УТВЕРЖДЕН
Советом НАПФ
Протокол № 6 от 31 марта 2023 г.

СИСТЕМА СТАНДАРТИЗАЦИИ НАПФ

ОБРАБОТКА И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В НЕГОСУДАРСТВЕННЫХ ПЕНСИОННЫХ ФОНДАХ

Москва 2023

Предисловие

Настоящий внутренний стандарт Саморегулируемой организации Национальная ассоциация негосударственных пенсионных фондов разработан в соответствии с частью 2 статьи 6 Федерального закона от 13 июля 2015 г. № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка», Федеральным законом от 7 мая 1998 г. № 75-ФЗ «О негосударственных пенсионных фондах» (далее - Федеральный закон № 75-ФЗ), Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и Уставом Саморегулируемой организации Национальная ассоциация негосударственных пенсионных фондов с учетом целей и принципов стандартизации в Саморегулируемой организации Национальная ассоциация негосударственных пенсионных фондов (далее – НАПФ), установленных стандартом «Система стандартизации НАПФ. Основные положения (СТО НАПФ 1.0-2008)».

Содержание:

1 Область применения

1.1 Негосударственные пенсионные фонды являются операторами персональных данных в соответствии со статьей 3 Федерального закона № 152-ФЗ, поэтому обязаны принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом № 152-ФЗ или другими федеральными законами.

1.2 Настоящий внутренний стандарт разработан для использования подразделениями негосударственного пенсионного фонда, осуществляющими организацию обработки и защиты персональных данных, а также подразделениями, осуществляющими контроль за обработкой и защитой персональных данных.

1.3 Настоящий внутренний стандарт содержит описание требований к обработке и защите персональных данных.

2 Термины и сокращения

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

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

2.3 Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.4 НАПФ - Саморегулируемая организация Национальная ассоциация негосударственных пенсионных фондов.

2.5 Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.6 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.

2.7 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.

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

2.9 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 № 152-ФЗ.

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

2.11 Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

2.12 РФ - Российская Федерация.

2.13 СКЗИ - средство криптографической защиты информации.

2.14 СФ - среда функционирования СКЗИ.

2.15 УЗ – уровень защищенности.

2.16 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.

2.17 ФСБ России - Федеральная служба безопасности Российской Федерации.

2.18 ФСТЭК России - Федеральная служба по техническому и экспортному контролю Российской Федерации.

3 Организация обработки и защиты персональных данных в негосударственных пенсионных фондах

3.1 Назначение ответственных лиц

3.1.1 С целью общей организации обработки персональных данных и в соответствии с требованиями статьи 22.1 Федерального закона № 152-ФЗ, негосударственный пенсионный фонд обязан назначить лицо, ответственное за организацию обработки персональных данных. Лицом, ответственным за организацию обработки персональных данных, может выступать как физическое лицо, в том числе работник негосударственного пенсионного фонда, так и юридическое лицо, привлекаемое негосударственным пенсионным фондом по договору.

Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от руководителя негосударственного пенсионного фонда, и подотчетно ему.

В обязанности лица, ответственного за организацию обработки персональных данных, должно войти:

- осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

3.1.2 В соответствии с Постановлением Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», при наличии информационных систем персональных данных, имеющих третий уровень защищенности, негосударственному пенсионному фонду также необходимо назначить должностное лицо, ответственное за обеспечение безопасности персональных данных в таких информационных системах, а при наличии информационных систем персональных данных, имеющих первый уровень защищенности, требуется создать структурное подразделение, ответственное за обеспечение безопасности персональных данных в таких информационных системах, или возложить обязанности на одно из существующих структурных подразделений.

Для разных информационных систем персональных данных по целям обработки может быть назначено одно должностное лицо\структурное подразделение при принятии руководителем негосударственного пенсионного фонда соответствующего решения.

3.2 Государственный контроль за соответствием обработки персональных данных

3.2.1 Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных является Роскомнадзор.

Негосударственный пенсионный фонд обязан сообщать в Роскомнадзор по запросам необходимую информацию в течение десяти рабочих дней с даты получения запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес Роскомнадзора мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.3 Уведомление Роскомнадзора об обработке персональных данных

3.3.1 Негосударственные пенсионные фонды обязаны уведомить Роскомнадзор о намерении осуществлять обработку персональных данных или об обработке персональных данных, если ранее такое уведомление не было подано. Негосударственный пенсионный фонд вправе не уведомлять Роскомнадзор об обработке персональных данных в случае, если деятельность по обработке персональных данных осуществляется исключительно без использования средств автоматизации.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Состав сведений, указываемых негосударственным пенсионным фондом в уведомлении, определен в части 3 статьи 22 Федерального закона № 152-ФЗ. Уведомление можно сформировать в бумажном или электронном виде с помощью официального портала персональных данных Роскомнадзора в информационно-телекоммуникационной сети «Интернет» по адресу: https://pd.rkn.gov.ru/.

3.3.2 В случае изменения сведений, направленных в Роскомнадзор, оператор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, обязан уведомить об этом Роскомнадзор. Также в случае прекращения обработки персональных данных негосударственный

пенсионный фонд обязан уведомить об этом Роскомнадзор в течение десяти рабочих дней с даты прекращения обработки персональных данных.

Для уведомления об изменениях или прекращении обработки персональных данных, Роскомнадзором предусмотрена отдельная форма информационного письма, сформировать которую можно на официальном портале персональных данных Роскомнадзора.

3.4 Уведомление об инцидентах

В соответствии с частью 12 статьи 19 Федерального закона № 152-ФЗ операторы персональных данных обязаны обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных. Такое взаимодействие негосударственные пенсионные фонды могут обеспечивать через автоматизированную систему обработки инцидентов ФинЦЕРТ Банка России, путем направления в Национальный координационный центр по компьютерным инцидентам соответствующего уведомления.

В соответствии с частью 3.1 статьи 21 Федерального закона № 152-ФЗ 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, Роскомнадзором или иным заинтересованным лицом уведомить Роскомнадзор:

- в течение двадцати четырех 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 Роскомнадзором, по вопросам, связанным с выявленным инцидентом;
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.5 Параметры обработки персональных данных

В соответствии с пунктом 2 части 1 статьи 18.1 Федерального закона № 152-ФЗ, негосударственные пенсионные фонды обязаны издать локальные

акты по вопросам обработки персональных данных, определяющие для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на негосударственные пенсионные фонды не предусмотренные законодательством Российской Федерации полномочия и обязанности.

3.5.1 Цели обработки персональных данных должны охватывать все процессы деятельности негосударственного пенсионного фонда, которые предусматривают обработку персональных данных.

3.5.2 Категории субъектов персональных данных напрямую связаны с целями обработками персональных данных. Для определения перечня в отношении каждой цели необходимо провести анализ циркулирующей информации. При анализе необходимо также определить перечень обрабатываемых персональных данных и отнести их к соответствующим категориям (общедоступные, биометрические, специальные или иные).

К биометрическим персональным данным относятся 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, а их обработка может осуществляться исключительно при наличии согласия на обработку персональных данных в письменной форме.

К специальным категориям персональных данных относятся сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Если обработка таких персональных данных осуществляется не в целях исполнения законодательства, то она допускается исключительно при наличии согласия на обработку персональных данных в письменной форме.

К общедоступным персональным данным относятся персональные данные, размещенные в общедоступном источнике персональных данных.

3.5.3 Общий принцип определения сроков обработки персональных данных – персональные данные должны обрабатываться не дольше, чем требуется для достижения заявленных целей обработки. В каждом процессе

обработки персональных данных негосударственные пенсионные фонды должны определить сроки обработки. Определение срока обработки должно осуществляться на основании нормативных правовых актов РФ, регулирующих рассматриваемый процесс обработки персональных данных. В соответствии с Федеральным законом № 152-ФЗ хранение является одним из действий по обработке персональных данных.

3.5.4 Среди способов обработки необходимо указывать, какой тип обработки осуществляется (автоматизированная и/или неавтоматизированная), а также использование технологий передачи данных (передача по внутренней сети или сети интернет)

3.6 Правовые основания для обработки персональных данных в негосударственных пенсионных фондах

Обработка персональных данных в соответствии с каждой целью обработки должна быть правомерна (для каждой цели должны быть определены правовые основания). Определение правовых оснований должно осуществляться негосударственным пенсионным фондом в соответствии со статьей 6 Федерального закона № 152-ФЗ.

3.6.1 Правовые основания обработки биометрических персональных данных и специальных категорий персональных данных отдельно устанавливаются статьями 10 и 11 Федерального закона № 152-ФЗ .

При этом, в соответствии со статьей 15 Федерального закона №75-ФЗ негосударственный пенсионный фонд не обязан получать согласие вкладчиков - физических лиц, страхователей - физических лиц, участников, застрахованных лиц, выгодоприобретателей на обработку в объеме, необходимом для исполнения договора, персональных данных, касающихся состояния здоровья указанных лиц и предоставленных ими или с их согласия третьими лицами.

3.6.2 В качестве правового основания обработки персональных данных негосударственным пенсионным фондом может применяться наличие согласия субъекта персональных данных на обработку. Положениями Федерального закона № 152-ФЗ предусмотрены три вида согласий на обработку персональных данных, каждое из которых требуется получать в зависимости от обстоятельств:

- Согласие на обработку персональных данных (без указания формы);
- Согласие на обработку персональных данных в письменной форме;

- Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

3.6.2.1 Согласие на обработку персональных данных (без указания формы) должно применяться во всех случаях, когда законодательством установлено получение согласия без указания его формы. Требования к его содержанию не установлены.

3.6.2.2 Согласие на обработку персональных данных в письменной форме требуется получать в ряде случаев, установленных Федеральным законом № 152-ФЗ или другими нормативными правовыми актами РФ, когда в явном виде указано, что должно быть получено согласие на обработку персональных данных в письменной форме. Требования к содержанию такого согласия установлены частью 4 статьи 9 Федерального закона № 152-ФЗ, в соответствии с которой в письменной форме согласия на обработку персональных данных не должно быть более одной цели обработки.

3.6.2.3 Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, должно быть получено при размещении персональных данных в общем доступе, если такое размещение не предусмотрено нормативными правовыми актами РФ или предусмотрено ими исключительно при наличии согласия. Требования к такому согласию установлены Приказом Роскомнадзора от 24 февраля 2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». В соответствии со статьей 10.1 Федерального закона № 152-ФЗ такое согласие должно оформляться отдельно от иных согласий на обработку персональных данных.

3.7 Передача персональных данных третьим лицам

Передача персональных данных является одним из действий по обработке и должна иметь правовое основание. Негосударственному пенсионному фонду требуется получить согласие субъекта, если передача его персональных данных осуществляется не в целях:

- исполнения нормативного правового акта РФ;
- законного требования государственной или регулирующей организации;
- исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

Если работодателем осуществляется передача персональных данных собственных работников, то в соответствии со статьей 88 Трудового кодекса РФ указанное выше согласие должно соответствовать согласию на обработку персональных данных в письменной форме.

3.8 Поручение обработки персональных данных третьим лицам

Поручение негосударственным пенсионным фондом обработки персональных данных третьему лицу является передачей третьему лицу функции, которую осуществляет негосударственный пенсионный фонд.

В соответствии с частью 3 статьи 6 Федерального закона № 152-ФЗ, для поручения обработки персональных данных другому лицу необходимо получить на это согласие субъекта персональных данных, если иное не предусмотрено законодательством.

Фонд не обязан получать согласие субъектов персональных данных на дачу поручения обработки персональных данных третьим лицам в случаях, предусмотренных статьей 15 Федерального закона № 75-ФЗ (фонд вправе поручить обработку персональных данных вкладчиков - физических лиц, страхователей - физических лиц, участников, застрахованных лиц, выгодоприобретателей, правопреемников участников и застрахованных лиц организациям, которые в соответствии с договором осуществляют ведение пенсионных счетов, если указание на такие организации содержится в правилах фонда, а также иным организациям, если это необходимо для исполнения пенсионного договора, договора об обязательном пенсионном страховании).

При поручении необходимо обеспечить выполнение требований, установленные частью 3 статьи 6 Федерального закона № 152-ФЗ, предусматривающих определение в поручении:

- перечня персональных данных;
- перечня действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- цели обработки;
- обязанность лица, осуществляющего обработку персональных данных, соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона № 152-ФЗ;
- обязанность лица, осуществляющего обработку персональных данных, по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных,

предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии со статьей 6 Федерального закона № 152-ФЗ;

- обязанность лица, осуществляющего обработку персональных данных, обеспечивать безопасность персональных данных при их обработке;

- требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ, в том числе требование об уведомлении оператора о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

3.9 Прекращение обработки и уничтожение персональных данных

3.9.1 Федеральным законом № 152-ФЗ установлены следующие случаи, в соответствии с которыми оператор обязан прекратить обработку и уничтожить персональные данные:

3.9.1.1 В соответствии с частью 2 статьи 15, оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку персональных данных, осуществляемую в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи;

3.9.1.2 В соответствии с частью 3 статьи 21, в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожить такие персональные данные или обеспечить их уничтожение;

3.9.1.3 В соответствии с частью 4 статьи 21, в случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если

иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами;

3.9.1.4 В соответствии с частью 5 статьи 21, в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами;

3.9.1.5 В соответствии с частью 5.1 статьи 21, в случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, когда у оператора имеется правовое основание, предусмотренное Федеральным законом № 152-ФЗ;

3.9.1.6 В соответствии с частью 3 статьи 20, в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом

персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.9.2 В соответствии с частью 6 статьи 21 Федерального закона № 152-ФЗ, в случае отсутствия у оператора возможности уничтожения персональных данных в течение установленных сроков, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.9.3 Уничтожение персональных данных должно производиться способом, исключающим возможность дальнейшей обработки.

3.9.4 Свидетельства уничтожения персональных данных должны быть оформлены в соответствии с приказом Роскомнадзора от 28 октября 2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных».

3.10 Оценка вреда субъектам персональных данных

В соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона № 152-ФЗ, оператор обязан проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ. Оценка вреда должна производиться в соответствии с приказом Роскомнадзора от 27 октября 2022 № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

3.11 Требования к неавтоматизированной обработке персональных данных

Требования по обработке и защите персональных данных, обработка которых осуществляется без использования средств автоматизации, устанавливаются Постановлением Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных

данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687).

К неавтоматизированной обработке относится любая обработка персональных данных, в которой не задействованы средства вычислительной техники.

Процесс обработки персональных данных может предусматривать сразу автоматизированную и неавтоматизированную обработку персональных данных. При этом на каждом технологическом участке обработки персональных данных должны быть реализованы соответствующие требования к обработке и защите персональных данных.

Для выполнения требований к обработке персональных данных, установленных постановлением Правительства РФ № 687, негосударственные пенсионные фонды должны обеспечить:

3.11.1Исключение фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

3.11.2Использование журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, только при наличии локальных актов, включающих в себя сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных. При этом занесение персональных данных каждого субъекта персональных данных в такой журнал (реестр, книгу) должно заноситься не более одного раза в каждом случае пропуска на территорию, а копирование информации из него - запрещено.

3.11.3Определение мест хранения материальных носителей персональных данных для каждой категории персональных данных путем издания локального акта.

3.11.4Определение перечня лиц, осуществляющих обработку персональных данных путем издания локального акта.

3.11.5Раздельное хранение персональных данных, обработка которых осуществляется в различных целях, путем их размещения в отдельных

запираемых хранилищах в одном помещении или их размещения в отдельных помещениях. В отношении хранилищ и помещений, в которых осуществляется хранение материальных носителей персональных данных, должны применяться меры, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.12 Ознакомление работников, осуществляющих обработку персональных, с информацией

3.12.1 В соответствии с пунктом 6 части 1 статьи 18.1 Федерального закона № 152-ФЗ оператор обязан осуществлять ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

3.12.2 В соответствии с пунктом 6 постановления Правительства РФ № 687, оператор обязан информировать всех лиц (работников или лиц, осуществляющих обработку по договору с оператором) о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами оператора.

3.13 Издание и публикация политики в отношении обработки персональных данных

В соответствии с частью 2 статьи 18.1 Федерального закона № 152-ФЗ оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных

данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3.14 Обработка обращений субъектов персональных данных

3.14.1 Субъекты персональных данных имеют право обращения к оператору по вопросам обработки их персональных данных или направления ему запроса, связанного с обработкой его персональных данных. Ответ на обращение/запрос должен быть направлен в течение десяти рабочих дней с даты получения обращения/запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3.14.2 Обращение субъекта должно содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

3.14.3 Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ. Оператор должен предоставить информацию субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

3.14.4 В соответствии с частью 3 статьи 20 Федерального закона № 152-ФЗ, оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с

персональными данными, относящимися к этому субъекту персональных данных.

3.14.5 Частью 8 статьи 14 Федерального закона № 152-ФЗ устанавливается ряд случаев, когда право субъекта персональных данных на доступ к его персональным данным может быть ограничено.

В случае отказа в предоставлении информации о наличии персональных данных, оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.14.6 В соответствии с частью 1 статьи 14 Федерального закона № 152-ФЗ 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.

В соответствии с частью 1 статьи 21 Федерального закона № 152-ФЗ, в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных,

или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В соответствии с частью 2 статьи 21 Федерального закона № 152-ФЗ, в случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.15 Обязательные требования при принятии решений на основании исключительно автоматизированной обработки персональных данных

В соответствии со статьей 16 Федерального закона № 152-ФЗ, решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

При этом оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

Оператор обязан рассмотреть возражение против такого решения в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

3.16 Обязанности оператора при сборе персональных данных

3.16.1 При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152-ФЗ.

3.16.2 В соответствии с частью 3 статьи 18 Федерального закона № 152-ФЗ, если персональные данные получены не от субъекта персональных данных, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- перечень персональных данных;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом № 152-ФЗ права субъекта персональных данных;
- источник получения персональных данных.

Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона № 152-ФЗ;
- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных указанных выше сведений нарушает права и законные интересы третьих лиц.

3.16.3 При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение

(обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона № 152-ФЗ.

4 Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных негосударственных пенсионных фондов

В соответствии с частью 2 статьи 19 Федерального закона № 152-ФЗ, обеспечение безопасности персональных данных должно достигаться, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.1 Выявление и описание информационных систем персональных данных

Для выявления, описания и учёта всех информационных систем персональных данных, используемых в негосударственном пенсионном фонде, должна быть проведена инвентаризация всех систем и содержащихся в них персональных данных. В ходе данного этапа выполняется описание конфигурации, физического расположения и структуры информационной системы, реализованных защитных мер, а также определяются границы информационных систем персональных данных. На основании проведенных работ определяется список информационных систем персональных данных, оформляемый в виде перечня и описаний информационных систем персональных данных, используемых в негосударственном пенсионном фонде.

4.2 Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных

С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в информационных системах персональных данных, проводятся анализ и оценка угроз безопасности персональных данных, по результатам которых определяются актуальные угрозы безопасности персональных данных. Оценка угроз безопасности информации должна осуществляться в соответствии с требованиями документа «Методический документ. Методика оценки угроз безопасности информации», утвержденного ФСТЭК России 5 февраля 2021.

Оценка угроз безопасности информации должна включать в себя следующие этапы:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- определение возможных объектов воздействия угроз безопасности информации;
- оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

На основании результатов проведенной оценки угроз безопасности персональных данных формируется документ «Модель угроз безопасности персональных данных», содержащая следующие сведения:

- описание систем и сетей и их характеристика как объектов защиты;
- возможные негативные последствия от реализации (возникновения) угроз безопасности информации;
- возможные объекты воздействия угроз безопасности информации;

- источники угроз безопасности информации;
- способы реализации (возникновения) угроз безопасности информации;
- актуальные угрозы безопасности информации.

Допускается разработка как одной модели угроз, включающей в себя все информационные системы персональных данных, так и отдельных моделей угроз для каждой информационной системы персональных данных.

4.3 Определение уровня защищенности информационных систем персональных данных

Для каждой информационной системы персональных данных должен быть определен уровень защищенности персональных данных. Для его определения необходимо в отношении каждой информационной системы установить тип информационной системы персональных данных, вид обработки по форме отношений между субъектами и негосударственным пенсионным фондом, количество субъектов, а также тип угроз актуальных для информационной системы.

В зависимости от категории обрабатываемых для каждой информационной системы персональных данных должен быть определен один из следующих типов:

- информационная система, обрабатывающая специальные категории персональных данных;
- информационная система, обрабатывающая биометрические персональные данные;
- информационная система, обрабатывающая общедоступные персональные данные;
- информационная система, обрабатывающая иные категории персональных данных.

Для каждой информационной системы персональных данных должна быть определена форма отношений между негосударственным пенсионным фондом и субъектами, обработка персональных данных которых осуществляется:

- обработка персональных данных работников негосударственного пенсионного фонда;
- обработка персональных данных субъектов, не являющихся работниками негосударственного пенсионного фонда.

Если в информационной системе персональных данных обрабатываются персональные данные субъектов, не являющихся работниками

негосударственного пенсионного фонда, необходимо определить количество субъектов, чьи персональные данные обрабатываются:

- менее 100 000 субъектов;
- более 100 000 субъектов.

Для каждой информационной системы персональных данных должен быть определен тип актуальных угроз:

- угрозы 1-го типа связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе персональных данных;
- угрозы 2-го типа связаны с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе персональных данных;
- угрозы 3-го типа не связаны с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе персональных данных.

Наличие актуальных угроз, связанных с наличием недокументированных (недекларированных) возможностей в системном либо прикладном программном обеспечении определяется на этапе оценки угроз безопасности персональных данных с учетом оценки возможного вреда. Определение уровня защищенности персональных данных должно быть оформлено документально.

4.4 Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных информационной системы персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных. Постановление Правительства Российской Федерации от 1 ноября 2012 № 1119 устанавливает требования к защите персональных данных в зависимости от уровня защищенности персональных данных при их обработке в информационных системах, представленные в Таблице 1.

Таблица 1 – Требования к защите персональных данных

Требования к защите персональных данных	Уровни защищенности персональных

	данных			
	4 уровень	3 уровень	2 уровень	1 уровень
организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
обеспечение сохранности носителей персональных данных	+	+	+	+
утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе	-	+	+	+
доступ к содержанию электронного журнала сообщений должен быть возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей	-	-	+	+
автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	-	-	-	+
создание структурного подразделения, ответственного за обеспечение безопасности	-	-	-	+

персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности				

После определения требований к защите персональных данных осуществляется выбор мер защиты информации, нейтрализующих актуальные угрозы безопасности. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, установлены в Приказе ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК России от 18 февраля 2013 № 21).

Меры по обеспечению безопасности персональных данных должны реализовываться в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

В случае применения компенсирующих мер в соответствии с Приказом ФСТЭК России от 18 февраля 2013 № 21 в системе защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных. Для таких мер должна проводиться оценка достаточности их применения.

При необходимости использования средств криптографической защиты информации для обеспечения безопасности персональных данных, необходимо реализовать ряд мер по защите информации и осуществлять выбор таких средств в соответствии с Приказом ФСБ России от 10 июля 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» (далее - Приказ ФСБ от 10 июля 2014 № 378), который устанавливает требования в зависимости от уровня защищенности

персональных данных и типа актуальных угроз информационной системы персональных данных. После определения и выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе, должны быть определены методы и средства их реализации. После этого необходимо осуществить внедрение мер выбранными методами и средствами.

На этапе внедрения системы защиты персональных данных должны быть проведены следующие мероприятия:

- осуществляется закупка, установка и настройка программных и технических средств защиты информации согласно требованиям, определенным в проектной документации;
- утверждаются и вводятся в действие локальные акты, определяющие требования и порядок действий по обеспечению безопасности персональных данных;
- проводится инструктаж работников, участвующих в обработке и обеспечении безопасности персональных данных. В качестве инструктажа может выступать ознакомление с утвержденными организационно-распорядительными документами, регламентирующими вопросы обеспечения безопасности персональных данных, а также иные формы доведения необходимой информации.

Если при внедрении системы защиты осуществляются приемо-сдаточные испытания, их результаты оформляются соответствующими протоколами и актами.

4.5 Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации

При применении средств защиты информации для обеспечения безопасности персональных данных в отношении них должна быть проведена процедура оценки соответствия. Подтверждение проведения такой процедуры должно быть предоставлено в виде сертификата соответствия, выданного ФСТЭК России или ФСБ России, или в виде испытаний, проводимых оператором самостоятельно или с привлечением организации-лицензиата ФСТЭК России по технической защите конфиденциальной информации.

В отношении средств криптографической защиты информации Приказом ФСБ от 10 июля 2014 № 378 предусмотрено подтверждение оценки соответствия исключительно в виде наличия сертификата ФСБ России, устанавливающего заданный класс криптографического средства.

4.6 Учет машинных носителей персональных данных

Негосударственные пенсионные фонды обязаны осуществлять учет машинных носителей информации. К ним относятся как съемные машинные носители информации, так и носители информации, постоянно размещаемые в технических средствах обработки информации (серверах и автоматизированных рабочих местах пользователей). Допускается учитывать машинные носители в составе сервера или рабочего места, если технологическим процессом обработки информации не предусматривается извлечение таких носителей. Для учета необходимо применять бумажный или электронный документ, в котором будут зафиксированы инвентарные\серийные номера машинных носителей информации или технических средств обработки информации.

4.7 Обнаружение инцидентов информационной безопасности

Негосударственный пенсионный фонд обязан осуществлять обнаружение инцидентов информационной безопасности и информирование о них в соответствии с пунктом 3.4 настоящего внутреннего стандарта. В этих целях должен быть разработан локальный акт, регламентирующий порядок обнаружения и реагирования на инциденты безопасности.

4.8 Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

Обеспечение возможности восстановления персональных данных должно осуществляться негосударственным пенсионным фондом путем регламентации и реализации процесса резервного копирования персональных данных, обрабатываемых в информационных системах персональных данных.

Негосударственным пенсионным фондом должна обеспечиваться безопасность резервных копий, предусматривающая в том числе наличие не менее двух копий данных (основная и не менее одной резервной), хранимых по не менее двум разным адресам.

4.9 Установление правил доступа к персональным данным

Негосударственный пенсионный фонд обязан определить порядок предоставления прав доступа к персональным данным, обрабатываемым с применением средств автоматизации путем издания соответствующего локального акта, а также путем реализации и/или применения механизмов разграничения доступа, если изданным локальным актом предусмотрены различные уровни доступа.

4.10 Регистрация действий, осуществляемых с персональными данными

Негосударственный пенсионный фонд обязан обеспечить регистрацию и учет всех действий, совершаемых с персональными данными в

информационной системе персональных данных пользователями таких систем. Регистрация действий должна быть реализована встроенными средствами программного обеспечения, используемого для обработки персональных данных, или наложенными средствами защиты, обеспечивающими регистрацию указанных действий.

5 Контроль выполнения требований по обработке и защите персональных данных

5.1 Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных

В соответствии с Приказом ФСТЭК России от 18 февраля 2013 № 21, негосударственный пенсионный фонд обязан провести оценку эффективности применяемых мер по обеспечению безопасности персональных данных для каждой информационной системы персональных данных (далее – оценка эффективности). Оценка эффективности проводится перед вводом информационной системы персональных данных в промышленную эксплуатацию и регулярно в процессе эксплуатации не реже 1 раза в 3 года.

Оценка эффективности может проводиться в следующих формах:

- собственными силами:
  - в форме приёмо-сдаточных испытаний мер обеспечения безопасности персональных данных, предусмотренных техническим заданием (частным техническим заданием) на систему защиты персональных данных оцениваемой информационной системы персональных данных;
  - в форме анализа защищенности информационной системы персональных данных;
  - в форме оценки (самооценки) соответствия;
  - в иной форме, не противоречащей требованиям нормативных документов в области обеспечения безопасности информации.
- с привлечением подрядчиков:
  - в форме аттестации (при этом подрядчик должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации с разрешенным видом деятельности - работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и систем информатизации);
  - в форме анализа защищенности информационной системы персональных данных (при этом подрядчик должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации с разрешенным видом деятельности - услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации);
  - в форме оценки соответствия (при этом подрядчик должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации с разрешенными видами деятельности, предусмотренными пунктами «б», «д» или «е» пункта 4 Положения о

лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства Российской Федерации от 3 февраля 2012 года №79 «О лицензировании деятельности по технической защите конфиденциальной информации»);

- в иной форме, не противоречащей требованиям нормативных документов в области обеспечения безопасности информации.

Результаты оценки эффективности должны быть зафиксированы документально.

5.2 Контроль и аудит соответствия обработки персональных данных

5.2.1 Контроль соответствия обработки персональных данных

В соответствии с пунктом 4 части 1 статьи 18.1 Федерального закона № 152-ФЗ, оператор обязан осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Внутренний контроль соответствия обработки персональных данных обязан осуществляет ответственный за организацию обработки персональных данных.

Для проведения внутренних проверок должны быть определены направления (предметы) контроля. Формы проведения внутреннего контроля определяется негосударственным пенсионным фондом самостоятельно.

Внутренние проверки требуется проводить не реже одного раза в год. Их результаты должны быть оформлены в виде акта внутреннего контроля, в который включаются сведения:

- о проведенных мероприятиях по контролю;
- о выявленных нарушениях;
- о мерах, необходимых для устранения выявленных нарушений;
- о структурных подразделениях, в деятельности которых выявлены нарушения, и сроки их устранения.

Результаты внутреннего контроля должны быть доведены под подпись до сведения руководителя негосударственного пенсионного фонда, а также руководителей структурных подразделений негосударственного пенсионного фонда, в деятельности которых выявлены нарушения.

Ответственный за организацию обработки персональных данных обеспечивает хранение документов по результатам внутреннего контроля не менее 5 лет.

5.2.2 Аудит

Для проведения аудита привлекаются сторонние организации (далее – аудиторская организация), которые:

- являются лицензиатами ФСТЭК России и ФСБ России;
- имеют опыт проведения соответствующих аудитов не менее 3 лет.

В договоре с аудиторской организацией должна быть прописана ответственность перед негосударственным пенсионным фондом за:

- достоверность выводов по результатам аудита;
- соблюдение конфиденциальности в отношении всех сведений, получаемых и составляемых в ходе проверки негосударственного пенсионного фонда (за исключением случаев, прямо предусмотренных законодательством РФ).

По результатам аудита негосударственный пенсионный фонд должен сформировать план устранения выявленных аудиторской организацией несоответствий и назначить ответственных за выполнение мероприятий данного плана.

6 Заключительные положения

6.1 Настоящий внутренний стандарт вступает в силу со дня принятия решения о его утверждении Советом НАПФ.

6.2 Изменения, вносимые в настоящий внутренний стандарт, вступают в силу по истечении десяти рабочих дней с даты их опубликования на официальном сайте НАПФ в информационно-телекоммуникационной сети «Интернет».

6.3 В случае изменения законодательства Российской Федерации в области обработки и защиты персональных данных настоящий внутренний стандарт действует в части, им не противоречащей.

7 Библиография

Настоящий стандарт основывается на следующих нормативных документах:

- Федеральный закон от 13 июля 2015 г. № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка»;
- Федеральный закон от 7 мая 1998 г. № 75-ФЗ «О негосударственных пенсионных фондах»;
- Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 07 августа 2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 16 марта 2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;
- Постановление Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 3 февраля 2012 года №79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Приказ Роскомнадзора от 24 февраля 2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;
- Приказ Роскомнадзора от 28 октября 2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных»;
- Приказ Роскомнадзора от 27 октября 2022 № 178 «Об утверждении требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона О персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ от 10 июля 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»;
- «ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденный и введенный в действие Приказом Росстандарта от 08.08.2017 № 822-ст;
- Стандарт «Система стандартизации НАПФ. Основные положения (СТО НАПФ 1.0-2008)»;
- «Методический документ. Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021;
- «Методический документ. Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014;
- «Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» РС БР ИББС-2.6-2014», принятые и введенные в действие Распоряжением Банка России от 10.07.2014 № Р-556.