Утверждено
Приказом и.о.генерального директора
Фонда капитального ремонта ВО
от 18.12.2018 № 110/3

ПОЛОЖЕНИЕ
по организации и ведению работ по обеспечению безопасности персональных данных при их обработке

1. Общие положения

Положение по организации и ведению работ по обеспечению безопасности персональных данных (ПДн) при их обработке (далее по тексту – Положение) в некоммерческой организации «Фонд капитального ремонта многоквартирных домов Владимирской области» (далее по тексту - Фонд) разработано в соответствии с требованиями Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ от 21.03.12 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», нормативно-методических документов ФСТЭК России и иных документов в области защиты ПДн.

Целью настоящего Положения является обеспечение безопасности ПДн физических лиц – граждан РФ (собственников общего имущества МКД); сотрудников (работников) Фонда.

Настоящий документ должен быть доведен до сведения всех работников Фонда, имеющих отношение к обработке ПДн.

2. Основные термины и определения

Для целей настоящего Положения используются следующие основные термины и определения:

– ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

– обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

– автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники;

– информационная система ПДн (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

– инцидент информационной безопасности - единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких

событий), которое может скомпрометировать бизнес-процессы компании или угрожает ее информационной безопасности;

– средства защиты информации (СЗИ) — программные, технические, программно-технические средства, предназначенные для защиты информации, а также средства контроля эффективности защиты информации.

3. Организация мероприятий по обеспечению безопасности персональных данных

В целях организации и проведения работ по обеспечению безопасности ПДн в Фонде, приказом генерального директора Фонда назначается лицо, ответственное за организацию обработки ПДн.

Лица, доступ которых к ПДн необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании перечня, утвержденного генеральным директором Фонда.

4. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

Для обеспечения безопасности ПДн в Фонде применяются следующие меры:

4.1. При оформлении на работу или при переводе работника на должность, подразумевающую работу с ПДн в ИСПДн, ответственный за организацию обработки персональных данных:

- в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление работника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных.
- проводит ознакомление работников с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации.
- отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

Работник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

4.2. Личные пароли должны выбираться пользователями ИСПДн самостоятельно с учетом условий, описанных в инструкции по применению парольной политики в информационной системе персональных данных. Контроль действий пользователей ИСПДн при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного за организацию обработки ПДн.

4.3. При увольнении работника или при переводе его на должность, не подразумевающую работу с ПДн в ИСПДн, ответственный за организацию обработки ПДн должен удалить учетную запись соответствующего работника, либо сменить на ней пароль.

4.4. Ремонтно-восстановительные работы технических средств обработки ПДн проводятся под контролем ответственного за организацию обработки ПДн работниками Фонда. При необходимости, ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе, в данном случае в договоре должны быть прописаны условия обеспечения

конфиденциальности и безопасности данных на съемных носителях информации. В противном случае, при передаче технических средств обработки ПДн сторонним специалистам, съемные носители информации должны быть извлечены.

4.5. Все находящиеся на хранении и в обращении машинные носители, которые являются собственностью Фонда (в том числе жесткие диски компьютеров, входящих в состав ИСПДн), содержащие ПДн подлежат учёту. Учет машинных носителей производится в журнале учета носителей ПДн, в соответствии с положениями Инструкции по работе с носителями ПДн. Ответственность за ведение журнала учета носителей ПДн и постановку на учет машинных носителей возлагается на начальника отдела информационно-технического обеспчения.

4.6. Установочные дистрибутивы программных, либо программно-аппаратных СЗИ, техническая и эксплуатационная документация к ним должны храниться в защищенном от НСД хранилище, доступ к которому имеют только начальника отдела информационно-технического обеспчения. Все СЗИ, техническая и эксплуатационная документация к ним подлежат учету в журнале учета средств защиты информации и эксплуатационной документации.

4.7. Контроль выполнения работ по обеспечению безопасности ПДн в Фонде осуществляется путем проведения периодических внутренних проверок состояния безопасности ПДн, а также по фактам произошедших инцидентов информационной безопасности. Порядок осуществления таких проверок описан в Правилах осуществления внутреннего контроля соответствия обработки ПДн требованиям в области обработки и защиты ПДн.

4.8. В Фонде применяются меры по ограничению доступа работников в помещения, где осуществляется обработка ПДн. Лица, не указанные в перечне должностей работников, допущенных к работе с ПДн, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения, в которых ведется обработка ПДн только в сопровождении ответственных лиц.

4.9. Все технические средства, позволяющие осуществлять обработку ПДн, размещаются исключительно в пределах охраняемой территории. Должна быть организована физическая защита помещений и технических средств, позволяющих осуществлять обработку ПДн.

4.10. Для использования в ИСПДн допускаются только СЗИ, прошедшие в установленном порядке процедуру оценки соответствия (имеющие сертификат соответствия по требованиям безопасности). Настройки СЗИ должны быть выполнены в соответствии с требованиями безопасности ПДн, отраженными в техническом задании на создание системы защиты ПДн, а также в эксплуатационной документации.

4.11. Антивирусная защита ИСПДн осуществляется с учетом требований инструкции по организации антивирусной защиты информационной системы персональных данных. Ответственность за организацию антивирусного контроля в ИСПДн возлагается на начальника отдела информационно-технического обеспчения.

4.12. Резервное копирование и хранение ПДн должно осуществляться в соответствии с положениями Инструкции о порядке действий во внештатных ситуациях и восстановлению после сбоя.