

Государственное автономное учреждение дополнительного образования  
«Центр опережающей профессиональной подготовки  
Республики Башкортостан»

УТВЕРЖДАЮ  
Директор государственного  
автономного учреждения  
дополнительного  
профессионального образования  
«Центр опережающей  
профессиональной подготовки  
Республики Башкортостан»

К.В. Галымова

Дополнительная профессиональная программа  
повышения квалификации

## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Направление «По компетенциям будущего, включая компетенции цифровой  
экономики»

г. Уфа, 2021

# **1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

## **Актуальность программы для заказчика**

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

### **1.1. Цель реализации программы**

Целью программы повышения квалификации является формирование и совершенствование профессиональных компетенций педагогов и иных должностных лиц в образовательной организации и обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

### **1.2. Планируемые результаты обучения.**

В результате освоения программы слушатель должен 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 определению и оценке угроз безопасности 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;

**уметь:**

- создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;
- планировать мероприятия по обеспечению безопасности персональных данных;
- проводить оценку 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;

**владеть:**

- навыками работы с правовыми базами данных;
- навыками определения уровней защищённости персональных данных;
- навыками определения и оценки угроз безопасности персональных данных в информационных системах персональных данных;
- навыками разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации;
- навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;
- навыками применения сертифицированных средств защиты информации.

### **1.3. Категория слушателей**

Лица, имеющие среднее профессиональное образование, имеющие/ получающие высшее образование.

#### **1.4. Нормативно-правовые основания разработки программы:**

- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ;
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

#### **1.5. Трудоемкость программы**

Нормативная трудоемкость обучения по данной программе – 36 часов, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

#### **1.6. Форма обучения**

Программа реализуется в очной форме с применением электронного обучения и дистанционных образовательных технологий.

**1.7. Форма итоговой аттестации:** итоговая аттестация в форме компьютерного тестирования.

При условии выполнения учебного плана и успешной итоговой аттестации слушатель получает удостоверение о повышении квалификации.

## 2. СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. Учебный план

№ п/п	Наименование модуля и тем	Всего, часов	Форма занятий				Форма контроля
			аудиторные	Практические занятия, час	Самостоятельная работа, час	дистанционные	
1.	<b>Информационные угрозы и их виды</b>	4				3	1
1.1	Основные понятия информационной безопасности	2				2	
1.2	Актуальность проблемы защиты персональных данных в информационных системах	2				1	1
2.	<b>Нормативно-правовое обеспечение защиты персональных данных</b>	12				7	2
2.1.	Международное и национальное право в области защиты персональных данных	2				2	
2.2.	Федеральное законодательство Российской Федерации в области защиты персональных данных	3				2	Тестирование 1
2.3.	Содержание и основные положения Федерального закона Российской Федерации № 152 ФЗ «О персональных данных»	5				2	Тестирование 1
2.4.	Специальные нормативные документы по технической защите сведений конфиденциального характера	2				1	Тестирование 1
3.	<b>Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах</b>	4				3	1
3.1.	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах	2				2	
3.2.	Наиболее часто реализуемые угрозы	2				1	Тестирование 1
4.	<b>Организационные и технические мероприятия по защите персональных данных в информационных системах</b>	14				9	4
4.1.	Порядок организации защиты персональных данных	2				2	
4.2.	Меры по обеспечению безопасности персональных данных	2				2	
4.3.	Построение системы защиты персональных данных	6				2	4
4.4.	Аттестация, сертификация и лицензирование в области защиты персональных данных	2				1	Тестирование 1
4.5.	Контроль в области защиты персональных данных	2				2	
5.	<b>Итоговая аттестация</b>	2					Тестирование 2
<b>ВСЕГО:</b>		<b>36</b>				<b>22</b>	<b>7</b>

## Примерный календарный учебный график

<b>Период обучения (дни, недели)<sup>1)</sup></b>	<b>Наименование модуля</b>
1 день	Основные понятия информационной безопасности Актуальность проблемы защиты персональных данных в информационных системах
2 день	Международное и национальное право в области защиты персональных данных Федеральное законодательство Российской Федерации в области защиты персональных данных Промежуточная аттестация
3 день	Содержание и основные положения Федерального закона Российской Федерации № 152 ФЗ «О персональных данных» Промежуточная аттестация
4 день	Специальные нормативные документы по технической защите сведений конфиденциального характера Промежуточная аттестация
5 день	Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах Наиболее часто реализуемые угрозы Промежуточная аттестация
6 день	Порядок организации защиты персональных данных Меры по обеспечению безопасности персональных данных
7 день	Построение системы защиты персональных данных
8 день	Аттестация, сертификация и лицензирование в области защиты персональных данных Промежуточная аттестация Контроль в области защиты персональных данных
9 день	<i>Итоговая аттестация</i>

<sup>1)</sup>Даты обучения будут определены в расписании занятий при наборе группы на обучение

### 2.3. Рабочие программы разделов

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Форма контроля и (или) реализации	Объем часов
<b>Модуль 1. Информационные угрозы и их виды</b>			<b>4</b>
<b>Тема 1.1 Основные понятия информационной безопасности</b>	<b>Содержание материала</b>		
	1. Теоретические аспекты информационной безопасности		2
	2. Подходы, принципы, методы и средства обеспечения безопасности		
	3. Федеральный закон «Об информации, информационных технологиях и о защите информации»		
<b>Тема 1.2 Актуальность проблемы защиты персональных данных в информационных системах</b>	<b>Содержание материала</b>		
	1. Обеспечение защиты персональных данных как элемент информационной безопасности		1
	2. Цифровизация субъекта персональных данных		
	<b>Практическая работа</b>		
	1. Проведение тестирования респондентов по вопросам защиты персональных данных		
<b>Модуль 2. Нормативно-правовое обеспечение защиты персональных данных</b>			<b>9</b>
<b>Тема 2.1. Международное и национальное право в области защиты персональных данных</b>	<b>Содержание материала</b>		
	1. Конвенция «О защите физических лиц при автоматизированной обработке персональных данных»		2
	2. Директива о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных		
	3. Директива в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи		
	4. Дополнительный протокол о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации		
<b>Тема 2.2. Федеральное законодательство Российской Федерации в области защиты персональных данных</b>	<b>Содержание материала</b>		
	1. Требования к защите персональных данных при их обработке в информационных системах персональных данных		1
	2. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации		
	3. Требования к материальным носителям биометрических персональных данных		
<b>Тема 2.3. Содержание и основные положения Федерального закона</b>	<b>Содержание материала</b>		
	1. Общие положения закона		2
	2. Принципы и условия обработки персональных данных		1

Российской Федерации № 152 ФЗ «О персональных данных»	3.	Категории персональных данных		
	4.	Права субъекта персональных данных		
	5.	Обязанности оператора персональных данных		
	<b>Практические занятия</b>			
	1.	Разработка соглашения субъекта персональных данных на обработку его персональных данных	2	
<b>Тема 2.4. Специальные нормативные документы по технической защите сведений конфиденциального характера</b>				
<b>Модуль 3. Угрозы и уязвимости персональных данных при их обработке в информационных системах</b>				
<b>Тема 3.1. Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах</b>				
Содержание материала				
1. Основные принципы моделирования угроз с использованием методических документов ФСТЭК и ФСБ				
2. Угрозы информационной безопасности				
3. Общая характеристика уязвимостей информационной системы персональных данных				
<b>Тема 3.2. Наиболее часто реализуемые угрозы</b>				
Содержание материала				
1. Угрозы утечки информации по техническим каналам				
2. Угрозы несанкционированного доступа к информации в информационной системе персональных данных				
<b>Модуль 4. Организационные и технические мероприятия по защите персональных данных в информационных системах</b>				
<b>Тема 4.1. Порядок организации защиты персональных данных</b>				
Содержание материала				
1. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных				
2. Оценка обстановки и формирование замысла защиты персональных данных				
3. Организационно распорядительная документация по защите персональных данных				
<b>Тема 4.2. Меры по обеспечению безопасности персональных данных</b>				
Содержание материала				
1. Состав и содержание мер по обеспечению безопасности персональных данных				
2. Порядок выбора мер по обеспечению безопасности персональных данных				

Тема 4.3. Построение системы защиты персональных данных	<b>Содержание материала</b>	2
	1. Основные этапы при построении системы защиты персональных данных 2. Комплекс организационных и технических мероприятий в рамках СЗПДн 3. Уведомление Роскомнадзора об обработке персональных данных	
Тема 4.4. Аттестация, сертификация и лицензирование в области защиты персональных данных	<b>Практические занятия</b>	4
	1. Разработка уведомления о внесении в Реестр Роскомнадзора 2. Разработка заявления о прекращении оператором обработки ПДн	
Тема 4.5. Контроль в области защиты персональных данных	<b>Содержание материала</b>	1
	1. Сертификация средств защиты персональных данных 2. Аттестации ИСЛДн по требованиям безопасности информации 3. Лицензирование деятельности по защите персональных данных	
<b>Итоговая аттестация</b>	<b>Содержание материала</b>	2
	Всего: 36 ч.	
<b>Тестирование</b>		1

## **2.4 Оценка качества освоения программы**

За правильный ответ слушатель получает 1 балл, за неправильный ответ – 0 баллов. Слушатель получает «зачет» за выполнение тестов, если количество правильных ответов составляет 60-100 %. «Незачет» – 59% баллов или менее. При выставлении оценки по 4-балльной системешкала перевода выглядит следующим образом:

- 59% и менее – неудовлетворительно;
- от 60% до 69% – удовлетворительно;
- от 70% до 84% – хорошо;
- от 85% до 100% – отлично.

### **2.4.1 Контрольные измерительные материалы**

#### **Перечень вопросов к промежуточной аттестации по Модулю 2, тема 2.2.**

1. Для какого типа информационной системы персональных данных НЕ подходит уровень защищённости 1-го уровня?
2. Как сокращённо обозначается информационная система, в которой 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, не обрабатываются сведения, относящиеся к специальным категориям персональных данных?
3. Как сокращённо обозначается информационная система, в которой обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных?
4. Как сокращённо обозначается информационная система, в которой обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных?
5. Какой документ находится выше остальных в иерархии документов, регламентирующих вопросы защиты персональных данных при их автоматизированной обработке в информационных системах?
6. Какой тип угрозы, если для информационной системы актуальны угрозы, не связанные с наличием не декларированных возможностей в системном и прикладном программном обеспечении, используемом в информационной системе?
7. Кем производится определение типа угроз безопасности персональных данных, актуальных для информационной системы?
8. С какой частотой производится контроль за выполнением требований уровня защищённости?
9. Сколько устанавливается уровней защищённости персональных данных?
10. Персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, каждого субъекта персональных данных могут заноситься в журнал (книгу, реестр) не более ... раз(а) в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор?

#### **Перечень вопросов к промежуточной аттестации по Модулю 2, тема 2.3.**

1. Какой из регуляторов, описанных в законе «О персональных данных», отвечает за защиту прав субъектов персональных данных?
2. Как называются действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц?
3. Какой из регуляторов, описанных в законе «О персональных данных», отвечает за требования по защите информации от несанкционированного доступа и утечки по техническим каналам?
4. Какой из регуляторов, описанных в законе «О персональных данных», отвечает за требования в области криптографии?
5. Какие называются сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность?
6. Какую информацию не может запросить субъект ПДн при обращении?
7. В каких случаях оператор обязан уведомлять Роскомнадзор об обработке ПДн?

8. В соответствии с какой статьёй Федерального закона №152 оператор Персональных данных до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) о своем намерении осуществлять обработку персональных данных?
9. Какая статья Уголовного кодекса говорит о наказании за причинение крупного ущерба гражданам в случае осуществления защиты персональных данных без лицензии в случаях?
10. Какими статьями Федерального закона №152 устанавливаются особенности обработки специальных категорий персональных данных, а также биометрических персональных данных?

**Перечень вопросов к промежуточной аттестации по Модулю 2, тема 2.4.**

1. Какое количество уровней защиты от несанкционированного доступа определено нормативными документами ФСБ России?
2. В каком документе изложены специальные требования и рекомендации по защите конфиденциальной информации?
3. На какой стадии создания системы защиты персональных данных (СЗПДн) производится определение (уточнение) угроз безопасности ПДн, конкретных условий функционирования (разработка частной модели угроз)?
4. На какой стадии создания системы защиты персональных данных (СЗПДн) производится определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения безопасности ПДн?
5. На какой стадии создания системы защиты персональных данных (СЗПДн) производится опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн?
6. Кем были выпущены и утверждены Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации?
7. Какое количество криптографических уровней защиты персональных данных различают?
8. В каком документе описаны криптографические уровни и уровни защиты от несанкционированного доступа?
9. На кого возлагается текущий контроль за организацией и обеспечением функционирования криптосредств?
10. В каких случаях не обязана производиться модернизация СЗПДн?

**Перечень вопросов к промежуточной аттестации по Модулю 3, тема 3.2.**

1. Что называется средой распространения информативного сигнала?
2. Чем обуславливается возникновение угроз утечки акустической информации обуславливается?
3. Что является носителем ПДн?
4. Чем может вестись перехват акустической информации?
5. К какому виду информации относятся угрозы угрозы, которые реализуются за счет просмотра ПДн с помощью оптических средств с экранов мониторов и других средств отображения средств вычислительной техники, входящих в состав ИСПДн?
6. Что является необходимым условием осуществления просмотра ПДн?
7. Каким угрозам подвергается ИСПДн, когда она представляет собой распределенную информационную систему, подключенную к сетям общего пользования и (или) сетям международного информационного обмена?
8. С помощью какой программы производится анализ сетевого трафика, угрозы, направленной на получение пароля и идентификатора пользователя?
9. Что является доверенным объектом?
10. Что является основным видом вредоносных программ?

**Перечень вопросов к промежуточной аттестации по Модулю 4, тема 4.4.**

1. Какие документы должен отправить соискатель в ФСТЭК?
2. При каких условиях орган по аттестации принимает решение об отказе в выдаче «Аттестата соответствия»?
3. Кто не является участником процесса сертификации?
4. В каких случаях аттестация является обязательной?

5. Что не входит в порядок проведения аттестации ИСПДн по требованиям безопасности?
6. Кто осуществляет аккредитацию предприятий?
7. Как называется деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного им формационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования?
8. Выполнение комплекса работ по защите персональных данных для собственных нужд подлежит лицензированию?
9. Для чего предназначение аттестация ИСПДн?
10. Аттестационные испытания предполагают проверку ИСПДн на целостность ПДн в ИСПДн?

**Перечень вопросов к итоговой аттестации.**

1. На какой стадии создания системы защиты персональных данных (СЗПДн) производится опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн?
2. Как сокращённо обозначается информационная система, в которой обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных?
3. Что относится к источникам угроз утечки информации по техническим каналам?
4. Что называется средой распространения информативного сигнала?
5. Какое количество криптографических уровней защиты персональных данных различают?
6. Относится ли к полномочиям Минцифры обеспечение безопасности персональных данных при их обработке в информационных системах с помощью криптосредств?
7. Является необходимым условием осуществления просмотра ПДн наличие непосредственного носителя ПДн?
8. Какой из регуляторов описывается в законе «О персональных данных»?
9. Является доверенный объектом элемент сети, передающий информацию хосту нарушителя сети?
10. Что из этого перечня является основным видом вредоносных программ: программные закладки, классические программные (компьютерные) вирусы, вредоносные программы, распространяющиеся по сети (сетевые черви)?

### 3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

#### 3.1. Требования к минимальному материально-техническому обеспечению:

- учебные аудитории для проведения учебных занятий;
- магнитно-маркерная доска (либо интерактивная доска);
- рабочее место преподавателя, оборудованное ноутбуком с выходом в интернет;
- рабочие места обучающихся – не менее 25;

Технические средства обучения:

- персональные компьютеры с выходом в интернет;
- мультимедийное оборудование.

#### 3.2. Условия для функционирования электронной информационно-образовательной среды

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения
Сайт Moodle ГЛУ ДПО Центр опережающей профессиональной	лекция, тестирование	1. Компьютер с выходом в интернет <a href="http://copp-rb.ru/diststudy">http://copp-rb.ru/diststudy</a>

подготовки Республики Башкортостан		2. Необходимый комплект лицензионного и свободно распространяемого программного обеспечения
---------------------------------------	--	--

### **3.3. Учебно-методическое и информационное обеспечение**

#### **3.3.1. Методическое обеспечение программы**

- учебная, методическая, справочная литература;
- материалы для промежуточного контроля (тестовые вопросы);
- комплект учебно-наглядных пособий.

#### **3.3.2. Информационные ресурсы:**

- Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>

#### **3.3.3. Список рекомендованной литературы**

1. Воробьев, Е. Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных: учебное пособие / Е. Г. Воробьев. — 3-е изд., перераб. — Санкт-Петербург: Интермедиа, 2017. — 432 с. — ISBN 978-5-4383-0120-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/161356>
2. Корнилова, А. А. Защита персональных данных: учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. — Уфа: БашГУ, 2020. — 120 с. — ISBN 978-5-7477-5228-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/179914>
3. Персональные данные в государственных информационных ресурсах / М. Ю. Брауде-Золотарёв, Е. С. Сербина, В. С. Негородов, И. Г. Волошкин. — Москва : Дело РАНХиГС, 2016. — 56 с. — ISBN 978-5-7749-1121-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/74913>
4. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/183744>
5. Скрипник, Д. А. Обеспечение безопасности персональных данных: учебное пособие / Д. А. Скрипник. — 2-е изд. — Москва: ИНТУИТ, 2016. — 121 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/100272>

### **3.4. Кадровое обеспечение образовательного процесса**

Кадровое обеспечение программы осуществляется преподавательский состав согласно ЕКТС.

#### **Разработчики:**

Храмов Е.А., преподаватель ГАУ ДПО ЦОПП РБ,  
Капитанова А.М., методист ГАУ ДПО ЦОПП РБ.