Положение о порядке организации и обеспечения безопасности персональных данных при их обработке ЗАО "Сбербанк Лизинг" (Утверждено Решением Правления ЗАО "Сбербанк Лизинг" от 31.07.2013 N 23-07/13. Зарегистрировано 07.08.2013 N 076-1)

УТВЕРЖДЕНО
Решением Правления
ЗАО "Сбербанк Лизинг"
от 31.07.2013 N 23-07/13

Зарегистрировано 07.08.2013 N 076-1

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ ЗАО "СБЕРБАНК ЛИЗИНГ"

Реквизиты ВНД смотри в файле Rekviziti_076_1.doc.

1. Назначение и область действия

1.1 Настоящее Положение предназначено для организации в ЗАО "Сбербанк Лизинг" (далее Компания) процесса обеспечения безопасности персональных данных (далее ПДн) согласно требованиям действующего федерального законодательства:

- Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ "О персональных данных";

- Постановление Правительства Российской Федерации от 01.11.2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2 Действие настоящего Положения распространяется на все процессы, связанные с обработкой ПДн.

1.3 Положение обязательно для ознакомления и исполнения руководителями и работниками структурных подразделений, принимающих участие в обработке ПДн, работниками Управления информационных технологий, являющимися Администраторами информационной системы персональных данных (далее ИСПДн), Ответственным за организацию обработки ПДн, Ответственным за обеспечение безопасности ПДн, Координатором по обращениям и запросам.

2. Меры по обеспечению безопасности ПДн при их обработке

2.1 Компания при обработке ПДн обязана принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного

доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.2 Обеспечение безопасности ПДн достигается, в частности:

- определением угроз безопасности ПДн при их обработке в ИСПДн;

- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

- использованием средств защиты информации (далее СЗИ), прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

- обеспечением сохранности носителей ПДн;

- учетом машинных носителей ПДн;

- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

3. Обязательные мероприятия по обеспечению безопасности ИСПДн

3.1 Общие требования

3.1.1 В Компании до начала проведения работ по обеспечению безопасности ПДн должна быть проведена инвентаризация ИСПДн путем опроса владельцев информационных систем (далее ИС) на предмет наличия обработки в них ПДн.

3.1.2 После инвентаризации ИС выявляются ИСПДн, в которых осуществляется автоматизированная обработка ПДн, и ИСПДн, в которых осуществляется неавтоматизированная обработка ПДн.

3.1.3 Для всех эксплуатируемых ИСПДн с автоматизированной обработкой ПДн должны быть определены уровни защищенности ПДн в ИСПДн в соответствии с Постановлением Правительства Российской Федерации от 01.11.2 г. N 1119 "Требования к защите персональных данных при их обработке в информационных системах персональных данных". Определение уровней защищенности ИСПДн проводится в следующей последовательности:

а) приказом Генерального Директора Компании создается Комиссия по определению уровней защищенности ПДн в ИСПДн;

б) Комиссия в определенный приказом срок устанавливает категории, объем и актуальность угроз, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программных обеспечениях для обрабатываемых ПДн в ИСПДн;

в) Комиссия определяет уровни защищенности ПДн для каждой ИСПДн.

3.1.4 В Компании должны быть разработаны Модели угроз для всех ИСПДн. Модель угроз разрабатывается сторонней компанией, имеющей лицензию Федеральной службы по техническому и экспортному контролю на техническую защиту информации, на основе методических документов ФСТЭК России.

3.1.5 Выбор и реализация методов и способов защиты информации в ИСПДн осуществляются на основе Модели угроз и в зависимости от уровня защищенности ПДн в ИСПДн.

3.1.6 Выбранные и реализованные методы и способы защиты ПДн в ИСПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИСПДн в составе создаваемой системы защиты ПДн.

3.1.7 Для проведения работ по выбору и реализации методов и способов защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.1.8 Общие технические требования по защите ПДн в ИСПДн Компании приведены в разделе 4.

3.2 Требования к разработке и вводу в эксплуатацию ИСПДн

3.2.1 Разработка ИСПДн должна включать следующие стадии:

а) предпроектная стадия (включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн, на основании которого определяется предварительный класс ИСПДн, степень участия должностных лиц, актуализируются угрозы безопасности);

б) стадия проектирования системы защиты ПДн для ИСПДн;

в) стадия ввода в эксплуатацию ИСПДн.

По результатам проведенного анализа и с учетом действующих требований федерального законодательства и регуляторов должны быть разработаны:

- Модель угроз безопасности ПДн при их обработке в ИСПДн;

- Требования к защите ПДн при их обработке в ИСПДн;

- Определение уровней защищенности ПДн в ИСПДн;

- Частное техническое задание на создание системы защиты ПДн для ИСПДн.

3.2.2 Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн должно производиться с учетом уже построенной в Компании системы защиты ПДн, включающей комплекс организационных и технических мер.

3.2.3 На стадии ввода в эксплуатацию ИСПДн должны быть проведены как минимум следующие мероприятия:

- установка пакета прикладных программ ИСПДн совместно со СЗИ (встроенными и наложенными);

- опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации.

3.2.4 В случае внедрения дополнительных средств защиты должны быть составлены Акты внедрения СЗИ по результатам их приемо-сдаточных испытаний, подготавливаемые и подписываемые Ответственным за обеспечение безопасности ПДн.

3.2.5 Перед вводом новой ИСПДн в опытную эксплуатацию Администраторами ИСПДн должен быть составлен Акт о вводе в опытную эксплуатацию ИСПДн, подписываемый Ответственным за обеспечение безопасности ПДн и Директором Управления информационных технологий, а также Акт определения уровней защищенности ПДн в ИСПДн, подготовленный и подписанный Комиссией по определению уровней защищенности ПДн в ИСПДн.

3.2.6 В случае успешного функционирования ИСПДн на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию, Администраторами ИСПДн должен быть составлен Акт о вводе в промышленную эксплуатацию новой ИСПДн, подписываемый Ответственным за обеспечение безопасности ПДн и Директором Управления информационных технологий.

3.3 Требования к выводу ИСПДн из эксплуатации

3.3.1 В случае принятия решения о выводе ИСПДн из промышленной эксплуатации Ответственным за обеспечение безопасности ПДн и Директором Управления информационных технологий должен быть подписан Акт о выводе ИСПДн из промышленной эксплуатации.

3.3.2 При выводе ИСПДн из промышленной эксплуатации с целью обеспечения справочной поддержки Компании доступ к ней должен быть ограничен только определенным составом лиц с правами только на чтение.

3.3.3 После подписания Акта о выводе ИСПДн из промышленной эксплуатации ИСПДн должна быть переведена в архивный фонд Компании, при этом должны быть выполнены следующие требования:

- доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководства Компании, по согласованию с Ответственным за организацию обработки ПДн и владельцем ИСПДн;

- ПДн, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации;

- должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

- доступ в помещения, где предполагается хранение выводимой из эксплуатации ИСПДн, должен быть ограничен;

- должен быть регламентирован перечень лиц, допущенных к работе с ИСПДн, переданной в архив;

- все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.), относящиеся к архивной ИСПДн, должны храниться в сейфах;

- должно быть разработано описание ИСПДн, переведенной в архивный фонд Компании. Описание ИСПДн разрабатывается Администраторами ИСПДн и Ответственным за обеспечение безопасности либо сторонней компанией, имеющей лицензию ФСТЭК России на осуществление технической защиты информации.

4. Обеспечение технической защиты ПДн

4.1 Общие требования

4.1.1 Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться на всех стадиях жизненного цикла ИСПДн и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования ИСПДн в случае реализации угроз.

4.1.2 В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн должны включать:

- определение уровней защищенности ПДн в ИСПДн на основании документа "Требования к защите персональных данных при их обработке в информационных системах персональных данных", утвержденное Постановлением Правительства РФ от 01.11.2012 г. N 1119;

- выявление и закрытие технических каналов утечки ПДн на основе анализа и актуализации Модели угроз безопасности ПДн;

- выбор и реализацию методов и способов защиты информации в ИС на основе Модели угроз безопасности ПДн и в зависимости от уровня защищенности ПДн в ИСПДн;

- установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных СЗИ;

- разработку дополнений к трудовым договорам (или должностным инструкциям) по

обеспечению безопасности ПДн при их обработке в ИСПДн для персонала, задействованного в эксплуатации данной ИСПДн.

4.1.3 Предотвращение утечки ПДн по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется в Компании организационными мерами и не требует специальных технических решений.

4.1.4 Защита ПДн при их обработке в ИСПДн от несанкционированного доступа и иных неправомерных действий должна осуществляться в Компании следующими методами и способами:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая ПДн), ИСПДн и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая ПДн), программным средствам обработки (передачи) и защиты ПДн;

- регистрация действий пользователей и обслуживающего персонала ИСПДн, мониторинг попыток несанкционированного доступа;

- учет и хранение съемных носителей информации с ПДн и их обращение, исключающее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей ПДн;

- использование защищенных каналов связи, используемых для передачи ПДн;

- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах контролируемой зоны.

- периодический анализ защищенности распределенных ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);

- предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) и программных закладок;

- регистрация событий и мониторинг процессов обработки информации;

- контроль целостности программных средств.

4.1.5 При организации взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты ПДн от несанкционированного доступа:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и

трансляции сетевых адресов для скрытия структуры ИСПДн;

- обнаружение вторжений в ИСПДн, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

- защита ПДн при их передаче по каналам связи;

- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

- использование средств антивирусной защиты;

- централизованное управление системой защиты ПДн.

4.1.6 В Компании также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

4.1.7 Конкретные методы и средства защиты ПДн в ИСПДн должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России исходя из уровней защищенности ПДн в ИСПДн и актуальных угроз безопасности ПДн.

4.1.8 Все технические СЗИ должны быть снабжены инструкциями по эксплуатации (рекомендациями по использованию).

4.1.9 Должен вестись учет технических СЗИ.

4.1.10 Форма Журнала учета технических СЗИ приведена в приложении (Приложение А).

4.1.11 Ответственность за ведение учета технических СЗИ возлагается на Ответственного за обеспечение безопасности ПДн.

4.2 Тестирование функций системы защиты ПДн

4.2.1 Тестирование функций системы защиты должно осуществляться периодически и на основании раздела 5 настоящего Положения.

4.2.2 Ответственность за тестирование функций системы защиты ПДн возлагается на Ответственного за обеспечение безопасности ПДн.

4.3 Учет электронных носителей ПДн

4.3.1 В Компании должен проводиться учет защищаемых электронных носителей ПДн. К защищаемым электронным носителям ПДн относятся следующие:

- носители информации серверов;

- носители информации автоматизированных рабочих мест (далее АРМ);

- ленты с резервными копиями;

- внешние запоминающие устройства (дискеты, флеш-накопители и т. п.), содержащие ПДн.

4.3.2 Форма учета защищаемых электронных носителей приведена в приложении (Приложение Б)
.

4.3.3 Ответственность за учет защищаемых электронных носителей ПДн возлагается на Ответственного за обеспечение безопасности ПДн.

5. Организация внутреннего контроля обработки и обеспечения безопасности ПДн

5.1 Цели организации внутреннего контроля

5.1.1 Организация внутреннего контроля процесса обработки ПДн в Компании осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

5.1.2 Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

- обеспечение соблюдения работниками Компании требований настоящего Положения и нормативных правовых актов, регулирующих защиту ПДн;

- оценка компетентности персонала, задействованного в обработке ПДн;

- обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

- выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

- принятие корректирующих мер, направленных на устранение выявленных нарушений как в порядке обработки ПДн, так и в работе технических средств ИСПДн;

- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

- осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

5.2 Проведение контрольных мероприятий

5.2.1 Ответственный за обеспечение безопасности ПДн на периодической основе организует проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн.

5.2.2 Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости внепланово. План мероприятий приведен в приложении (Приложение В).

5.2.3 Решение о необходимости проведения внеплановых контрольных мероприятий принимает Ответственный за обеспечение безопасности ПДн в Компании. Данное решение должно быть

обосновано возросшими рисками информационной безопасности для обрабатываемых ПДн и при существенных изменениях в среде обработки ПДн.

5.2.4 Плановые проверки включают в себя как минимум следующие типы проверок:

- проверка деятельности работников Компании, допущенных к работе с ПДн в ИСПДн на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, Положением о порядке обработки ПДн и другими внутренними документами;

- проверка правильности приема и обработки обращений и запросов субъектов ПДн или их представителей;

- проверка работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн;

- проверка ведения эталонных копий средств защиты;

- проверка ведения копий ПДн;

- проверка соответствия предоставленных прав доступа пользователей к ПДн утвержденной матрице доступа;

- проверка минимальной длины и сложности паролей;

- проверка периодичности смены паролей;

- проверка отсутствия на АРМ пользователей средств разработки;

- проверка отсутствия на АРМ пользователей нештатного программного обеспечения.

5.2.5 Ответственный за обеспечение безопасности ПДн составляет план контрольных мероприятий на полугодие, в котором определяет состав и периодичность проведения проверок на данный период времени.

5.2.6 План контрольных мероприятий утверждает Ответственный за организацию обработки ПДн в Компании.

5.2.7 Все результаты проверок должны быть предоставлены в виде Актов Ответственному за организацию обработки ПДн для проведения анализов результатов и подготовки соответствующего Отчета о проведении внутреннего контроля обработки и обеспечения безопасности ПДн. Форма Акта приведена в приложении (Приложение Г).

5.2.8 Выявленные в ходе проверок нарушения, а также отметки об их устранении, фиксируются в Журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности ПДн. Форма Журнала приведена в приложении (Приложение Д).

5.2.9 Выявленные нарушения расследуются в соответствии с разделом 7 данного Положения.

5.2.10 При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационной безопасности.

6. Порядок проведения разбирательств по фактам нарушений порядка обработки и защиты ПДн

6.1 Инициирование процесса разбирательства

Проведение разбирательств может быть инициировано в одном из следующих случаев:

- обращение субъекта ПДн по поводу неправомерных действий с его ПДн;

- выявление нарушений сотрудниками Компании в рамках выполнения своих должностных обязанностей, связанных с обработкой или защитой ПДн;

- выявление нарушений, приводящих к снижению уровня защищенности ПДн, в ходе проведения проверок состояния защищенности ПДн.

6.2 Проведение расследования

6.2.1 В ходе проведения расследования Ответственным за обеспечение безопасности ПДн проводится опрос очевидцев и подозреваемых лиц, предположительно допустивших нарушение.

6.2.2 В ходе проведения опроса выясняется:

- дата и время совершения нарушения;

- обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

- последствия, возникшие вследствие совершения нарушения.

6.2.3 Все опрашиваемые лица должны предоставить объяснительные записки (заявления) (показания, изложенные на бумажном носителе с подписью опрашиваемого).

6.2.4 Ответственный за обеспечение безопасности ПДн оценивает последствия, возникшие вследствие совершения нарушения.

6.3 Формирование заключения по результатам разбирательств

6.3.1 По результатам разбирательства Ответственный за обеспечение безопасности ПДн в течение трех рабочих дней составляет заключение по результатам разбирательств (далее Заключение).

6.3.2 В Заключении должны быть приведены:

- краткая справка по нарушению, в отношении которого проводилось разбирательство;

- лицо(а), которое совершило нарушение;

- предложения по привлечению виновника к юридической ответственности (дисциплинарной ответственности (замечание, выговор, увольнение) или к гражданско-правовой ответственности (взыскание причиненного ущерба)) и (или) применению к нему мер дисциплинарного воздействия (депремирование, указание на недостатки и т. п.);

- план мероприятий по предотвращению подобных нарушений.

6.3.3 Форма Заключения приведена в приложении (Приложение Е).

6.3.4 Заключение предоставляется Ответственному за организацию обработки ПДн.

7. Ответственность

7.1 В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Компании, ее работникам и посетителям материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

7.2 Ответственный за обеспечение безопасности ПДн несет ответственность за:

- организацию проведения проверочных мероприятий;

- непредвзятое проведение разбирательств по фактам нарушений порядка защиты ПДн;

- ведение учета технических СЗИ;

- тестирование функций системы защиты ПДн;

- учет защищаемых электронных носителей ПДн.

7.3 Ответственный за организацию обработки ПДн несет ответственность за непредвзятое проведение разбирательств по фактам нарушений порядка обработки ПДн.

8. Перечень терминов

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

Администратор информационной системы персональных данных работник Управления информационных технологий ЗАО "Сбербанк Лизинг", осуществляющий сопровождение программных и аппаратных компонентов информационной системы персональных данных в процессах внедрения, эксплуатации и вывода из эксплуатации и техническую поддержку пользователей системы.

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

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

Контролируемая зона территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Конфиденциальность персональных данных обязательное требование для операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Координатор по обращениям и запросам работник ЗАО "Сбербанк Лизинг", отвечающий за обработку обращений и запросов субъектов персональных данных и уполномоченного органа по защите прав субъектов персональных данных, сбор сведений и составление ответов на обращения и запросы в законодательно установленные сроки.

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.

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. В настоящем Положении под Оператором понимается ЗАО "Сбербанк Лизинг".

Ответственный за обеспечение безопасности персональных данных работник ЗАО "Сбербанк Лизинг", осуществляющий мероприятия по организации защиты персональных данных.

Ответственный за организацию обработки персональных данных работник ЗАО "Сбербанк Лизинг", подотчетный исполнительному органу ЗАО "Сбербанк Лизинг" и отвечающий за соблюдение Компанией и ее работниками законодательства Российской Федерации о персональных данных.

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

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

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

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

Приложение А. Форма журнала учета технических СЗИ

Форму журнала учета технических СЗИ смотри в файле Приложение А.doc.

Приложение Б. Форма журнала учета защищаемых электронных носителей

Форму журнала учета защищаемых электронных носителей смотри в файле Приложение Б.doc.

Приложение В. План внутренних проверок состояния защиты ПДн

План внутренних проверок состояния защиты ПДн смотри в файле Приложение В.doc.

Приложение Г. Форма акта о результатах проведения проверки

Форму акта о результатах проведения проверки смотри в файле Приложение Г.doc.

Приложение Д. Форма журнала учета выявленных нарушений в порядке обработки и обеспечения безопасности ПДн

Форму журнала учета выявленных нарушений в порядке обработки и обеспечения безопасности ПДн смотри в файле Приложение Д.doc.

Приложение Е. Форма заключения о проведении разбирательства

Форму заключения о проведении разбирательства смотри в файле Приложение Е.doc.