Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики Российской академии наук»
(ИПФ РАН)

П Р И К А З

11.09.2020 г. № 146 а/х

Нижний Новгород

Об утверждении положения об обеспечении безопасности персональных данных

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

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемое Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – Положение).
2. Ответственному за организацию обработки персональных данных обеспечить выполнение требований Положения.
3. Требования прилагаемого Положения довести до работников, непосредственно осуществляющих защиту персональных данных.
4. Утвердить Инструкцию по организации парольной защиты в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 2).
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
член-корреспондент РАН Г.Г. Денисов

Приложение № 1 к приказу
от 11.09. 2020 г. № 146 а/х

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Нижний Новгород
2020

1. Основные термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

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.

Основные технические средства и системы - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.

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.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных**).**

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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 Настоящее Положение об обеспечении безопасности персональных данных (далее – Положение), обрабатываемых в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (далее – ИПФ РАН), разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных при их обработке в информационных системах.

2.2 Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ИПФ РАН.

2.3 Настоящее Положение вступает в силу с момента его утверждения директором Института и действует бессрочно, до замены его новым Положением.

2.4 Все изменения в Положение вносятся приказом директора ИПФ РАН.

2.5 Положение обязательно для исполнения всеми работниками ИПФ РАН, непосредственно осуществляющими защиту персональных данных.

3. Цели и задачи обеспечения безопасности персональных данных

3.1 Основной целью обеспечения безопасности персональных данных, при их обработке в информационной системе, является защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления,

распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2 Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности персональных данных при их обработке в информационной системе с помощью системы защиты информации, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

4. Основные принципы построения системы защиты информации

4.1 Система защиты информации основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости системы защиты;
- простоты применения средств защиты.

4.2 Принцип системности - предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

4.3 Принцип комплексности - предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

4.4 Принцип непрерывности защиты – это процесс обеспечения безопасности персональных данных, осуществляемый руководством, ответственным за организацию обработки персональных данных и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри организации, и каждый сотрудник должен принимать участие в этом процессе.

4.5 Принцип разумной достаточности - предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.6 Принцип гибкости системы защиты - система обеспечения безопасности персональных данных должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

4.7 Принцип простоты применения средств защиты - механизмы защиты должны быть интуитивно понятны и просты в применении. Применение средств защиты не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

5. Основные мероприятия по обеспечению безопасности персональных данных

5.1 Для обеспечения защиты персональных данных, обрабатываемых в информационной системе, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты персональных данных;
- определение актуальных угроз безопасности персональных данных;
- определение уровня защищенности персональных данных;
- реализация правил разграничения доступа и введение ограничений на действия пользователей;

- ограничение доступа пользователей в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку персональных данных;
- учет и хранение съемных машинных носителей персональных данных;
- организация резервирования и восстановления работоспособности программного обеспечения, баз данных персональных данных и средств защиты информации;
- организация парольной защиты;
- организация антивирусной защиты;
- организация обновления программного обеспечения и средств защиты информации;
- использование средств защиты информации;
- использование средств шифровальной (криптографической) защиты
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию системы защиты информации;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- аттестация информационной системы и ввод ее в действие;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

5.2 За вопросы обеспечения безопасности персональных данных, обрабатываемых в информационной системе, отвечают:

- Директор ИПФ РАН.
- Ответственный за организацию обработки персональных данных - работник, отвечающий за организацию и состояние процесса обработки персональных данных.
- Ответственный за защиту информации– работник, отвечающий за правильность использования и нормальное функционирование установленной системы защиты информации.
- Администратор информационных систем персональных данных – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки персональных данных.

5.3 Актуальные угрозы безопасности персональных данных, обрабатываемых в информационной системе, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности персональных данных и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

5.4 Для определения угроз безопасности персональных данных и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

5.5 Уровень защищенности персональных данных, обрабатываемых в информационной системе, определяется, в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и оформляется в виде "Акта об определения уровня защищенности персональных данных».

5.6 Реализация правил разграничения доступа, к персональным данным, обрабатываемым в информационной системе, осуществляется в соответствии с положением «О разрешительной системе доступа», утвержденным приказом директора ИПФ РАН.

5.7 Основные технические средства и системы информационной системы должны быть расположены в помещениях в пределах границ контролируемой зоны, определенных приказом «Об определении границ контролируемой зоны», утвержденным приказом директора ИПФ РАН.

5.8 Доступ работников в помещения, в которых ведется обработка персональных данных, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных», утвержденными приказом директора ИПФ РАН.

5.9 Работа со съемными машинными носителями персональных данных в информационной системе осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных», утвержденным приказом директора ИПФ РАН.

5.10 Организация резервирования и восстановления работоспособности программного обеспечения, баз данных персональных данных и средств защиты информации в информационной системе осуществляется в соответствии с «Инструкцией о порядке организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации», утвержденной приказом директора ИПФ РАН.

5.11 Организация парольной защиты в информационной системе осуществляется в соответствии с «Инструкцией по организации парольной защиты», утвержденной приказом директора ИПФ РАН.

5.12 Организация антивирусной защиты в информационной системе осуществляется в соответствии с «Инструкцией по организации антивирусной защиты», утвержденной приказом директора ИПФ РАН.

5.13 Организация обновления программного обеспечения и средств защиты информации в информационной системе осуществляется в соответствии с «Инструкцией по организации обновления программного обеспечения и средств защиты информации», утвержденной приказом директора ИПФ РАН.

5.14 Для обеспечения защиты персональных данных, обрабатываемых в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

5.15 Все средства защиты информации, эксплуатационная и техническая документация к ним, учитываются и заносятся ответственным за защиту информации в «Журнал учета средств защиты информации, эксплуатационной и технической документации к ним в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук» (Приложение 1).

5.16 Установка и настройка средств защиты информации в информационной системе персональных данных проводится в соответствии с эксплуатационной документацией на систему защиты персональных данных и документацией на средства защиты информации.

5.17 Для обеспечения защиты персональных данных, обрабатываемых в информационной системе персональных данных, при их передаче по открытым каналам связи, применяются шифровальные (криптографические) средства защиты информации.

5.18 Обращение с шифровальными (криптографическими) средствами защиты информации, эксплуатируемыми в информационной системе персональных данных, осуществляется в соответствии с «Инструкцией по обращению с шифровальными (криптографическими) средствами защиты информации», утвержденной приказом директора ИПФ РАН.

5.19 Ответственному за защиту информации или администратору информационной системы персональных данных должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в информационную систему персональных данных;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка персональных данных;
- факты сбоя или некорректной работы систем обработки персональных данных;
- факты сбоя или некорректной работы средств защиты информации;

- факты разглашения информации, содержащей персональные данные, обрабатываемые в информационной системе персональных данных;
- факты разглашения информации о методах и способах защиты и обработки персональных данных в информационной системе.

5.20 Разбор инцидентов информационной безопасности проводится, согласно «Регламенту реагирования на инциденты информационной безопасности в информационных системах персональных данных», утвержденному приказом директора ИПФ РАН.

5.21 Контроль за принимаемыми мерами по обеспечению безопасности персональных данных, осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных», утвержденным приказом директора ИПФ РАН.

6. Ответственность

6.1 Все работники Управления, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

6.2 Ответственность за доведение требований настоящего Положения до работников Управления несет ответственный за организацию обработки персональных данных.

6.3 Ответственность за обеспечение мероприятий по реализации требований настоящего Положения несет ответственный за защиту информации.

Приложение 1
к Положению об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Журнал учета средств защиты информации, эксплуатационной и технической документации к ним в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

Инв. № _____

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание
1	2	3	4	5	6	7