МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ярославский государственный университет им. П.Г. Демидова»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.А.Кузнецова
(подпись)
«05» сентября 2022 г.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА**

программа повышения квалификации

# «Защита информации и персональных данных»

для лиц, имеющих высшее и/или среднее профессиональное образование

*Программа разработана для государственных гражданских служащих, работающих в службах ответственных за организацию обработки и защиту информации, в том числе персональных данных, или исполняющих обязанности лиц, ответственных за организацию обработки и защиту персональных данных,*

*в соответствии с требованиями Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и приказом Министерства образования и науки Российской Федерации от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»*

*с учетом требований профессионального стандарта Специалист по защите информации в автоматизированных системах (Приказ Минтруда России от 15.09.2016 № 522н)*

16 академических часов

Форма обучения: очная

Ярославль 2022

# АННОТАЦИЯ

Дополнительная профессиональная программа повышения квалификации «Защита информации и персональных данных» направлена на формирование и развитие компетенций, необходимых для организации и осуществления деятельности по обеспечению безопасности персональных данных, как при их обработке в информационных системах, так и при их обработке без использования средств автоматизации.

Программа разработана в соответствии с требованиями Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» и приказом Министерства образования и науки Российской Федерации от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», с учетом общеотраслевых квалификационных характеристик должностей работников, занятых на предприятиях, в учреждениях и организациях (Постановление Минтруда РФ от 21.08.1998 № 37 «Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих»), а также требований профессионального стандарта Специалист по защите информации в автоматизированных системах (Приказ Минтруда России от 15.09.2016 № 522н).

В результате обучения выпускник:

**будет знать:**

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- последовательность проведения работ по защите персональных данных;
- порядок и методику классификации информационных систем и определения уровня защищенности персональных данных;
- основные идеи, лежащие в основе моделирования нарушителей безопасности персональных данных;
- основные внешние и внутренние угрозы для персональных данных при их обработке в информационных системах и без использования средств автоматизации;
- порядок обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации;
- полномочия и зоны ответственности регуляторов в сфере обеспечения безопасности персональных данных;

**будет уметь:**

- планировать мероприятия по обеспечению безопасности персональных данных;
- выявлять процессы, связанные с обработкой персональных данных и устанавливать границы информационных систем;
- разрабатывать необходимые уведомительные документы;
- определять уровень защищенности персональных данных;
- осуществлять выбор и контроль выбора средств защиты информации.

**Требования к слушателям**

Высшее или среднее профессиональное образование.

**Объем программы** 16 акад.часов.

**Срок реализации программы:** 2 недели, в соответствии с календарным графиком.

**Форма обучения:** очная.

**Особенности программы:**

Программа предназначена для государственных гражданских служащих, работающих в службах ответственных за организацию обработки и защиту информации, в том числе персональных данных, или исполняющих обязанности лиц, ответственных за организацию обработки и защиту персональных данных.

Лица, освоившие дополнительную профессиональную программу повышения квалификации и прошедшие итоговую аттестацию, получают **удостоверение о повышении квалификации установленного образца**.

1. **Общие сведения**

Дополнительная профессиональная программа повышения квалификации (ДПП ПК) «Защита информации и персональных данных» устанавливает требования к результатам обучения, определяет содержание и виды учебных занятий и контроля результатов обучающихся.

ДПП ПК предназначена для преподавателей и лиц, осваивающих образовательную программу (обучающихся).

2. **Цели и результаты освоения программы**

Дополнительная профессиональная программа повышения квалификации «Защита информации и персональных данных» направлена на формирование и развитие профессиональных компетенций, необходимых для организации и осуществления деятельности по обработке и защите персональных данных в органах государственной власти и местного самоуправления.

Программа разработана с учетом:

- общеотраслевых квалификационных характеристик должностей работников, занятых на предприятиях, в учреждениях и организациях (Постановление Минтруда РФ от 21.08.1998 № 37 «Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих»), а также требований профессионального стандарта Специалист по защите информации в автоматизированных системах (Приказ Минтруда России от 15.09.2016 № 522н).

Целью программы является **совершенствование профессиональных компетенций,** необходимых, в частности, для осуществления следующих трудовых функций работников в соответствии с профессиональными стандартами:

| Наименование профессионального стандарта | Трудовая функция |
|---|---|
| Специалист по защите информации в автоматизированных системах | С/02.6 Разработка организационно-распорядительных документов по защите информации в автоматизированных системах |
| | С/04.6 Внедрение организационных мер по защите информации в автоматизированных системах |

В результате обучения выпускник будет:

**будет знать:**

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- последовательность проведения работ по защите персональных данных;
- порядок и методику классификации информационных систем и определения уровня защищенности персональных данных;
- основные идеи, лежащие в основе моделирования нарушителей безопасности персональных данных;
- основные внешние и внутренние угрозы для персональных данных при их обработке в информационных системах и без использования средств автоматизации;
- порядок обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации;
- полномочия и зоны ответственности регуляторов в сфере обеспечения безопасности персональных данных;

**будет уметь:**

- планировать мероприятия по обеспечению безопасности персональных данных;
- выявлять процессы, связанные с обработкой персональных данных и устанавливать границы информационных систем;
- разрабатывать необходимые уведомительные документы;
- определять уровень защищенности персональных данных;
- осуществлять выбор и контроль выбора средств защиты информации.

Лица, освоившие дополнительную профессиональную программу повышения квалификации и прошедшие итоговую аттестацию, получают ***удостоверение о повышении квалификации установленного образца.***

**Требования к слушателям**

Высшее или среднее профессиональное образование.

3. **Нормативно-правовая база программы**

Программа разработана с учетом требований следующих правовых документов:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Приказ Министерства образования и науки Российской Федерации от 01.07.2013 № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
6. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
8. Приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
9. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 года № 152.

4. **Объем и сроки реализации программы**

Объем программы 16 акад. часа, с учетом всех видов учебной нагрузки. Срок реализации программы: 2 недели, в соответствии с календарным учебным графиком.

5. **Форма обучения и форма реализации программы**

Форма обучения – очная.

6. **Учебный план и структура программы повышения квалификации**

«Защита информации и персональных данных» 16 акад. часа.

| № | Наименование тем, разделов | Всего акад. часов | В том числе | | | |
|---|---|---|---|---|---|---|
| | | | Лекции | Практические работы, лабораторные, семинарские занятия | СР | Форма контроля результатов освоения |
| **1.** | **Общие вопросы технической защиты информации. Техническая защита персональных данных** | **10** | **2** | **8** | | |
| 1.1 | Правовые и организационные основы технической защиты информации ограниченного доступа (основные принципы информационной безопасности: конфиденциальность, целостность, доступность, «черные» и «белые» списки, зонирование (изоляция) информационных ресурсов, минимизация привилегий):<br>- законодательство Российской Федерации в области информационной безопасности, ответственность за нарушение требований законодательства;<br>- состав, назначение и содержание организационно-распорядительных документов в области информационной безопасности;<br>- система нормативно-методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации;<br>- система нормативно-методических документов Федеральной службы безопасности Российской Федерации; | | 2 | | | |
| 1.2 | Выявление угроз безопасности информации в информационных системах, основные организационные меры, технические и программные средства защиты информации, в том числе:<br>- основные организационные меры обеспечения информационной безопасности;<br>- технические средства обеспечения информационной безопасности, их классификация и назначение;<br>- идентификация, аутентификация, разграничение доступа, мониторинг и аудит;<br>- обеспечение информационной безопасности при работе с интернет-ресурсами;<br>- обеспечение информационной безопасности при использовании электронной почты;<br>- использование антивирусных средств; | | | 4 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | - использование средств резервного копирования;<br>- криптографические методы и средства защиты информации;<br>парольная политика;<br>- необходимость и механизмы установки обновлений (как операционной системы, так и средств защиты информации). | | | | | |
| 1.3 | Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных | | | 2 | | |
| 1.4 | Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных | | | 1 | | |
| 1.5 | Практические реализации типовых моделей защищенных информационных систем обработки персональных данных | | | 1 | | |
| **2.** | **Организационно-правовые основы обеспечения безопасности персональных данных** | **4** | **2** | **2** | | |
| 2.1 | Правовые и нормативные акты в сфере обработки и защиты персональных данных | | | | | |
| 2.2 | Основные понятия Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» | | | | | |
| 2.3 | Принципы и основания обработки персональных данных | | | | | |
| 2.4 | Персональные данные, разрешенные субъектом персональных данных для распространения | | | | | |
| 2.5 | Согласие субъекта на обработку его персональных данных | | | | | |
| 2.6 | Категории персональных данных (специальные биометрические, общедоступные, иные) | | | | | |
| 2.7 | Права субъектов персональных данных | | | | | |
| 2.8 | Обязанности оператора персональных данных | | | | | |
| 2.9 | Лицо, ответственное за организацию обработки персональных данных | | | | | |
| 2.10 | Уведомление об обработке персональных данных | | | | | |
| 2.11 | Уполномоченный орган по защите прав субъектов персональных данных – Роскомнадзор | | | | | |
| 2.12 | Федеральный государственный контроль (надзор) за обработкой персональных | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | данных | | | | | |
| 2.13 | Особенности обработки персональных данных, осуществляемой без использования средств автоматизации | | | | | |
| **8.** | **Итоговая аттестация** | **2** | | | | **Итоговое тестирование** |
| | Всего часов | **16** | **4** | **10** | | |