УТВЕРЖДЕНО
Приказом Генерального директора
ООО МФК «Кватро-Н Фанд»
№ УВД-15 от «26» июня 2019 г.

С.Ю. Землянов

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МИКРОФИНАНСОВАЯ КОМПАНИЯ «КВАТРО-Н ФАНД»

Москва
2019

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с действующим законодательством в области защиты персональных данных и определяет состав и содержание организационных и технических мер Общества с ограниченной ответственностью Микрофинансовая компания «Кватро-Н Фанд» (далее - **Оператор**) по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения установленных требований к защите персональных данных (далее - **Положение**).

1.2. Положение по организации и проведению работ по обеспечению безопасности персональных данных и изменения к нему утверждаются Оператором в соответствии с его Уставом. Все сотрудники Оператора должны быть ознакомлены под расписку с содержанием Положения и всеми изменениями к нему.

1.3. Обработка персональных данных осуществляется путем совершения следующих действий (операций): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.4. Обработка персональных данных осуществляется смешанным способом:

- автоматизированная обработка персональных данных с передачей полученной информации по внутренней сети Оператора и информационно-коммуникационной сети «Интернет»;
- неавтоматизированная обработка персональных данных (ведение личных карточек).

2. ОСНОВНЫЕ ПОНЯТИЯ

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

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

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

Защита персональных данных - регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий надежную безопасность информации при осуществлении Оператором деятельности.

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

Неавтоматизированная обработка персональных данных - обработка персональных данных, осуществляемая при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав или правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту 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.

Обработка персональных данных на бумажном носителе - обработка персональных данных, в том числе неавтоматизированная, осуществляемая Оператором с помощью фиксации персональных данных каждого из субъектов персональных данных на бумажном носителе.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

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

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать сбор, запись, систематизация, накопление, хранение, изменение, извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, удаление, уничтожение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

3. СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. При обработке персональных данных граждан допущенные к ним лица обязаны соблюдать требования, действующего законодательства в области защиты персональных данных, а также правила, установленные настоящим Положением, иными внутренними документами Оператора.

3.2. Защита персональных данных субъектов персональных данных от неправомерного их использования или утраты обеспечивается за счет средств Оператора. Безопасность персональных данных обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.3. В соответствии Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» Оператор осуществляет выполнение следующих обязательных требований:

3.3.1. 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, посредством:

- оснащения указанных помещений входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их

открытия только для санкционированного прохода;

- утверждения правил доступа в указанное помещение в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в помещение;

3.3.2. обеспечение сохранности носителей персональных данных путем:

- осуществления хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием средств криптографической защиты информации (далее - СКЗИ) виде, допускается хранение таких носителей вне сейфов (металлических шкафов);
- осуществления поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров;

3.3.3. разработка и утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей, а также своевременная актуализация сведений, содержащихся в данном документе;

3.3.4. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых средствами криптографической защиты информации персональных данных или создания условий для этого (далее - атака), которое достигается путем:

- получения исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;
- использования для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше.

3.4. Дополнительно в состав мер по обеспечению Оператором безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности персональных данных;
- защита среды виртуализации;
- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;
- резервное копирование электронных документов и баз данных;
- резервное копирование виртуальных серверов.

3.4.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

3.4.2. Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также контроль за соблюдением этих правил.

3.4.3. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения и исключают возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

3.4.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

3.4.5. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

3.4.6. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

3.4.7. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

3.4.8. Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной

системы и тестированию работоспособности системы защиты персональных данных.

3.4.9. Меры по обеспечению целостности информационной системы и персональных данных обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

3.4.10. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

3.4.11. Меры по защите среды виртуализации исключают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

3.4.12. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

3.4.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

3.5. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При использовании в информационных системах, сертифицированных по требованиям безопасности информации средств защиты информации, применяются средства защиты информации не ниже 6 класса.

3.6. Оператор проводит систематический анализ инфраструктуры информационной системы персональных данных с целью определения:

- перечня автоматизированных рабочих мест, обрабатывающих персональные данные;
- перечня серверного, коммутационного и сетевого оборудования;
- используемого в информационной системе персональных данных общесистемного и прикладного программного обеспечения;
- наличия подключения информационной системы персональных данных к сетям связи общего пользования.

3.7. Обеспечивается обязательное назначение структурного подразделения или должностного лица (работника), ответственных за обеспечение безопасности персональных данных.

3.8. Руководители структурных подразделений Оператора предоставляют ответственному за обеспечение безопасности персональных данных актуальные списки сотрудников, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей. Лицо, ответственное за обеспечение безопасности персональных данных предоставляет на утверждение список лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей.

3.9. Оператор разрабатывает и утверждает модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных. На основании утвержденной модели угроз в виде отдельного документа разрабатываются требования по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

3.10. В случае выявления недостоверных персональных данных субъекта персональных данных или неправомерных действий с ними работников Оператора при обращении или по запросу субъекта персональных данных, или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, осуществляется блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.11. В случае подтверждения факта недостоверности персональных данных субъекта персональных данных на основании документов, представленных субъектом персональных данных, или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов Оператор уточняет персональные данные и снимает их блокирование.

3.12. В случае выявления неправомерных действий с персональными данными, допущенные нарушения подлежат устранению в срок, не превышающий трех рабочих дней. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления факта неправомерного использования персональных данных, такие персональные данные подлежат уничтожению. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных, или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.13. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. В случае достижения цели обработки персональных данных Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

3.14. Сотрудник Оператора, виновный в нарушении норм, регулирующих получение, обработку, хранение и передачу персональных данных субъектов персональных данных, несет ответственность в соответствии с действующим законодательством Российской Федерации.

3.15. Конкретные меры по обеспечению безопасности персональных данных и их состав представлены в Приложении 1 к настоящему Положению.

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Доступ к персональным данным осуществляется на основании утвержденного списка лиц, доступ которых к персональным данным необходим для выполнения служебных обязанностей.

4.2. Разрешительная система доступа пользователей к информационным ресурсам информационной системы персональных данных оформляется структурным подразделением или должностным лицом, ответственным за обеспечение безопасности персональных данных, в виде матриц доступа, утверждаемых руководителем, и реализуется с помощью средств защиты от несанкционированного доступа. Матрицы доступа должны отражать полномочия пользователей по выполнению конкретных действий в отношении информационных ресурсов информационной системы персональных данных (чтение, запись, корректировка, удаление).

4.3. Оператор ведет электронный журнал обращений пользователей информационной системы к персональным данным.

4.4. Доступ к персональным данным осуществляется согласно Приложению 1 к настоящему Положению.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче персональных данных субъекта персональных данных Оператор должен соблюдать следующие требования:

- передача персональных данных внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- при передаче персональных данных субъекта персональных данных третьим лицам, такие данные не должны сообщаться третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральным законом;
- не допускается отвечать на вопросы, связанные с передачей персональной

информации по телефону, факсу и другим средствам связи;

- по возможности персональные данные обезличиваются.

5.2. Иные условия и ограничения по передаче персональных данных предусмотрены в Приложении 1 к настоящему Положению.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Все магнитные, оптические и другие машинные носители персональных данных подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет. Машинные носители информации, в том числе с резервными копиями персональных данных, регистрируются в журнале учета машинных носителей, в котором отражается:

- тип и емкость носителя;
- учетный номер носителя;
- место установки (использования) носителя;
- дата установки носителя;
- ответственное должностное лицо;
- сведения о списании носителя и уничтожении информации.

6.2. Пользователям запрещается использовать съемные носители информации за исключением случаев, когда использование съемных носителей необходимо в рамках должностных обязанностей.

6.3. Средства защиты информации должны учитываться в специальном журнале учета средств защиты информации, эксплуатационной и технической документации к ним.

6.4. При нарушении работоспособности средств защиты информации удаленных пользователей, передача персональных данных должна быть приостановлена.

6.5. Для защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками Оператора;
- обеспечение порядка приема, учета и контроля деятельности посетителей;
- организация пропускного режима Оператора;
- поддержание порядка охраны территории, зданий, помещений, транспортных средств.

6.6. С целью исключения нарушения работоспособности технических средств информационной системы персональных данных, все технические средства должны быть

опломбированы.

6.7. В отношении данных, содержащихся в информационной системе, для обеспечения безопасности персональных данных при их обработке осуществляются следующие меры:

- организационные меры (ограничение доступа сотрудников Оператора к системе, наличие положения о неразглашении конфиденциальной информации в трудовых договорах с сотрудниками Оператора, ограничение доступа посетителей в помещения Оператора, охрана помещений в ночное время);
- технические (защита персональных данных от несанкционированного доступа посредством средств защиты информации от несанкционированного доступа, обеспечение безопасного межсетевого взаимодействия и обнаружения вторжений, применение средств антивирусной защиты, осуществления анализа защищенности информационной системы персональных данных посредством сетевого сканера).

6.8. Оператор производит периодическое тестирование средств защиты информации и отражает результаты тестирования в специальном журнале периодического тестирования средств защиты информации.

7. ПРАВИЛА ПАРОЛЬНОЙ ЗАЩИТЫ

7.1. Пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

7.2. Установку пароля производит пользователь при первом входе в систему с новой учетной записью.

7.3. Пользователи должны выбирать пароли стойкие к подбору, руководствуясь основными правилами:

- длина пароля должна быть не менее 6 символов;
- пароль не должен иметь семантический смысл (имя пользователя, дата рождения и т.д.);
- пароль не должен являться легко прогнозируемой последовательностью символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов.

7.4. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

7.5. Рекомендуется ежеквартально производить смену пароля, соблюдая требования Положения.

7.6. Восстановление забытого пароля пользователя осуществляется системным администратором путем изменения (сброса) пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

7.7. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору и изменить основной пароль.

8. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ

8.1. К использованию в информационной системе персональных данных допускаются только лицензионные антивирусные средства.

Ответственность за поддержание установленного порядка проведения антивирусного контроля возлагается на системного администратора Оператора.

8.2. На объектах вычислительной техники запрещается установка программного обеспечения, не связанного с выполнением служебных функций.

8.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации должен проводиться автоматически непосредственно после ее приема.

8.4. Системный администратор обязан систематически производить следующие действия:

- осуществлять обновление антивирусных пакетов и контроль их работоспособности;
- проводить тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов. При обнаружении компьютерного вируса пользователь обязан немедленно поставить в известность системного администратора и прекратить какие-либо действия на персональном компьютере;
- в случае необходимости осуществлять лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы, после чего вновь произвести антивирусный контроль. В случае обнаружения на съемном носителе информации нового вируса, не поддающегося лечению, системный администратор обязан запретить использование съемного носителя. В случае обнаружения на жестком магнитном диске не поддающегося лечению вируса, системный администратор обязан запретить работу на персональном компьютере и в возможно короткие сроки обновить пакет антивирусных программ.

9. ПРАВИЛА ОБНОВЛЕНИЯ ОБЩЕСИСТЕМНОГО И ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.1. Под обновлением понимается замена программного обеспечения устаревшей версии на новую версию этого же программного обеспечения. Поскольку программное обеспечение, установленное на персональном компьютере и серверах информационной системы персональных данных документально фиксируется при его аттестации, его обновление будет допустимо лишь в той мере и в том случае, если это подтверждено производственной необходимостью и имеет непосредственное отношение к технологическому процессу (например, антивирусные базы данных, сервисные пакеты обновления операционной системы, исправления и дополнения собственного программного обеспечения).

9.2. В процессе обновления программного обеспечения допускается ввод информации со съемных носителей.

9.3. Операция обновления производится системным администратором и

фиксируется в соответствующем журнале.

10. ФИЗИЧЕСКАЯ ЗАЩИТА ПОМЕЩЕНИЙ И ТЕХНИЧЕСКИХ СРЕДСТВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Размещение технических средств информационной системы персональных данных, специального оборудования, охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

10.2. Помещения, в которых ведется обработка персональных данных, должны быть оборудованы системами охранной и пожарно-охранной сигнализацией. При отсутствии пользователя в помещении, где обрабатываются персональные данные, двери должны запираться на ключ.

11. МЕРЫ, ПРИНИМАЕМЫЕ ОПЕРАТОРОМ ПРИ НАРУШЕНИИ РЕЖИМА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Несоблюдение условий хранения и использования носителей персональных данных и средств защиты информации, режима конфиденциальности информации, режима доступа в помещения может привести к нарушению конфиденциальности, целостности и доступности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

11.2. По фактам несоблюдения указанных условий Оператором создается комиссия для проведения разбирательств и принятия мер по предотвращению возможных опасных последствий подобных нарушений.

11.3. Оператор ведет журнал учета нештатных ситуаций информационной системы персональных данных, выполнения профилактических работ, установки и модификации программных средств на компьютерах информационной системы персональных данных.

12. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

12.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

12.2. Каждый сотрудник Оператора, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

12.3. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет ответственность граждан и юридических лиц, установленную действующим законодательством Российской Федерации.

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Настоящее Положение, а также любые изменения и дополнения к нему утверждаются Генеральным директором Общества, и вступают в силу со дня утверждения.

13.2. В случае если какие-либо нормы настоящего Положения станут противоречить законодательству Российской Федерации, соответствующие нормы не подлежат применению.