Содержание протокола аттестационных испытаний объекта информатизации по требованиям безопасности персональных данных.  Содержание аттестата соответствия объекта информатизации по требованиям безопасности персональных данных. | Нет |
| 5 | Направления, принципы и условия организационной защиты персональных данных.  Подходы и требования к организации системы защиты персональных данных.  Методы, силы и средства, используемые для организации защиты персональных данных.  Средства и методы физической защиты объекта персональных данных.  Структура системы физической защиты персональных данных.  Процедурные меры обеспечения защиты персональных данных.  Программно-технические методы обеспечения защиты персональных данных. | Нет |
| 6 | Структура и состав законодательства РФ в области защиты персональных данных.  Основные определения в области правового регулирования защиты персональных данных.  Классификация и виды персональных данных.  Правовая защита персональных данных.  Нормативно-правовое регулирование профессиональной и служебной тайны в сфере персональных данных. | Нет |

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

По результатам зачета обучающемуся выставляется оценка «зачтено» или «незачтено».

Оценка «зачтено» выставляется обучающемуся, если:

обучающийся знает и воспроизводит основные положения дисциплины в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;

обучающийся продемонстрировал базовые знания, умения и навыки важнейших разделов программы и содержания лекционного курса;

у обучающегося не имеется затруднений в использовании научно-понятийного аппарата в терминологии курса, а если затруднения имеются, то они незначительные;

на дополнительные вопросы преподавателя обучающийся дал правильные или частично правильные ответы.

Компетенция (и) или ее часть (и) сформированы на базовом уровне

Оценка «не зачтено» ставится на зачете обучающийся, если:

обучающийся имеет представление о содержании дисциплины, но не знает основные положения темы, к которому относится задание, не способен выполнить задание с очевидным решением;

имеются существенные пробелы в знании основного материала по программе курса;

в процессе ответа по теоретическому и практическому материалу, содержащемуся в вопросах билета, допущены принципиальные ошибки при изложении материала;

имеются систематические пропуски обучающийся лекционных и практических занятий по неуважительным причинам;

во время текущего контроля обучающийся набрал недостаточные для допуска к зачету баллы;

вовремя не подготовил отчет по практическим занятиям, предусмотренным РПД.

Компетенция(и) или ее часть (и) не сформированы..

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

Практическое задание №1: Разработка частной модели угроз безопасности персональных данных в информационной системе персональных данных (ИСПДн)

Исходный уровень защищенности ИСПДн.

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице 1 представлены характеристики уровня исходной защищенности для ИСПДн «…..» в ООО «………………..».

Таблица 1 – Исходный уровень защищенности

| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
| --- | --- | --- | --- |
| Высокий  0 | Средний  5 | Низкий  10 |
| 1. По территориальному размещению: | | | |
| - распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | - | - |  |
| - городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); | - | - |  |
| - корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | - |  | - |
| - локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; | - |  | - |
| - локальная ИСПДн, развернутая в пределах одного здания |  | - | - |
| 2. По наличию соединения с сетями общего пользования: | | | |
| - ИСПДн, имеющая многоточечный выход в сеть общего пользования; | - | - |  |
| - ИСПДн, имеющая одноточечный выход в сеть общего пользования | - |  | - |
| - ИСПДн, физически отделенная от сети общего пользования |  | - | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: | | | |
| - чтение, поиск; |  | - | - |
| - запись, удаление, сортировка; | - |  | - |
| - модификация, передача | - | - |  |
| 4. По разграничению доступа к персональным данным: | | | |
| - ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн; | - |  | - |
| - ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПД; | - | - |  |
| - ИСПДн с открытым доступом | - | - |  |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн | | | |
| - интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | - | - |  |
| - ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн |  | - | - |
| 6. По уровню обобщения (обезличивания) ПДн: | | | |
| - ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации); |  | - | - |
| - ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; | - |  | - |
| - ИСПДн, в которой предоставляемые пользователю не являются обезличенными (присутствует информация, позволяющая идентифицировать субъекта ПДн) | - | - |  |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: | | | |
| - ИСПДн, предоставляющая всю БД с ПДн; | - | - |  |
| - ИСПДн, предоставляющая часть ПДн; | - |  | - |
| - ИСПДн, не предоставляющие никакой информации |  | - | - |
| Характеристики ИСПДн |  |  |  |

Исходная степень защищенности определяется следующим образом – (кол-во «+» делим на 7 и умножаем на 100 = %)

ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу).

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.

ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Yx, а именно:

0 для высокой степени исходной защищенности;

5 для средней степени исходной защищенности;

10 для низкой степени исходной защищенности.

ИСПДн имеет \_\_\_\_\_\_\_\_уровень исходной защищенности, показатель исходной защищенности Y1 =\_\_\_\_.

Вероятность реализации УБПДн.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

* маловероятно -– отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
* низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
* средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
* высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы: (смотрим Типовую модель угроз для конкретной ИСПДн).

Угрозы утечки информации по техническим каналам.

#### Угрозы утечки акустической (речевой) информации.

Вероятность реализации угрозы – маловероятна.

#### Угрозы утечки видовой информации.

Вероятность реализации угрозы – маловероятна.

Угрозы утечки информации по каналам ПЭМИН.

Вероятность реализации угрозы – средняя вероятность.

Угрозы несанкционированного доступа к информации.

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

##### Кража ПЭВМ.

Вероятность реализации угрозы – средняя вероятность.

Кража носителей информации.

Вероятность реализации угрозы – средняя вероятность.

Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Непреднамеренная модификация (уничтожение) информации сотрудниками.

Вероятность реализации угрозы – низкая вероятность.

Реализуемость угроз.

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы

следующим образом:

если 0 < Y <0,3, то возможность реализации угрозы признается низкой;

если 0,3 < Y < 0,6, то возможность реализации угрозы признается средней;

если 0,6 < Y < 0,8, то возможность реализации угрозы признается высокой;

если Y > 0,8, то возможность реализации угрозы признается очень высокой.

Таблица 2 – Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации |  |  |
| 1.2. Угрозы утечки видовой информации |  |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |  |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | |
| 2.1.1. Кража ПЭВМ |  |  |
| 2.1.2.Кража носителей информации |  |  |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками |  |  |

Оценка опасности угроз.

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Таблица 3 – Опасность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ | Средняя |
| 2.1.2. Кража носителей информации | Средняя |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками | Средняя |

Определение актуальности угроз в ИСПДн.

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 4 – Правила определения актуальности УБПДн

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности представлена в таблице 5.

Таблица 5 – Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации |  |
| 1.2. Угрозы утечки видовой информации |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ |  |
| 2.1.2. Кража носителей информации |  |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками |  |

**.**

**8.4. Тесты и обучающие задачи (кейсы), иные практико-ориентированные формы заданий**

Практическое задание №1: Разработка частной модели угроз безопасности персональных данных в информационной системе персональных данных (ИСПДн)

Исходный уровень защищенности ИСПДн.

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице 1 представлены характеристики уровня исходной защищенности для ИСПДн «…..» в ООО «………………..».

Таблица 1 – Исходный уровень защищенности

| Технические и эксплуатационные характеристики ИСПДн | Уровень защищенности | | |
| --- | --- | --- | --- |
| Высокий  0 | Средний  5 | Низкий  10 |
| 1. По территориальному размещению: | | | |
| - распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | - | - |  |
| - городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); | - | - |  |
| - корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; | - |  | - |
| - локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; | - |  | - |
| - локальная ИСПДн, развернутая в пределах одного здания |  | - | - |
| 2. По наличию соединения с сетями общего пользования: | | | |
| - ИСПДн, имеющая многоточечный выход в сеть общего пользования; | - | - |  |
| - ИСПДн, имеющая одноточечный выход в сеть общего пользования | - |  | - |
| - ИСПДн, физически отделенная от сети общего пользования |  | - | - |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: | | | |
| - чтение, поиск; |  | - | - |
| - запись, удаление, сортировка; | - |  | - |
| - модификация, передача | - | - |  |
| 4. По разграничению доступа к персональным данным: | | | |
| - ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн; | - |  | - |
| - ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПД; | - | - |  |
| - ИСПДн с открытым доступом | - | - |  |
| 5. По наличию соединений с другими базами ПДн иных ИСПДн | | | |
| - интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | - | - |  |
| - ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн |  | - | - |
| 6. По уровню обобщения (обезличивания) ПДн: | | | |
| - ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации); |  | - | - |
| - ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации; | - |  | - |
| - ИСПДн, в которой предоставляемые пользователю не являются обезличенными (присутствует информация, позволяющая идентифицировать субъекта ПДн) | - | - |  |
| 7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: | | | |
| - ИСПДн, предоставляющая всю БД с ПДн; | - | - |  |
| - ИСПДн, предоставляющая часть ПДн; | - |  | - |
| - ИСПДн, не предоставляющие никакой информации |  | - | - |
| Характеристики ИСПДн |  |  |  |

Исходная степень защищенности определяется следующим образом – (кол-во «+» делим на 7 и умножаем на 100 = %)

ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу).

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности.

ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Yx, а именно:

0 для высокой степени исходной защищенности;

5 для средней степени исходной защищенности;

10 для низкой степени исходной защищенности.

ИСПДн имеет \_\_\_\_\_\_\_\_уровень исходной защищенности, показатель исходной защищенности Y1 =\_\_\_\_.

Вероятность реализации УБПДн.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

* маловероятно -– отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
* низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
* средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
* высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

При обработке персональных данных в ИСПДн можно выделить следующие угрозы: (смотрим Типовую модель угроз для конкретной ИСПДн).

Угрозы утечки информации по техническим каналам.

#### Угрозы утечки акустической (речевой) информации.

Вероятность реализации угрозы – маловероятна.

#### Угрозы утечки видовой информации.

Вероятность реализации угрозы – маловероятна.

Угрозы утечки информации по каналам ПЭМИН.

Вероятность реализации угрозы – средняя вероятность.

Угрозы несанкционированного доступа к информации.

Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

##### Кража ПЭВМ.

Вероятность реализации угрозы – средняя вероятность.

Кража носителей информации.

Вероятность реализации угрозы – средняя вероятность.

Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

Непреднамеренная модификация (уничтожение) информации сотрудниками.

Вероятность реализации угрозы – низкая вероятность.

Реализуемость угроз.

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы

следующим образом:

если 0 < Y <0,3, то возможность реализации угрозы признается низкой;

если 0,3 < Y < 0,6, то возможность реализации угрозы признается средней;

если 0,6 < Y < 0,8, то возможность реализации угрозы признается высокой;

если Y > 0,8, то возможность реализации угрозы признается очень высокой.

Таблица 2 – Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| 1. Угрозы от утечки по техническим каналам. | | |
| 1.1. Угрозы утечки акустической информации |  |  |
| 1.2. Угрозы утечки видовой информации |  |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |  |
| 2. Угрозы несанкционированного доступа к информации. | | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | | |
| 2.1.1. Кража ПЭВМ |  |  |
| 2.1.2.Кража носителей информации |  |  |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками |  |  |

Оценка опасности угроз.

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Таблица 3 – Опасность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации | Низкая |
| 1.2. Угрозы утечки видовой информации | Низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | Низкая |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ | Средняя |
| 2.1.2. Кража носителей информации | Средняя |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками | Средняя |

Определение актуальности угроз в ИСПДн.

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 4 – Правила определения актуальности УБПДн

|  |  |  |  |
| --- | --- | --- | --- |
| Возможность реализации угрозы | Показатель опасности угрозы | | |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности представлена в таблице 5.

Таблица 5 – Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Актуальность  угрозы |
| 1. Угрозы от утечки по техническим каналам. | |
| 1.1. Угрозы утечки акустической информации |  |
| 1.2. Угрозы утечки видовой информации |  |
| 1.3. Угрозы утечки информации по каналам ПЭМИН |  |
| 2. Угрозы несанкционированного доступа к информации. | |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн | |
| 2.1.1. Кража ПЭВМ |  |
| 2.1.2. Кража носителей информации |  |
| 2.2. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. | |
| 2.2.1.Непреднамеренная модификация (уничтожение) информации сотрудниками |  |

Практическое задание №2: Определение класса защищенности информационной системы персональных данных (ИСПДн)

Класс защищенности информационной системы.

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации.

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерный доступ, копирование, предоставление или распространение), целостности (уничтожение или модифицирование) или доступности (блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации, заказчиком и (или) оператором самостоятельно экспертным или иными методами и может быть:

Высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции.

Средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций.

Низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Информация имеет минимальный уровень значимости (УЗ 4), если обладателем информации и (или) оператором степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) не может быть определена, но при этом информация подлежит защите в соответствии с законодательством Российской Федерации.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Информационная система имеет федеральный масштаб, если она функционирует в пределах Российской Федерации (федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система.

Информационная система имеет региональный масштаб, если она функционирует в пределах субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует в пределах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, подведомственных и иных организациях.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

Вариант 1

Организация: ООО «…»

Персональные данные, обрабатываемые в ИСПДн:

Адрес;

данные об образовании;

ИНН;

паспортные данные;

ПСС;

сведения о трудовом стаже, метах работы;

состав семьи.

Масштаб информационной системы: объектовый.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

УЗ =\_\_\_\_\_\_.

На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_.

Вариант 2

Организация: ООО «…»

Персональные данные, обрабатываемые в ИСПДн:

Данные о клиенте:

ФИО руководителя;

ФИО сотрудника;

рабочий телефон руководителя;

рабочий телефон сотрудника;

Масштаб информационной системы: федеральный.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

УЗ =\_\_\_\_\_\_.

На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_.

Вариант 3

Организация: ООО «…» (ЖКХ).

Персональные данные, обрабатываемые в ИСПДн:

Данные о проживающих:

адрес;

задолженность по оплате;

паспортные данные;

родственные отношения проживающих;

ФИО.

Масштаб информационной системы: региональный.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

УЗ =\_\_\_\_\_\_.

На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_.

Вариант 4

Организация: Больница.

Персональные данные, обрабатываемые в ИСПДн:

истории болезни.

Масштаб информационной системы: объектовый.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

УЗ =\_\_\_\_\_\_.

На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_.

Вариант 5

Организация: Законодательное собрание.

Персональные данные, обрабатываемые в ИСПДн:

Сотрудники и депутаты Законодательного собрания:

данные о родственниках (свидетельство о браке, свидетельство о рождении);

данные об образовании;

ИНН;

паспортные данные;

сведения о трудовом стаже;

сведения о составе семьи.

Физические лица, обратившиеся в Законодательное Собрание:

данные пенсионного удостоверения;

домашний телефон и адрес;

ИНН;

паспортные данные;

сведения о доходах;

сведения о постановке на воинский учет для военнообязанных;

сведения об образовании, трудовой деятельности, составе семьи;

ФИО.

Масштаб информационной системы: объектовый.

Класс защищенности информационной системы определяется в соответствии с таблицей:

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень значимости  информации | Масштаб информационной системы | | |
| Федеральный | Региональный | Объектовый |
| УЗ 1 | К1 | К1 | К1 |
| УЗ 2 | К1 | К2 | К2 |
| УЗ 3 | К2 | К3 | К3 |
| УЗ 4 | К3 | К3 | К4 |

УЗ =\_\_\_\_\_\_.

На основании полученных данных информационной системе персональных данных присвоен класс защищенности К \_\_\_.

Практическое задание №3: Определение уровня защищенности информационной системы персональных данных (ИСПДн)

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются 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, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Вариант 1

Организация: ООО «…».

Персональные данные, обрабатываемые в ИСПДн:

Сотрудники:

данные о родственниках (свидетельство о браке, свидетельство о рождении);

данные об образовании;

ИНН;

паспортные данные;

сведения о трудовом стаже;

сведения о составе семьи.

Внешние контрагенты:

должность;

ИНН;

паспортные данные;

сведения о доходах;

служебный телефон и адрес;

ФИО.

Объем обрабатываемых персональных данных: объектовый. до 100 000 субъектов ПДн.

Актуальны угрозы 2-типа.

На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности.

Вариант 2

Организация: ООО «…».

Персональные данные, обрабатываемые в ИСПДн:

данные о клиенте: ФИО руководителя, рабочий телефон.

Объем обрабатываемых персональных данных: объектовый. до 100 000 субъектов ПДн.

Актуальны угрозы 3-типа.

На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности.

Вариант 3

Организация: ООО «…» (ЖКХ).

Персональные данные, обрабатываемые в ИСПДн:

Данные о проживающих:

адрес;

задолженность по оплате;

паспортные данные;

родственные отношения проживающих;

ФИО.

Объем обрабатываемых персональных данных: объектовый. более 100 000 субъектов ПДн.

Актуальны угрозы 2-типа.

На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности.

Вариант 4

Организация: Больница.

Персональные данные, обрабатываемые в ИСПДн:

истории болезни.

Объем обрабатываемых персональных данных: объектовый. до 100 000 субъектов ПДн.

Актуальны угрозы 2-типа.

На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности.

Вариант 5

Организация: Законодательное собрание.

Персональные данные, обрабатываемые в ИСПДн:

Сотрудники и депутаты Законодательного собрания:

данные о родственниках (свидетельство о браке, свидетельство о рождении);

данные об образовании;

ИНН;

паспортные данные;

сведения о трудовом стаже;

сведения о составе семьи.

Физические лица, обратившиеся в Законодательное Собрание:

данные пенсионного удостоверения;

домашний телефон и адрес;

ИНН;

паспортные данные;

сведения о доходах;

сведения о постановке на воинский учет для военнообязанных;

сведения об образовании, трудовой деятельности, составе семьи;

ФИО.

Объем обрабатываемых персональных данных: объектовый. до 100 000 субъектов ПДн.

Актуальны угрозы 1-типа.

На основании полученных данных информационной системе персональных данных присвоен: \_\_\_\_\_\_ уровень защищенности.

**8.5. Описание процедуры оценивания результатов обучения**

Проверка полученных результатов индивидуальных заданий.

**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 | Газизов Андрей Равильевич | ДГТУ, доцент кафедры «Вычислительные системы и информационная безопасность, Кандидат педагогических наук |  | C:\Users\achebysheva\Desktop\пцс\фото преподавателей\Газизов.jpg | Да |
| 2 | Фатхи Владимир Ахатович | ДГТУ, зав. кафедры «Вычислительные системы и информационная безопасность, Доктор технических наук, профессор |  | C:\Users\achebysheva\Desktop\пцс\фото преподавателей\фатхи.jpg | Да |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| **Методы, формы и технологии** | **Методические разработки,**  **материалы курса, учебная литература** |
| Опрос (беседа преподавателя и обучающегося) на лабораторном занятии – для проведения текущего контроля по итогам освоения отдельных тем | <http://fpk.skif.donstu.ru/enrol/index.php?id=312> |
| Тест (стандартизированное задание, позволяющее автоматизировать процедуру измерения уровня знаний, умений и навыков обучающегося) на лабораторном занятии – для проведения текущего контроля по итогам освоения отдельных тем | <http://fpk.skif.donstu.ru/enrol/index.php?id=312> |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| **Электронные**  **образовательные ресурсы** | **Электронные**  **информационные ресурсы** |
| <http://fpk.skif.donstu.ru/enrol/index.php?id=312> | Информационно-справочная система «Гарант».  Информационно-справочная система «Кодекс».  Информационно-справочная система «Консультант плюс».  Информационно-справочная система «Техэксперт»  Международная реферативная база данных научных изданий Scopus https://www.scopus.com/.  Международная реферативная база данных научных изданий Web of Science http://www.wokinfo.com/.  Профессиональная база данных ЭБС IPRbooks http://www.iprbookshop.ru/.  Профессиональная база данных ЭБС Лань https://e.lanbook.com/.  Профессиональная база данных ЭБС Университетская библиотека онлайн https://biblioclub.ru/. |

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

|  |  |
| --- | --- |
| **Вид занятий** | **Наименование оборудования,**  **программного обеспечения** |
| Лекция | Помещения для лекционных занятий, оснащенные компьютерной техникой с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду университета, к профессиональным базам данных, информационным справочным и поисковым системам |
| Практическое занятие | Помещения для практических занятий, оснащенные компьютерной техникой с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду университета, к профессиональным базам данных, информационным справочным и поисковым системам |
| Самостоятельная работа | Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду университета, к профессиональным базам данных, информационным справочным и поисковым системам |

**III. ПАСПОРТ КОМПЕТЕНЦИЙ**

**программы повышения квалификации**

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

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

1. **Компетенция ОПК-1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | **Наименование компетенции** | | ОПК-1 | |
| 2. | **Указание типа компетенции** | **общекультурная/**  **универсальная** | Нет | |
| **общепрофессиональная** | Нет | |
| **профессиональная** | способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-l);  способность использовать нормативные право вые документы в своей профессиональной деятельности (ПК-3);  способность формировать комплекс мер по информационной безопасности с учетом его пра­вовой обоснованности, административно-управленческой и технической реализуемости и эконо­мической целесообразности (ПК-4);  способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организацион­ной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития техно­логий защиты информации (ПК-5);  способность организовать про ведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);  способность определять виды и формы информации, подверженной угрозам, виды и возможные методы, и пути реализации угроз на основе анализа структуры и содержания информаци­онных процессов предприятия, целей и задач деятельности предприятия (ПК-8);  способность выполнять работы по установке, настройке и обслуживанию технических и про­граммно-аппаратных средств защиты информации (ПК -11);  способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-12);  способность применять методы анализа изучаемых явлений, процессов и проектных решений (ПК-20);  способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);  способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-23). | |
| профессионально-специализированная | Нет | |
| 3. | **Определение, содержание и основные сущностные характеристики компетенции** | | Слушатели, прошедшие обучение, должны:  **а) знать:**  основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;  основные виды угроз безопасности персональных данных в информационных системах персональных данных;  содержание и порядок организации работ по выявлению угроз безопасности персональных данных;  процедуры задания и реализации требований по защите информации в информационных системах персональных данных;  меры обеспечения безопасности персональных данных;  требования по обеспечению безопасности персональных данных;  порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.  **б) уметь:**  создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;  планировать мероприятия по обеспечению безопасности персональных данных;  обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;  проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;  определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.  **в) владеть:**  навыками работы с правовыми базами данных;  навыками определения уровней защищённости персональных данных;  навыками выявления угроз безопасности персональных данных в информационных системах персональных данных;  навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;  навыками применения сертифицированных средств защиты информации. | |
| 4. | **Дескриптор знаний, умений и навыков по уровням** | | **Уровни сформированности компетенции обучающегося** | **Индикаторы** |
|  | | **Начальный уровень** | Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается |
|  | | **Базовый уровень** | Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности |
|  | | **Продвинутый** | Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности |
|  | | **Профессиональный** | Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности |
| 5. | **Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции** | | Нет | |
| 6. | **Средства и технологии оценки** | | Оценка «зачтено» выставляется обучающемуся, если:  обучающийся набрал по текущему контролю необходимые и достаточные баллы для выставления оценки автоматом;  обучающийся знает и воспроизводит основные положения дисциплины в соответствии с заданием, применяет их для выполнения типового задания в котором очевиден способ решения;  обучающийся продемонстрировал базовые знания, умения и навыки важнейших разделов программы и содержания лекционного курса;  у обучающегося не имеется затруднений в использовании научно-понятийного аппарата в терминологии курса, а если затруднения имеются, то они незначительные;  на дополнительные вопросы преподавателя обучающийся дал правильные или частично правильные ответы.  Компетенция (и) или ее часть (и) сформированы на базовом уровне (  Оценка «не зачтено» ставится на зачете обучающийся, если:  обучающийся имеет представление о содержании дисциплины, но не знает основные положения темы, к которому относится задание, не способен выполнить задание с очевидным решением;  имеются существенные пробелы в знании основного материала по программе курса;  в процессе ответа по теоретическому и практическому материалу, содержащемуся в вопросах билета, допущены принципиальные ошибки при изложении материала;  имеются систематические пропуски обучающийся лекционных и практических занятий по неуважительным причинам;  во время текущего контроля обучающийся набрал недостаточные для допуска к зачету баллы;  вовремя не подготовил отчет по практическим занятиям, предусмотренным РПД.  Компетенция(и) или ее часть (и) не сформированы. | |

**IV.Иная информация о качестве и востребованности образовательной программы**

Нет в наличии

**V.Рекомендаций к программе от работодателей**:

отзыв-рекомендации

**VI.Указание на возможные сценарии профессиональной траектории граждан**

**Сценарии профессиональной траектории граждан**

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

|  |  |
| --- | --- |
| **Цели получения персонального цифрового сертификата** | |
| **текущий статус** | **цель** |
| **Трудоустройство** | |
| состоящий на учете в Центре занятости | трудоустроенный, самозанятый (фриланс), |
| безработный по состоянию здоровья |
| **Развитие компетенций в текущей сфере занятости** | |
| Работающий по найму в организации, на предприятии | Развитие профессиональных качеств |
| Работающий по найму в организации, на предприятии | Повышение заработной платы, смена работы без изменения сферы профессиональной деятельности |
| Временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | Повышение уровня дохода |
| Временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | Сохранение и развитие квалификации |
| **Переход в новую сферу занятости** | |
| Освоение смежных профессиональных областей | Повышение уровня дохода, расширение профессиональной деятельности |

**VII.Дополнительная информация**

отсутствует

**VIII.Приложенные Скан-копии**

Утвержденной рабочей программа (подпись, печать, в формате pdf)