УТВЕРЖДЕНО
Правлением ООО БАНК «КУРГАН»
Протокол № 21 от «30» июня 2020 года
Председатель Правления

_____ А.О. Лушников

ПОЛОЖЕНИЕ
о защите персональных данных в ООО БАНК «КУРГАН»

г. Курган
2020

Содержание

1. Общие положения

Настоящее Положение устанавливает применяемые в ООО БАНК «КУРГАН» (далее – Банк) способы обеспечения безопасности при сборе, записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), извлечении, использовании, передачи (распространение, предоставление, доступ), блокировании, удалении, уничтожении персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные.

1.1. Настоящее Положение разработано на основании:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационно-технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. В соответствии с законодательством РФ под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.3. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное исполнение для соблюдения должностными лицами Банка, допущенными к обработке персональных данных, не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.4. Обеспечение конфиденциальности персональных данных не требуется в случае:

– обезличивания персональных данных;

– обработки общедоступных персональных данных.

1.5. Перечень информационных систем, обрабатывающих персональные данные, и список ответственных за хранение и обработку персональных данных сотрудников Банка, либо имеющих к ним доступ, утверждается приказом по Банку.

1.6. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных, Банк предоставляет сотрудникам, допущенным к обработке персональных данных, необходимые условия для выполнения указанных требований:

– знакомит работника под подпись с требованиями «Политики ООО БАНК «КУРГАН» в отношении обработки персональных данных» (далее – Политика), с настоящим «Положением о защите персональных данных» (далее – Положение), с должностной инструкцией и иными внутренними нормативно-распорядительными документами Банка в сфере обеспечения конфиденциальности и безопасности персональных данных, а также другой информации ограниченного доступа;

– предоставляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);

– обучает правилам эксплуатации средств защиты информации;

– проводит иные необходимые мероприятия.

1.7. Без согласования с ответственным за организацию обработки персональных данных в Банке, формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих информацию ограниченного доступа, запрещается.

1.8. Должностные лица Банка, допущенные к обработке персональных данных, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

1.9. При прекращении выполнения трудовых функций, связанных с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, материальные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

1.10. Передача персональных данных третьим лицам допускается только с согласия субъекта персональных данных или в случаях, предусмотренных действующим законодательством РФ, в соответствии с Политикой, настоящим Положением, «Правилами обработки персональных данных в ООО БАНК «КУРГАН» (далее – Правила), должностными инструкциями и иными локальными нормативными актами Банка.

1.11. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной настоящим Положением форме (Приложение № 1).

1.12. Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.13. Должностные лица Банка, допущенные к обработке персональных данных, обязаны немедленно сообщать своему непосредственному руководителю и (или) ответственному за организацию обработки персональных данных обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

1.14. Должностные лица, допущенные к обработке персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

1.15. Отсутствие контроля со стороны Банка за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством РФ ответственности.

2. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой без использования средств автоматизации

2.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение

персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2.2. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

– определяет места хранения персональных данных (материальных носителей);

– осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

– совместно с ответственным за организацию обработки персональных данных в Банке, информирует лиц, допущенных к обработке персональных данных без использования средств автоматизации, о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

– организует раздельное, т.е. не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

2.2.1. Ответственный за организацию обработки персональных данных, осуществляет:

– проверку соответствия обработки персональных данных нормативно-распорядительным документам Банка;

– расследования при инцидентах информационной безопасности;

– консультации и обучение сотрудников Банка правилам обработки ПДн;

– учёт мест хранения ПДн и сотрудников, допущенных к обработке ПДн;

– общую организацию работ по защите ПДн и другой информации ограниченного доступа.

2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации, должен принять меры по обеспечению раздельной обработки персональных данных:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим

дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации, производится путем обновления или изменения данных на материальном носителе. Если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой с использованием средств автоматизации

3.1. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в локальной компьютерной сети Банка (далее – ЛКС).

Безопасность персональных данных при их обработке в ЛКС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ЛКС информационные технологии.

3.2. Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.3. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется только после ознакомления с «Положением о порядке обращения с информацией ограниченного доступа в ООО БАНК «КУРГАН» и подписания прилагаемого к нему «Обязательства о неразглашении защищаемой информации» (Приложение № 2).

Работа с персональными данными осуществляется в соответствии с Политикой, Правилами, «Инструкцией пользователя по соблюдению режима информационной безопасности», должностными инструкциями и другими внутренними нормативными документами Банка.

3.4. Работа с персональными данными должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в помещениях, где ведется обработка персональных данных, посторонних лиц.

3.5. Компьютеры, через которые сотрудники получают доступ к базам данных информационных систем с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 8 и более символов. Работа на компьютерах без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается. Запрещается хранить пароли в свободном доступе.

3.6. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.7. При обработке персональных данных пользователями должно быть обеспечено:

– постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.8. При обработке персональных данных в информационных системах, ответственным за организацию обработки персональных данных и администраторами безопасности информационных систем, должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые на рабочей станции, правилам работы с ними;

– учет лиц, допущенных к работе с персональными данными, прав и паролей доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, материальными носителями и их утилизации

4.1. Все находящиеся на хранении и в обращении в Банке машинные носители (жёсткие диски, CD/DVD диски), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер или серийный номер при наличии.

4.2. При работе со съемными носителями, содержащими персональные данные, запрещается:

– хранить электронно-оптические носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить электронно-оптические носители с персональными данными из служебных помещений для работы за пределами территории Банка, дополнительного офиса или ОКВКУ.

4.3. При отправке или передаче персональных данных адресатам на электронно-оптические носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на машинных носителях осуществляется в порядке, установленном Политикой, Правилами и другими внутренними документами Банка.

Передача машинных носителей с персональными данными для непосредственной передачи адресату, осуществляется по письменному разрешению председателя Правления Банка и согласованию с ответственным за организацию обработки персональных данных в соответствии с п.1.11 настоящего Положения.

4.4. О фактах утраты машинных и материальных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено ответственному за организацию обработки персональных данных и руководителю структурного подразделения. Для проведения расследования обстоятельств произошедшего, приказом по Банку создается комиссия, по результатам расследования составляется акт и делаются соответствующие отметки в Журнале (Приложение № 5 Политики).

4.5. Машинные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей с информацией ограниченного доступа осуществляется комиссией, созданной приказом председателя Правления Банка.

По результатам уничтожения носителей составляется акт по форме, определенной в Политике (Приложение № 6 Политики).

5. Контроль изменений в составе и структуре информационных систем персональных данных

Все изменения в составе и структуре информационных систем персональных данных (далее – ИСПДн) должны контролироваться, и подлежат регистрации в электронном журнале регистрации работ в ИСПДн (Приложение 2). Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

– изменение мест включения существующих компонент ИСПДн;

– удаление устройства из состава ИСПДн;

– изменение мест установки устройства из состава ИСПДн;

– прокладка новых кабельных линий связи структурированной кабельной сети и внешних линий связи или удаление старых кабельных линий связи;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

– создание новых и изменение существующих технологических процессов, связанных с обработкой ПДн.

Все потенциальные изменения оцениваются с точки зрения возможных негативных последствий на эксплуатацию системы и ее функциональность. Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация средств защиты ПДн.

6. Защита от несанкционированного физического доступа к элементам ИСПДн

Мероприятия по физическому контролю доступа включают:

– мероприятия по контролю доступа на территорию Банка;

– мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

– мероприятия по контролю доступа к техническим средствам ИС;

– мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа должны обеспечить контролируемое нахождение посетителей на территории Банка.

Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн, должны иметь прочные входные двери с механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время и приспособлениями для опечатывания или внутренней сигнализацией. Двери должны быть постоянно закрыты и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в помещении посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающего персонала, других сотрудников), должно осуществляться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

При выносе устройств, хранящих ПДн, за пределы контролируемой зоны для ремонта, замены и других работ, должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

В отношении некоторых ИСПДн возможны дополнительные, либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз и нарушителя, а также технического задания на создание средств защиты персональных данных. Мероприятия по защите таких ИСПДн определяются эксплуатационной (проектной) документацией.

7. Резервирование ПДн

Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

Во внутренних документах, утвержденных Правлением Банка, описаны процессы резервирования и учтены следующие вопросы:

– порядок резервирования;
– ответственные за резервирование;
– порядок восстановления информации после аварий;
– порядок хранения резервных копий.

Резервированию должна подвергаться информация, хранящаяся на машинных носителях ИСПДн. Резервирование должно осуществляться на носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий на машинных носителях, должно осуществляться в хранилищах, имеющих замок, а само хранилище должно располагаться в помещении с сигнализацией. Хранение (по возможности) должно осуществляться в месте, удаленном от основного хранилища информации.

Резервирование осуществляется в соответствии с Порядком резервного копирования.

8. Контроль за обеспечением необходимого уровня защищенности ПДн

Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

– контроль за соблюдением требований по обработке и защите персональных данных;
– контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
– контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

– текущими;
– внезапными;
– плановыми внешними;
– плановыми внутренними.

Ответственность за текущий контроль и плановый контроль эффективности обеспечения безопасности ПДн возлагается на отдел информационной безопасности. Данный контроль должен включаться в план мероприятий по обеспечению информационной безопасности на год.

Для планового контроля эффективности средств защиты персональных данных должны проводиться проверки на своевременность обновления, правильность работы, в соответствии с заданными настройками.

Внезапные проверки эффективности, при необходимости, могут проводиться по решению начальника отдела информационной безопасности или на основании жалоб сотрудников Банка при подозрении на неправильную работу информационных систем.

При проведении контроля эффективности в общем случае должно проверяться:

– наличие установленных средств защиты информации;
– корректность настроек средств защиты информации;

– выполнение пользователями и администраторами требований внутренних документов Банка по защите ПДн;

– исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);

– правильность организации работы с носителями ПДн;

– правильность обращения ключевой информации;

– соответствие системы защиты ПДн реальному положению дел в Банке.

9. Реагирование на нештатные ситуации

Для эффективного реагирования на нештатные ситуации, возникающие при обработке ПДн, в Банке регламентированы следующие вопросы:

– порядок определения нештатной ситуации;

– порядок оповещения сотрудников при возникновении различных нештатных ситуаций;

– порядок действий по нейтрализации нештатных ситуаций, сведения их негативных последствий к минимуму.

На основании разработанного Плана ОНиВД[1], регулярно (не реже 1 раз в 2 года), проверяется порядок действий сотрудников в случае возникновения нестандартных и чрезвычайных обстоятельств посредством проведения проверки (тестирования) с корректировкой порядков по результатам проведенного тестирования.

В Банке проводятся расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями, все инциденты регистрируются в Журнале регистрации событий информационной безопасности. По результатам расследования инцидентов разрабатываются методики противодействия.

В рамках данного процесса должны решаться следующие задачи:

– расследование инцидентов, связанных с безопасностью ПДн;

– ликвидация последствий инцидентов связанных с безопасностью ПДн;

– принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Реагирование на нештатные ситуации должно производиться в соответствии с «Порядком обнаружения, регистрирования и реагирования на инциденты ИБ в ООО БАНК «КУРГАН».

10. Контроль лояльности персонала

В Банке проводится комплекс мероприятий, направленных на исключение присутствия злоумышленников среди администраторов и ответственного за организацию обработки персональных данных, а также возможность сговора двух и более злоумышленников. Комплекс мероприятий включает, в том числе:

– периодические проверки на лояльность;

– периодический мониторинг действий персонала.

Мероприятия по обеспечению безопасности персонала должны обеспечить невозможность злоумышленного сговора двух или более сотрудников Банка. Проверки должны выполняться как в скрытом, так и в явном режиме. При приеме на работу должна проводиться проверка идентичности личности и подлинности документа, удостоверяющего личность, а также документа об образовании.

---

[1] План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности ООО БАНК «КУРГАН» в случае возникновения нестандартных и чрезвычайных ситуаций обстоятельств.

11. Организация работы с носителями ПДн

Порядок организации работы с носителями, содержащими ПДн, должен соответствовать следующим требованиям:

– использование, хранение, передача, копирование, уничтожение носителей, содержащих персональные данные;
– систематизация носителей, содержащих персональные данные;
– подготовка носителей, содержащих персональные данные для передачи их в архив;
– подготовка носителей, содержащих персональные данные для их уничтожения;
– проверка наличия носителей, содержащих персональные данные;
– распечатка ПДн.

В «Правилах работы с персональными данными» регламентирован порядок работ с ПДн для документов на следующих носителях:

– бумажных носителях;
– машинных съемных носителях;
– машинных несъемных носителях, используемых в технических средствах ИСПДн.

12. Заключительные положения.

12.1. Настоящее Положение вступает в силу с 01.07.2020 года.

12.2. С даты вступления в силу настоящего Положения считать утратившим силу «Положение по защите персональных данных в БАНК «КУРГАН» ПАО», утверждённое Правлением Банка 07.09.2016 (протокол № 55).

Приложение 1

Форма

АКТ
передачи персональных данных третьим лицам

г. Курган «__»_____20__г.

_____
(ФИО, должность сотрудника)
передал(а) следующие документы, содержащие персональные данные

_____:
(ФИО клиента)

_____
(перечислить наименования передаваемых документов, содержащих персональные данные)
по запросу

_____
(номер, дата запроса, наименование организации)
с целью

_____.

_____ _____
подпись передающего ФИО, должность передающего

Согласовано:
Ответственный за организацию обработки персональных данных

_____ _____
подпись ФИО, должность ответственного

Документы, содержащие персональные данные принял(а), экземпляр акта получил(а):

_____
(ФИО, должность, получившего данные)

_____ _____
подпись расшифровка подписи

«____»_____ 202__ г.

Форма
Приложение 2

ЖУРНАЛ
УЧЕТА ПРОВОДИМЫХ РАБОТ В ИСПДн

Ответственный за ведение Журнала /_____/
Начат «___» _____20____г.
Окончен «___» _____20____г.

№	Дата	Вид работ	Наименование ИСПДн	ФИО проводившего работы	№ Пломбы	Замечания