МИНОБРНАУКИ РОССИИ

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

УТВЕРЖДАЮ
Первый проректор
(по цифровой трансформации и
стратегическому развитию)
_____ М.В. Чистяков
(подпись)
«17» сентября 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

программа повышения квалификации

«Обеспечение безопасности персональных данных»

для лиц, имеющих высшее и/или среднее профессиональное образование

Программа разработана для руководителей организаций; руководителей и специалистов служб (отделов), специалистов-практиков, работающих в службах, ответственных за организацию обработки и защиту персональных данных в организации или исполняющих обязанности лиц, ответственных за организацию обработки и защиту персональных данных,

с учетом требований профессионального стандарта Специалист по защите информации в автоматизированных системах (Приказ Минтруда России от 14.09.2022 № 525н)

72 академических часа

Форма обучения: заочная, с использованием электронного обучения и дистанционных образовательных технологий

Ярославль 2024

АННОТАЦИЯ

Дополнительная профессиональная программа повышения квалификации «Обеспечение безопасности 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 информатизации.

Программа предназначена для руководителей организаций любых организационно-правовых форм и форм собственности; руководителей и специалистов служб (отделов) организаций, специалистов-практиков, работающих в службах ответственных за организацию обработки и защиту персональных данных в организации или исполняющих обязанности лиц, ответственных за организацию обработки и защиту персональных данных.

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 № 525н от 14 сентября 2022 г.).

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 информатизации;

полномочия и зоны ответственности регуляторов в сфере обеспечения безопасности персональных данных;

основы обеспечения безопасности операционных систем;

основы информационной безопасности в локальных вычислительных сетях;

будет уметь:

планировать мероприятия по обеспечению безопасности персональных данных;

выявлять процессы, связанные с обработкой персональных данных и устанавливать границы информационных систем;

определять уровень защищенности персональных данных;

проводить базовую установку и настройку средств защиты от несанкционированного доступа;

проводить базовую установку и настройку средств антивирусной защиты информации;

проводить базовую установку и настройку средств анализа защищенности.

Требования к слушателям

Высшее или среднее профессиональное образование.

Объем программы 72 акад.часа.

Срок реализации программы: 6 недель**,** в соответствии с календарным графиком.

Форма обучения: заочная, с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ).

Особенности программы:

Программа реализуется с применением ЭО и ДОТ, на платформе DemidOnline.

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) «Обеспечение безопасности персональных данных» устанавливает требования к результатам обучения, определяет содержание и виды учебных занятий и контроля результатов обучающихся.

ДПП ПК реализуется с применением электронного обучения и дистанционных образовательных технологий. Используемый при реализации онлайн-курс «Обеспечение безопасности персональных данных» содержит учебные и контрольно-измерительные материалы, необходимые для осуществления мероприятий текущего, промежуточного и итогового контроля и достижения всех запланированных результатов обучения.

2. Цели и результаты освоения программы

Дополнительная профессиональная программа повышения квалификации «Обеспечение безопасности персональных данных» направлена на формирование и развитие профессиональных компетенций, необходимых для организации и осуществления деятельности по обработке и защите персональных данных в организациях любых организационно-правовых форм и форм собственности.

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 14.09.2022 № 525н).

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	B/07.6 Установка и настройка средств защиты информации в автоматизированных системах
	B/08.6 Разработка организационно-распорядительных документов по защите информации в автоматизированных системах
	B/10.6 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 информатизации;
- полномочия и зоны ответственности регуляторов в сфере обеспечения безопасности персональных данных;

- основы обеспечения безопасности операционных систем;
- основы информационной безопасности в локальных вычислительных сетях;

будет уметь:

- планировать мероприятия по обеспечению безопасности персональных данных;
- выявлять процессы, связанные с обработкой персональных данных и устанавливать границы информационных систем;
- определять уровень защищенности персональных данных;
- проводить базовую установку и настройку средств защиты от несанкционированного доступа;
- проводить базовую установку и настройку средств антивирусной защиты информации;
- проводить базовую установку и настройку средств анализа защищенности.

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. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. 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».
7. «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 72 акад. часа, с учетом всех видов учебной нагрузки. Срок реализации программы: 6 недель, в соответствии с календарным учебным графиком.

5. Форма обучения и форма реализации программы

Форма обучения – заочная, с применением электронного обучения и дистанционных образовательных технологий.

6. Учебный план

«Обеспечение безопасности персональных данных» 72 акад. часа.

№	Наименование тем, разделов	Всего акад. часов	В том числе			
			Лекции	Практические работы, лабораторные, семинарские занятия	СР	Форма контроля результатов освоения
0.1	Архитектура компьютера (необходимо для получения базового представления, может быть пропущено, не влияет на аттестацию)					
0.2	Введение в криптографические методы защиты информации (необходимо для получения базового представления, может быть пропущено, не влияет на аттестацию)					
1.	Общие вопросы технической защиты информации: понятия и принципы	4	2		2	Тест
2.	Организационно-правовые основы обеспечения безопасности персональных данных	14	8		6	Тест
3.	Организация и обеспечение защиты информации в Российской Федерации	10	6		4	Тест
4.	Основы информационной безопасности в операционных системах	12	3	6	3	Тесты
5.	Основы информационной безопасности в локальных вычислительных сетях	12	3	6	3	Тесты
6.	Основы администрирования средств защиты информации	12		8	4	Тесты
7.	Организация и обеспечение безопасности персональных данных с использованием шифровальных (криптографических) средств	6	4		2	Тест
8.	Итоговая аттестация	2			2	Итоговое тестирование
	Всего часов	72	26	20	26	

7. Календарный учебный график

Планируемый срок освоения учебного материала – 6 недель (без отрыва от работы, 12 часов в неделю).

№ п/п	Тема	Учебная неделя					
		1	2	3	4	5	6
1.	Общие вопросы технической защиты информации: понятия и принципы						
2.	Организационно-правовые основы обеспечения безопасности персональных данных						
3.	Организация и обеспечение защиты информации в Российской Федерации						
4.	Основы информационной безопасности в операционных системах						
5.	Основы информационной безопасности в локальных вычислительных сетях						
6.	Основы администрирования средств защиты информации						
7	Организация и обеспечение безопасности персональных данных с использованием шифровальных (криптографических) средств						
8.	Итоговая аттестация						Тестовое задание

Календарный учебный график представлен в онлайн-курсе «Обеспечение безопасности персональных данных» на платформе DemidOnline.

8. Оценка качества освоения программы

Оценка качества освоения программы производится с использованием контрольно-измерительных материалов, представленных в онлайн-курсе «Обеспечение безопасности персональных данных»: тестовые задания.

Программа считается освоенной, а результаты обучения достигнутыми, если количество правильных ответов на вопросы итогового теста составляет не менее 65%.

9. Рекомендуемые источники и литература

Основная литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. 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».
7. 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».
8. «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.

Дополнительная литература

9. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
10. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
11. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).

Программное обеспечение и Интернет-ресурсы

https://www.consultant.ru/ – компьютерная справочная правовая система в России, содержит свыше 102 миллионов документов.

https://garant.ru – справочно-правовая система по законодательству Российской Федерации.

https://fstec.ru/dokumenty-filter – содержит нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации.

https://bdu.fstec.ru/ – банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

https://pd.rkn.gov.ru/ – портал персональных данных Роскомнадзора.

https://rkn.gov.ru/ – сайт Роскомнадзора.

https://fstec.ru/ – сайт Федеральной службы технического и экспортного контроля Российской Федерации.

https://fsb.ru/ – сайт Федеральной службы технического и экспортного контроля Российской Федерации.

Материально-технические условия организации обучения:

Каждый слушатель должен иметь персональный компьютер (мобильный телефон) с доступом в Интернет. А также авторизованный доступ к образовательной платформе DemidOnline.

10. Авторы программы:

№ п/п	ФИО	Ученая степень и ученое звание	Основное место работы, должность
1.	Мурин Дмитрий Михайлович	Канд. физ.-мат. наук	Ярославский государственный университет им. П.Г.Демидова, директор Института информационной безопасности