Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

ПРИКАЗ

23.05.2024 № 192

Нижний Новгород

Об утверждении Политики в отношении обработки персональных данных

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных», а также прочих нормативных документов по защите информации, приказываю:

1. Утвердить прилагаемую Политику в отношении обработки персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее - Политика).
2. Обеспечить неограниченный доступ к Политике.
3. Заведующему отделом информационных технологий Калашникову Л. Б. в срок не позднее десяти рабочих дней от даты подписания настоящего приказа опубликовать Политику на официальном сайте Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук».
4. Руководителям структурных подразделений ознакомить с настоящим приказом и Политикой работников подразделений.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
академик РАН Г.Г. Денисов

Приложение № 1 к приказу
от «23» 05 2024 г. № 192

ПОЛИТИКА
в отношении обработки персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (ИПФ РАН)

Нижний Новгород
2024

1. Основные термины и определения

1.1 **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

1.2 **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.3 **Доступ к информации** – возможность получения информации и ее использования.

1.4 **Законодательство о персональных данных** – Конституция Российской Федерации, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и иные нормативные правовые акты, регулирующие отношения, связанные с обработкой персональных данных.

1.5 **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.6 **Информационно-телекоммуникационная сеть** – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

1.7 **Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.8 **Информация** – сведения (сообщения, данные) независимо от формы их представления.

1.9 **Использование персональных данных** – действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающие права и свободы субъекта персональных данных или других лиц.

1.10 **Конфиденциальность персональных данных** – обязательное для соблюдения должностным лицом Оператора, иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.11 **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

1.13 **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.14 **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

1.15 **Персональные данные, разрешенные субъектом персональных данных для распространения** – персональные данные, доступ неограниченного круга лиц к которым

предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом.

1.16 **Политика информационной безопасности** – система взглядов на информационную безопасность, совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

1.17 **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.18 **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.19 **Субъекты персональных данных** – определенные или определяемые (поддающиеся определению) физические лица.

1.20 **Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.21 **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

2.1 Политика в отношении обработки персональных данных (далее - Политика) в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее – Оператор) является официальным документом, в котором определены общие принципы, цели и порядок обработки персональных данных, а также сведения о реализуемых мерах защиты персональных данных.

2.2 Политика распространяется на всех сотрудников Оператора, включая сотрудников, работающих по договору подряда, а также на сотрудников сторонних организаций, взаимодействующих с Оператором на основании соответствующих нормативных, правовых, организационно-распорядительных и иных документов.

2.3 Политика вступает в силу с момента ее утверждения и действует бессрочно, до замены ее новой Политикой.

3. Правовые основания обработки персональных данных

3.1 Оператор обрабатывает персональные данные в соответствии со следующими нормативными и правовыми актами:

- Конституцией Российской Федерации.
- Гражданским кодексом Российской Федерации.
- Трудовым кодексом Российской Федерации.
- Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Иными нормативными и правовыми актами Российской Федерации.

4. Принципы обработки персональных данных

4.1 Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.2 Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.3 Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.4 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.5 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.6 При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

4.7 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных работников ИПФ РАН (в том числе справочники, электронные базы). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год рождения, сведения о профессии и иные персональные данные, предоставленные работником.

4.8 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Цели обработки персональных данных

Обработка персональных данных осуществляется в целях соблюдения Конституции Российской Федерации, федеральных законов, иных нормативных правовых актов Российской Федерации.

Оператор обрабатывает персональные данные исключительно в следующих целях:

- Ведение кадрового и бухгалтерского учета;
- Обеспечение соблюдения трудового законодательства РФ;
- Обеспечение соблюдения налогового законодательства РФ;
- Обеспечение соблюдения пенсионного законодательства РФ;
- Обеспечение соблюдения законодательства РФ в сфере образования;
- Обеспечение соблюдения законодательства о противодействии коррупции;
- Подготовка, заключение и исполнение гражданско-правового договора;
- Осуществление научной, литературной или иной творческой деятельности;
- Обеспечение пропускного режима на территорию Оператора;
- Подбор персонала (соискателей) на вакантные должности Оператора;
- Обеспечение прохождения ознакомительной, производственной или преддипломной практики на основании договора с учебным заведением;

– Обеспечение соблюдения законодательства РФ в сфере здравоохранения;
– Обеспечение соблюдения законодательства РФ об обороне;
– Обеспечение соблюдения жилищного законодательства РФ;
– Исполнение требований статьи 6-ой пункта 2 части 1 ФЗ №152 "О персональных данных" (Обработка и передача персональных данных сотрудников в системе ЕГИСУ НИОКТР и ИАС Мониторинг).

1.1 Категории субъектов, персональные данные которых обрабатываются:

– Работники;
– Соискатели;
– Родственники работников;
– Уволенные работники;
– Контрагенты;
– Учащиеся;
– Студенты;
– Аспиранты;
– Арендаторы;
– Посетители;
– Пользователи официального сайта и личного кабинета ИПФ РАН;
– Участники интерактивного мероприятия (выборы, голосование, конференции);
– Иные физические лица.

1.2 Категории и перечень обрабатываемых персональных данных

В зависимости от задач и функций, возложенных на структурные подразделения, осуществляется обработка следующих персональных данных:

– Фамилия, имя, отчество;
– Год рождения;
– Месяц рождения;
– Дата рождения;
– Место рождения;
– Семейное положение;
– Социальное положение;
– Имущественное положение;
– Доходы;
– Пол;
– Адрес электронной почты;
– Адрес места жительства;
– Адрес регистрации;
– Номер телефона;
– СНИЛС;
– ИНН;
– Гражданство;
– Данные документа, удостоверяющего личность;
– Данные водительского удостоверения;
– Данные документа, удостоверяющего личность за пределами российской федерации;
– Данные документа, содержащиеся в свидетельстве о рождении;
– Реквизиты банковской карты;

– Номер расчетного счета;
– Номер лицевого счета;
– Профессия;
– Должность;
– Сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
– Отношение к воинской обязанности, сведения о воинском учете;
– Сведения об образовании;
– Иные персональные данные.

Специальные персональные данные:
– Национальная принадлежность;
– Сведения о судимости;
– Сведения о состоянии здоровья;
– Сведения о наличии инвалидности.

Иные персональные данные:
– Сведения, содержащиеся в свидетельствах о государственной регистрации актов гражданского состояния (рождение, заключение брака, расторжение брака, усыновление (удочерение), установление отцовства, перемена имени, смерть)
– Данные о родственниках (фамилия, имя, отчество, степень родства, дата рождения, иждивенцы)
– Сведения о месте работы и/или учебы членов семьи и родственников;
– Сведения о дисциплинарных взысканиях;
– Сведения о законных представителях;
– Сведения о знании иностранного языка;
– Сведения о наградах/поощрениях;
– Сведения о социальных льготах;
– Данные о командировках;
– Сведения о пребывании за границей;
– Коды категорий налогоплательщика;
– Сведения об аттестации;
– Сведения о повышении квалификации или наличии специальных знаний;
– Сведения о форме и дате оформления допуска к государственной тайне, ранее имевшегося и (или) имеющегося.

1.3 Информация о персональных данных может содержаться:
– На бумажных носителях;
– На электронных носителях;
– В информационно-телекоммуникационных сетях и иных информационных системах.

6. Условия и сроки прекращения обработки персональных данных

6.1 Оператор прекращает обработку персональных данных при наступлении одного из следующих условий:
– достижение целей обработки персональных данных или максимальных сроков хранения - в течение 30 дней;

– утрата необходимости в достижении целей обработки персональных данных - в течение 30 дней;

– предоставление субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки - в течение 7 дней;

– невозможность обеспечения правомерности обработки персональных данных - в течение 10 дней;

– отзыв субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных - в течение 30 дней;

– истечение сроков исковой давности для правоотношений, в рамках которых осуществляется либо осуществлялась обработка персональных данных.

7. Меры обеспечения безопасности персональных данных

7.1 Безопасность персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных.

7.2 Оператор предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.3 Оператор предпринимает следующие организационно-технические меры:

– назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

– ограничение и регламентация состава работников, имеющих доступ к персональным данным;

– ознакомление работников с требованиями федерального законодательства и локальных нормативных документов по обработке и защите персональных данных;

– обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;

– определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;

– разработка на основе модели угроз системы защиты персональных данных для соответствующего класса информационных систем;

– проверка готовности и эффективности использования средств защиты информации;

– реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

– регистрация и учёт действий пользователей информационных систем персональных данных;

– парольная защита доступа пользователей к информационной системе персональных данных;

– применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;

– применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на съемных машинных носителях информации;

– осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;

– применение в необходимых случаях средств межсетевого экранирования;

– применение в необходимых случаях средств обнаружения вторжений в корпоративную сеть, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– применение в необходимых случаях централизованного управления системой защиты персональных данных;

– резервное копирование информации;

– обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

– учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

– проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных;

– размещение технических средств обработки персональных данных, в пределах охраняемой территории;

– организация пропускного режима;

– поддержание технических средств охраны, сигнализации помещений в состоянии постоянной готовности.

8. Права субъектов персональных данных

8.1 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Оператором;

– правовые основания и цели обработки персональных данных;

– цели и применяемые Оператором способы обработки персональных данных;

– наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников/работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

8.2 Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.3 Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в вышестоящий орган по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - Роскомнадзор) или в судебном порядке.

8.4 Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

9. Уточнение, блокирование и уничтожение персональных данных

9.1 Уточнение персональных данных, в том числе их обновление и изменение, осуществляется с целью обеспечения достоверности, полноты и актуальности персональных данных.

Уточнение персональных данных осуществляется Оператором по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными. Об уточнении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя любым доступным способом.

9.2 Блокирование персональных данных осуществляется Оператором по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними. О блокировании персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя любым доступным способом.

В случае выявления неправомерной обработки персональных данных, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице,

уполномоченном Оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии)

9.3 Уничтожение персональных данных осуществляется:

– по достижении цели обработки персональных данных, Оператор обязан прекратить их обработку в срок, не превышающий 30 дней с даты, достижения цели обработки персональных данных;

– в случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, в срок, не превышающий 30 дней с даты, поступления указанного отзыва;

– в случае обращения субъекта персональных данных к Оператору с требованием о прекращении обработки персональных данных, в срок, не превышающий 10 рабочихдней с даты получения Оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

– в случае отсутствия возможности уничтожения персональных данных в течение указанных сроков, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование и обеспечивает уничтожение персональных данных в срокне более чем 6 месяцев.

В целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, Оператор вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных. О блокировании и (или) уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

10. Доступ к персональным данным

Доступ к персональным данным работников имеют следующие должностные лица, непосредственно использующие эти данные в рамках выполнения своих должностных обязанностей:

Персональные данные:

- Директор учреждения;
- Научный руководитель ИПФ РАН;
- Заместитель директора учреждения по научной работе;
- Заместитель директора учреждения по общим вопросам и экономике;
- Заместитель директора учреждения по режиму;
- Ученый секретарь учреждения;
- Помощник директора;
- Помощник директора по обеспечению информационной безопасности;
- Помощник директора по связям с общественностью;
- Главный инженер;
- Председатель профорганизации;
- Ведущий инженер по связям с общественностью;

– Специальное подразделение (заведующий отделом, ведущий инженер, специалист по технической защите информации, специалист по противодействию иностранным техническим разведкам)

– Главный экономист;

– Заместитель заведующего отделом (финансово-экономический отдел);

– Ведущий экономист (финансово-экономический сектор);

– Сектор труда и заработной платы (заведующий сектором, ведущий инженер по труду, ведущий экономист)

– Главный бухгалтер;

– Заместитель главного бухгалтера;

– Заместитель заведующего отделом;

– Сектор налогового учета, учета целевых средств и финансовых активов (заведующий сектором, ведущий бухгалтер, бухгалтер 1 категории);

– Сектор учета расчетов с рабочими и служащими (заведующий сектором, ведущий бухгалтер);

– Сектор земельных и имущественных отношений (заведующий сектором, ведущий инженер)

– Сектор организации научной работы и международных связей (заведующий сектором, ведущий инженер, инженер 2 категории;

– Отдел кадров (заведующий отделом, заместитель заведующего отделом, ведущий инженер);

– Служба безопасности (начальник отдела, заместитель начальника);

– Начальник бюро пропусков;

– Дежурный бюро пропусков;

– Инспектор (служба безопасности);

– Контролер контрольно-пропускного пункта;

– Отдел информационных технологий (заведующий отделом, заместитель заведующего отделом, ведущий электроник, ведущий программист);

– Заведующий сектором (сектор системного и технического обеспечения);

– Заведующий сектором (сектор прикладного программирования);

– Заведующий канцелярией;

– Делопроизводитель;

– Заведующий аспирантурой;

– Руководители отделений;

– Экономисты отделений;

– Сотрудники амбулатории.

Специальные персональные данные:

– Отдел кадров (заведующий отделом, заместитель заведующего отделом, ведущий инженер);

– Сектор земельных и имущественных отношений (заведующий сектором);

Иные персональные данные:

– Отдел кадров (заведующий отделом, заместитель заведующего отделом, ведущий инженер);

– Специальное подразделение (заведующий отделом, ведущий инженер, специалист по технической защите информации, специалист по противодействию иностранным техническим разведкам);

– Сектор земельных и имущественных отношений (заведующий сектором);

11. Условия обеспечения конфиденциальности информации

Должностные лица, имеющие в силу исполнения своих должностных обязанностей доступ к персональным данным, при их обработке должны обеспечивать конфиденциальность этих данных.

Обеспечение конфиденциальности сведений, содержащих персональные данные, осуществляется в соответствии с Политикой и иными локальными нормативными актами Оператора в части, касающейся обеспечения безопасности персональных данных.

Обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- для данных, включенных в справочники, адресные книги и т.п.

5.1. Ответственность за разглашение персональных данных.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Руководители структурных подразделений, в функции которых входит обработка персональных данных, несут персональную ответственность за нарушение порядка доступа работников данных структурных подразделений, и третьих лиц к информации, содержащей персональные данные.

Должностные лица, обрабатывающие персональные данные, несут персональную ответственность за:

- необеспечение конфиденциальности информации, содержащей персональные данные;
- неправомерный отказ субъекту персональных данных в предоставлении собранных в установленном порядке персональных данных либо предоставление неполной или заведомо ложной информации.

12. Защита персональных данных

Оператор при обработке персональных данных принимает необходимые организационные и технические меры, в том числе использует шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Защита персональных данных от неправомерного их использования или утраты обеспечивается за счёт средств Оператора в порядке, установленном законодательством Российской Федерации.

В случае выявления неправомерных действий с персональными данными Оператор обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

12.1 Внутренняя защита персональных данных

Персональные данные, содержащиеся на бумажных носителях, должны находиться в местах, обеспечивающих ограниченный доступ.

Персональные данные, содержащиеся на электронных носителях информации, хранятся в памяти персональных компьютеров Операторов. Доступ к указанным персональным компьютерам должен быть строго ограничен кругом лиц, ответственных за обработку персональных данных (уполномоченные работники Оператора персональных данных).

Информация на электронных носителях должна быть защищена паролем доступа, который подлежит смене не реже одного раза в шесть месяцев.

12.2 Внешняя защита персональных данных

– Помещения и территория охраняются, в том числе с помощью средств визуального наблюдения.

– Персональные данные в зависимости от способа их фиксации (бумажный носитель, электронный носитель) подлежат обработке таким образом, чтобы исключить возможность ознакомления с содержанием указанной информации сторонними лицами.

12.3 Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

– проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– анализ фактов несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных; составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.