УТВЕРЖДЕНО
Правлением АКБ «МАЙКОПБАНК» (ЗАО)
протокол №10 от 15.03.2013г.
_____ Люленкова Л.Г.

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в АКБ «МАЙКОПБАНК» (ЗАО)

Майкоп 2013

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», требованиями комплекса БР ИББС и устанавливает единый порядок обработки персональных данных в АКБ «МАЙКОПБАНК» (ЗАО) (далее – банк).

1.2. В целях настоящего Положения используются следующие термины и понятия:

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- 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;
- информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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;
- информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

1.3. Состав, цели, сроки обработки и хранения персональных данных указаны в «Перечне персональных данных, обрабатываемых в АКБ «МАЙКОПБАНК» (ЗАО)».

2. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных производится при наличии:

- согласия субъекта персональных данных, составленного по форме согласно приложениям 1а, 1б, 1в, 1г, 1д к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона 152-ФЗ;
- принятия необходимых мер по защите персональных данных.

Согласие на обработку персональных данных заполняется субъектом персональных данных по форме Банка в присутствии уполномоченного сотрудника Банка.

Фамилия, имя, отчество, паспортные данные и место регистрации могут быть указаны субъектом персональных данных собственноручно, либо заполнены сотрудником Банка с помощью программных средств.

Субъект персональных данных проставляет знак «√ » напротив целей для достижения которых предоставлено согласие на обработку персональных данных.

В конце согласия (в нижней части) субъект персональных данных собственноручно проставляет дату предоставления согласия, свою подпись и указывает свои фамилию и инициалы.

Согласие на обработку персональных данных помещается в юридическое либо кредитное дело субъекта персональных данных, которое первым оформлено во исполнение целей для которых предоставлено согласие, либо прилагается к иному документу (созданному либо исполненному Банком) в котором содержатся персональные данные.

Согласие на обработку персональных данных сотрудников банка помещается в их личное дело.

2.2. Для защиты персональных данных используется следующий ряд мер:

- определение перечня персональных данных, обрабатываемых в Банке;
- утверждение перечня должностей и должностных лиц, осуществляющих обработку персональных данных без использования средств автоматизации;
- доведение до сведения должностных лиц порядка обработки, в том числе хранения и использования персональных данных;
- разработка типовых форм документов, в которых содержатся персональные данные, с определением цели их обработки
- пропускной режим банка;
- учет и порядок выдачи пропусков;
- технические средства охраны, сигнализация и видео-наблюдение (все помещения банка снабжены средствами сигнализации для предотвращения несанкционированного доступа);
- порядок охраны территории, зданий, помещений;
- резервное копирование.

2.3. Дополнительные меры для обеспечения внутренней защиты персональных данных:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключается бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение состава работников, имеющих право доступа (входа) в помещение, в котором находится электронные базы данных АБС банка;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- ограничение и регламентация состава работников, в функциональные обязанности которых входит обработка персональных данных;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты сведений при работе с конфиденциальными документами;

2.4. Защита сведений, хранящихся в электронных базах данных АБС банка, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается разграничением прав доступа с использованием учетной записи и системой паролей.

Система управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю.

2.5. В банке приказом председателя Правления назначаются сотрудники: ответственные за защиту персональных данных, обрабатываемых без использования средств автоматизации, и персональных данных, обрабатываемых с использованием средств автоматизации, а также определяется перечень лиц, допущенных к обработке персональных данных.

2.6. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении конфиденциальной информации, содержащей персональные данные, по форме согласно приложению 1 к Перечню сведений конфиденциального характера в АКБ «МАЙКОПБАНК» (ЗАО).

2.7. Сотрудникам запрещается:
- осуществлять ввод персональных данных под диктовку;
- отвечать на вопросы, связанные с передачей персональной информации по телефону или передавать их факсу или электронной почте.

3. ОРГАНИЗАЦИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ В БАНКЕ

3.1. Доступ сотрудников банка к персональным данным, обрабатываемым в банке.

3.1.1. Право доступа к персональным данным (без специального разрешения) имеют:
- председатель Правления;
- зам.председателя Правления;
- руководители структурных подразделений по направлению деятельности и к личным данным сотрудников своего подразделения;
- сотрудники банка при выполнении ими своих служебных обязанностей и к персональным данным, относящимся непосредственно к ним (личное дело).

3.1.2. Сотрудник банка имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Сотрудник имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

3.1.3. Сотрудникам банка предоставляется доступ к работе с персональными данными (не относящимся к ним) исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей и в соответствии с порядком, установленным настоящим Положением, а также в соответствии со следующими документами:
- План защиты автоматизированной банковской системы АКБ «МАЙКОПБАНК» (ЗАО) от несанкционированного доступа к информации и незаконного вмешательства в процессе ее функционирования;
- Инструкция по организации парольной защиты автоматизированной системы, утверждено Председателем Правления АКБ «МАЙКОПБАНК» ЗАО;
- Инструкция пользователю автоматизированной системы.

3.1.4. Сотрудники банка, которые в силу выполняемых служебных обязанностей постоянно работают с персональными данными, получают допуск к необходимым категориям персональных данных с установленными правами доступа на срок выполнения ими соответствующих должностных обязанностей, что должно быть отражено в Журнале лиц, допущенных к работе с персональными данными (см. Приложение 2 к настоящему Положению).

Должностные лица банка, имеющие доступ к персональным данным, при их обработке

должны обеспечивать конфиденциальность этих данных.

В случае замещения какой-либо должности замещающий сотрудник получает право доступа к персональным данным соответствующее замещаемой должности.

3.1.5. Временный или разовый допуск к работе с ПДн сотрудника банка в связи со служебной необходимостью может быть получен сотрудником банка на основании приказа Председателя Правления, путем подачи заявки на доступ с указанием цели и срока доступа.

Доступ к ПДн может быть прекращен или ограничен в случае нарушения требований настоящего Положения и Плана защиты автоматизированной банковской системы АКБ «МАЙКОПБАНК» (ЗАО) от несанкционированного доступа к информации и незаконного вмешательства в процессе ее функционирования, либо в случае перевода или увольнения сотрудника.

3.2. Порядок доступа в помещения, в которых ведется обработка персональных данных, регламентируется Правилам пропускного режима в АКБ «МАЙКОПБАНК» (ЗАО), утвержденным Правлением АКБ «МАЙКОПБАНК» (ЗАО), протокол № 4 от 12 февраля 2010г.

3.3. Доступ к персональным данным со стороны внешних организаций и лиц, не являющихся сотрудниками банка.

3.3.1. Право доступа к персональным данным имеют:

- сам субъект персональных данных, к данным относящимся непосредственно к нему;
- налоговые органы;
- правоохранительные органы;
- Росфинмониторинг;
- органы статистики;
- организации осуществляющие страховую деятельность;
- военкоматы;
- органы социального и медицинского страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления, в случаях предусмотренным действующим законодательством;

3.3.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

3.3.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

3.3.4. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника о согласии на передачу персональных данных.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК РФ).

3.4. Передача персональных данных третьему лицу осуществляется банком с согласия субъекта персональных данных, за исключением случаев, когда в соответствии с законодательством такое согласие не требуется.

При передаче банком персональных данных третьему лицу на обработку на основании договора, в договор следует включать обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

3.5. Передача документов (иных материальных носителей), содержащих персональные данные работников банка, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Банку;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных работника;
- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

4. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

4.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации банка осуществляется в соответствии с требованиями отраслевого Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» серии СТО БР ИББС, введенным в действие распоряжением Банка России от 21 июня 2010 г. № Р-705 и согласованным с ФСТЭК России, ФСБ России и Роскомнадзором, а также требованиями постановления Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», внутренних нормативных документов банка.

4.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:
- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

5. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

5.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

5.2. При обработке в банке персональных данных на бумажных носителях, в частности, при использовании в банке типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008г. № 687.

5.3. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.4. При неавтоматизированной обработке персональных данных на бумажных носителях:
- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

5.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы),

должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, наименование и адрес банка, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых банком способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.6. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

5.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

5.8. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению За к настоящему Положению. Для учета электронных носителей, содержащих списки на зачисление денежных средств, заполняется журнал по форме согласно приложению 3б к настоящему Положению.

5.9. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

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;

6. ПОРЯДОК ХРАНЕНИЯ МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Хранение персональных данных субъектов осуществляется структурными подразделениями банка на бумажных и электронных носителях в служебных помещениях (в соответствии с приложением 4), при организации ограниченного доступа к ним и условий, обеспечивающих их сохранность.

6.2. Персональные данные сотрудников банка обрабатываются кадровой службой и бухгалтерией. Ответственным за хранение личных дел сотрудников банка является старший инспектор по кадрам.

Личные дела сотрудников хранятся в бумажном виде в папках, в специальном сейфе.

Личные дела, помещенные в архив, хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам, скрепленные печатями, в металлическом шкафу.

6.3. Персональные данные Клиента хранятся в его личном досье, которое ведется сотрудником, работающим с этим Клиентом.

Досье Клиентов[1], журналы и книги учета, содержащие персональных данные, хранятся в рабочее и нерабочее время в закрытых шкафах. Сотрудникам банка не разрешается при выходе из помещения оставлять какие-либо документы, содержащие персональные данные, на рабочем столе или оставлять шкафы открытыми, оставлять компьютер, не активировав блокировку клавиатуры.

На рабочем столе сотрудника должен всегда находиться только тот пакет документов и учетных карточек, с которым в настоящий момент он работает. Другие документы, дела, карточки, журналы должны находиться в закрытом шкафу. Исполняемые документы не разрешается хранить в россыпи, их следует помещать в папки.

В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны в шкафы, сейфы. На рабочем столе не должно оставаться ни одного документа (содержащего персональные данные). Черновики документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются, путем измельчения.

Личные дела клиентов, помещенные в архив, хранятся в бумажном виде в папках, сгруппированные в пачки по годам, в металлическом шкафу.

6.4. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он передает документы и иные носители, содержащие персональные данные работников лицу, на которое приказом, будет возложено исполнение его трудовых обязанностей.

6.5. Персональные данные на электронных носителях (резервные копии, дискеты со списками на зачисление заработной платы) должны храниться в сейфах. При использовании сотрудниками электронных носителей, в процессе выполнения своих служебных обязанностей, электронные носители с содержащимися на них персональными данными не должны оставаться без внимания сотрудника и быть доступны другим лицам.

6.6. Рабочие электронные базы данных автоматизированной банковской системы расположены в помещении ОАБО, в нерабочее время помещение опечатывается, в рабочее время доступ в помещение ограничен.

6.7. Контроль выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных возложен на начальников структурных подразделений банка.

6.8. Начальник структурного подразделения в конце рабочего дня должен убедиться, что подчиненные не оставили на своих рабочих столах документов, АРМ сотрудников выключены, шкафы с документами закрыты.

6.9. Не реже 1 раза в полугодие сотрудники ОАБО проверяют компьютеры сотрудников на установление фактов изменения их конфигурации.

6.10. Во вне рабочее время помещения банка закрываются и ставятся под охрану на центральный пульт Частного охранного предприятия, который осуществляет охрану помещений на основании заключенного договора и отвечает за контроль физического доступа, который организован следующим образом:

- помещения банка оборудованы системами автоматической пожарной сигнализации и комплексом технических средств охраны (тревожной сигнализации) с подачей соответствующих сигналов на пульт централизованной охраны банка;
- контроль доступа в здание банка и в его помещения организован при помощи системы видеонаблюдения, которая выведена на круглосуточный пост охраны.

7. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

7.2. Банк прекращает обработку персональных данных и уничтожает собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

[1] Под досье Клиента понимается юридическое дело Клиента либо кредитное досье Клиента.

- о достижении целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
- при невозможности устранения банком допущенных нарушений при обработке персональных данных.

7.3. Банком используются следующие способы уничтожения персональных данных:
- Физическое уничтожение материального носителя:
- Уничтожение информации (содержащей персональные данные) с носителя

7.4. Уничтожение материального носителя.
- Бумажный носитель. Банком используется 2 вида уничтожения: уничтожение через измельчение (допускается только при уничтожении черновиков документов, испорченных бланков и листов со служебными записями) и уничтожение бумажных носителей персональных данных через термическую обработку (сжигание).
- Электронный носитель. Уничтожение заключается в воздействии на рабочие слои дисков или других накопителей, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя.

7.5. Уничтожение информации с носителя.

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.

При этом способе уничтожения персональных данных сам носитель не уничтожается, а уничтожается только информация, содержащая персональные данные. Использоваться следующие методы уничтожения информации с носителя:
- форматирование носителя с гарантированным уничтожением данных (без возможности их восстановления);
- уничтожение конкретной информации с носителя, при помощи специализированных программных средств, без возможности восстановления данных.

7.6. Для уничтожения материальных носителей создается комиссия (в составе трех человек) производится уничтожение и составляется Акт об уничтожении материальных носителей персональных данных (см. приложение 5)

Акт составляется раздельно на каждый способ уничтожения носителей.

Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

При уничтожении бумажных носителей путем измельчения комиссия не собирается.

7.7. Ответственным за уничтожение персональных данных с электронных носителей является сотрудник ответственный за защиту персональных данных, обрабатываемых с использованием средств автоматизации.

8. ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИЛИ ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) ПО ВОПРОСАМ ОБРАБОТКИ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАК ЖЕ ДЕЙСТВИЙ В СЛУЧАЕ ЗАПРОСОВ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИНЫХ НАДЗОРНЫХ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ КОНТРОЛЬ И НАДЗОР В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Субъект персональных данных имеет право на получение сведений о банке, о месте его нахождения, о наличии у банка персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 ФЗ № 152. Субъект персональных данных вправе требовать от банка уточнения своих персональных данных, их блокирования или

уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2. Сведения о наличии персональных данных предоставляются субъекту персональных данных банком в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

8.3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю банком при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

8.4. Граждане (субъекты персональных данных) по вопросам обработки персональных данных обращаются к юрисконсульту банка, о чем последний делает отметку в соответствующем журнале (по форме предусмотренной приложением 6).

8.5. Субъект персональных данных имеет право на получение при обращении или при направлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных банком, а также цель такой обработки;
- способы обработки персональных данных, применяемые банком;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

8.6. Банк сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с ними непосредственно при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

8.7. Банк обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет банк, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах банк обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

8.8. Банк сообщает в уполномоченный орган по защите прав субъектов персональных данных или иные надзорные органы, осуществляющие контроль и надзор в области персональных данных, по их запросу информацию, необходимую для осуществления деятельности указанных органов, в течение семи рабочих дней с даты получения такого запроса.

9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В РАМКАХ БАНКОВСКИХ ПЛАТЕЖНЫХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ И В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКА

9.1. Правовая основа обеспечения безопасности обработки персональных данных в АС

9.1.1. В соответствии с требованиями Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных» банк принимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Настоящая глава определяет подход АКБ «МАЙКОПБАНК» (ЗАО) к обеспечению безопасности обработки персональных данных в автоматизированной банковской системе.

При установлении требований к обеспечению безопасности персональных данных банк руководствуется отраслевым Комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» серии СТО БР ИББС, введенным в действие распоряжением Банка России от 21 июня 2010г. № Р-705 и согласованным с ФСТЭК России, ФСБ России и Роскомнадзором. В настоящей главе используются термины и определения Стандарта Банка России СТО БР ИББС-1.0-2010.

Перечень сведений, составляющих персональные данные, а также цели и сроки их обработки банком зафиксированы в документе «Перечень персональных данных, обрабатываемых в банке.

9.1.2. Для выбора и реализации методов и способов защиты информации в АС банка председателем Правления назначается лицо ответственное за обеспечение безопасности персональных данных, также может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

9.1.3. Обработка персональных данных в АС банка происходит как в информационных системах персональных данных (ИСПДн), так и АБС, реализующие банковские платежные технологические процессы.

К ИСПДн банк относит АБС, целью создания и использования которых является обработка персональных данных. При этом к ИСПДн так же могут быть отнесены и другие АБС по усмотрению банка.

9.1.4. Выбор и реализация методов и способов защиты информации в информационной системе банка осуществляются на основе «Отраслевой частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ» (далее — Отраслевая модель угроз) определенной стандартом РС БР ИББС-2.4-2010, и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008г. № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008г., регистрационный № 11462).

9.1.5. В соответствии со стандартом СТО БР ИББС_1.0 все ИСПДн банка относятся к специальным. ИСПДн банка классифицируются на основе категорий обрабатываемых в ИСПДн персональных данных. Выделяются следующие основные классы ИСПДн:

- ИСПДн_С - ИСПДн обработки специальных категорий персональных данных (далее – ИСПДн 1 класса);
- ИСПДн_Б - ИСПДн обработки биометрических персональных данных (далее – ИСПДн 2 класса);
- ИСПДн_И - ИСПДн обработки персональных данных, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным (далее – ИСПДн 3 класса);
- ИСПДн_Д - ИСПДн обработки общедоступных и (или) обезличенных персональных данных (далее – ИСПДн 4 класса).

Банком не используются ИСПДн 1 и 2 классов.

9.1.6.- В целях поддержания на должном уровне системы обеспечения информационной безопасности (СОИБ) банком принята «Методика оценки нарушения рисков информационной безопасности» РС БР ИББС-2.2-2009, утвержденная ЦБ РФ 01.01.2010г.

Данная методика устанавливает способы и порядок проведения оценки рисков нарушения ИБ в банке, и является составной частью системы менеджмента ИБ (СМИБ) банка.

Оценка рисков нарушения ИБ проводится СВК и/или ОЭА и ДО (совместно с администратором ИБ), в рамках построения/совершенствования системы обеспечения информационной безопасности (СОИБ) банка. О результатах оценки рисков нарушения ИБ составляются периодические отчеты и предоставляются председателю Правления.

Деятельность по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ относится к компетенции комиссии состоящей из руководителя СВК, администратора ИБ и лиц ответственных за обеспечение безопасности персональных данных.

Процедуры мониторинга и анализа функционирования СОИБ и контроля защитных мер, и их пересмотр относятся к компетенции руководителя СВК и администратора ИБ.

9.2. Методы и способы защиты информации, содержащей персональные данные от несанкционированного доступа

9.2.1. Методами и способами защиты персональных данных от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

9.2.2. Все информационные активы банка, содержащие персональные данные, должны быть защищены от воздействий вредоносного кода средствами антивирусной защиты.

9.2.3. В системе защиты персональных данных информационной системы в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

Методы и способы защиты информации от несанкционированного доступа,

обеспечивающие функции управления доступом, регистрации и учёта, обеспечения целостности, анализа защищённости, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы определяются банком (ответственным сотрудником) в соответствии с пунктом 9.4.

9.2.4. При взаимодействии **информационных систем** с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в пункте 9.2.1, основными методами и способами защиты информации от несанкционированного доступа являются:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации при ее 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 персональных данных информационной системы;
- фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным банком (ответственным сотрудником);
- периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;
- активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;
- анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

Для реализации указанных методов и способов защиты информации банком могут применяться ***межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.***

9.2.5. Для обеспечения безопасности персональных данных при удаленном доступе к **информационной системе** через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в пунктах 9.2.1 и 9.2.4, применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

- проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;
- управление доступом к защищаемым персональным данным информационной сети;
- использование атрибутов безопасности.

9.2.6. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем разных операторов через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, указанных в пунктах 9.2.1 и 9.2.4, применяются следующие основные методы и способы защиты информации от несанкционированного доступа:

- создание канала связи, обеспечивающего защиту передаваемой информации;
- аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
- обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

- обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

9.2.7. Обмен персональными данными при их обработке в **информационных системах** осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств.

9.2.8. В зависимости от особенностей обработки персональных данных и структуры **информационных систем** могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

9.3. Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные

9.3.1. Системы ИБ банковского платежного технологического процесса, в рамках которого обрабатываются персональные данные, должна соответствовать требованиям пунктов 7.2 - 7.8 стандарта СТО БР ИББС-1.0-2010.

СИБ банковского информационного технологического процесса, в рамках которого обрабатываются персональные данные вне ИСПДн, должна соответствовать требованиям пункта 7.9 стандарта СТО БР ИББС-1.0-2010.

СИБ банковского информационного технологического процесса, в рамках которого обрабатываются персональные данные в ИСПДн, должна соответствовать требованиям пунктов 7.9 и 7.11 стандарта СТО БР ИББС-1.0-2010..

9.3.2. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;
- доступ работника банка только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию входящих электронных платежных сообщений;
- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
- возможность ввода платежной информации в АБС только для авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;
- доставку электронных платежных сообщений участникам обмена.

9.3.3. При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы:

- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;
- доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

Клиенты систем дистанционного банковского обслуживания должны быть обеспечены детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

9.3.4. Должна осуществляться и быть регламентирована процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по

обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы с администратором ИБ.

9.3.5. Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы с администратором ИБ.

9.3.6. Банковские информационные технологические процессы должны быть документированы в банке, и согласованы с администратором ИБ.

Указанные технологические процессы должны быть реализованы в рамках созданных для этих целей АБС. Не входящие в состав данных АБС серверы, офисные ЭВМ и другое оборудование рекомендуется изолировать от АБС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ.

9.3.7. Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских информационных технологических процессов. Состав установленного и используемого в ЭВМ и АБС программного обеспечения должен соответствовать определенному перечню.

Выполнение данных требований должно контролироваться с документированием результатов.

9.3.8. Должна быть регламентирована и осуществляться процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации. Регламентирующие документы должны быть согласованы с администратором ИБ.

9.4. Требования по защите информации от несанкционированного доступа в зависимости от класса ИСПДн

Отнесение ИСПДн банка к специальным (см.п.9.1.5) подразумевает тот факт, что вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн определяются для каждого класса ИСПДн.

Пользователи и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных. С этой целью организационно-техническими мерами должно быть запрещено несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

9.4.1. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки общедоступных и (или) обезличенных персональных данных

9.4.1.1. Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов.

При наличии технической возможности количество последовательных неудачных попыток ввода пароля должно быть ограничено — от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.

Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности.

9.4.1.2. Передача персональных данных должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию со структурным подразделением или должностным лицом (работником) банка, ответственным за обеспечение безопасности персональных данных.

9.4.2. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным

9.4.2.1. Для информационных систем обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным, применяются все требования по обеспечению безопасности, определенные в разделе 9.4.1, а также следующие требования.

9.4.2.2. Выполнение функций обеспечения безопасности персональных данных в ИСПДн должно обеспечиваться средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

9.4.2.3. На стадии ввода в действие разработчиком ИСПДн должны быть выполнены настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий. Разработчиком ИСПДн должен быть определен порядок постоянного контроля фактического состояния указанных настроек на предмет их соответствия установленным правилам.

Указанный порядок должен быть согласован структурным подразделением или должностным лицом (работником) банка, ответственным за обеспечение безопасности персональных данных.

9.4.2.4. Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время входа в систему (выхода из системы) субъекта доступа;
- идентификатор субъекта, предъявленный при запросе доступа;
- результат попытки входа: успешная или неуспешная (несанкционированная);
- идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

9.4.2.5. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журнале регистрации событий, указанном в пункте 9.4.2.4.

Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

9.4.2.6. В банке должен быть определен и документально зафиксирован порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения персональных данных.

Снятие с учета машинных носителей, на которых были размещены персональные данные, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения.

Процедура стирания информации регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн в зависимости от применяемого средства гарантированного стирания.

При наличии технической возможности осуществляется очистка освобождаемых областей памяти на носителях, ранее использованных для хранения персональных данных.

9.4.2.7. Состав и назначение ПО ИСПДн должны быть определены и зафиксированы документально в соответствии с требованиями пункта 7.9.7 СТО БР ИББС_1.0.

9.4.2.8. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован. Соответствующие регламенты в виде инструкций, руководств готовятся разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

9.4.2.9. Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий,

9.4.2.10. Восстановление функций обеспечения безопасности персональных данных в ИСПДн в случае нештатной ситуации должно осуществляться администратором ИСПДн с обязательным привлечением администратора информационной безопасности ИСПДн (при необходимости — с привлечением специалистов структурного подразделения или должностного лица работника) банка, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации БС РФ). Процедура восстановления должна быть регламентирована разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

9.4.2.11. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- возможность проверки (контроля) целостности программной и информационной частей средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования).

Приложение 1а
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма для акционеров банка

Согласие на обработку персональных данных
Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество)
г. Майкоп, ул. Пионерская, 276

Я, _____
(ФИО полностью)
_____,
(номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе)

_____

_____
(адрес регистрации)
_____

не возражаю против обработки (автоматизированным и неавтоматизированным способом) Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение моих персональных данных, необходимых для осуществления
нижеследующих целей:
√ идентификация акционера при заключении договора купли-продажи акций АКБ "МАЙКОПБАНК" (ЗАО);
√ осуществление возложенных на АКБ "МАЙКОПБАНК" (ЗАО) законодательством РФ функций в соответствии с Налоговым кодексом РФ, федеральными законами: «О банках и банковской деятельности», «Об акционерных обществах», «О рынке ценных бумаг», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О персональных данных», нормативными актами Банка России, в том числе: №345-П от 27.10.2009г. "О порядке раскрытия в официальном представительстве Банка России в сети Интернет информации о лицах, оказывающих существенное (прямое или косвенное) влияние на решения, принимаемые органами управления банков - участников системы обязательного страхования вкладов физических лиц в банках Российской Федерации", №128-И от 10.03.2006г. «О правилах выпуска и регистрации ценных бумаг кредитными организациями на территории Российской Федерации», а также Уставом и нормативными актами Банка;
√ оформление и исполнение договоров купли-продажи акций АКБ "МАЙКОПБАНК" (ЗАО), иных документов, оформляемых во исполнение договоров, заключенных между Банком и Клиентом;
√ формирование списков лиц, имеющих право на дивиденды, списков лиц, имеющих право на участие в общем собрании акционеров, списков аффилированных лиц, иных сопутствующих достижению указанных целей документов.
срок действия согласия: с момента подписания настоящего согласия и действительно в течение срока хранения договоров купли-продажи акций, списков лиц, имеющих право на дивиденды, списков лиц, имеющих право на участие в общем собрании акционеров, списков аффилированных лиц, иных сопутствующих достижению указанных целей документов, определенного действующим законодательством.

Банк может проверить достоверность предоставленных мной персональных данных, в том числе с использованием услуг других операторов при рассмотрении вопросов о предоставлении других услуг и заключении новых договоров.

В вышеизложенных целях АКБ "МАЙКОПБАНК" (ЗАО) производит обработку следующих персональных данных, предоставленных мной добровольно: фамилия, имя, отчество (при наличии), паспортные данные, гражданство, адрес регистрации, адрес фактического проживания, год, месяц, дата и место рождения, индивидуальный налоговый номер (при наличии), доля в уставном капитале Банка – эмитента и иных обществах, доля принадлежащих мне акций Банка, данные о трудовой деятельности, сведения о почетных и специальных званиях и поощрениях.

Настоящее согласие может быть отозвано мной, после исполнения договорных обязательств, путем направления письменного заявления в АКБ "МАЙКОПБАНК" (ЗАО), если иное не установлено законодательством Российской Федерации.

_____
Дата

_____ /_____/
Подпись *Фамилия инициалы*

Приложение 1б
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма при открытии и обслуживании банковского счета юр. лиц, ИП

Согласие на обработку персональных данных
Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество)
г. Майкоп, ул. Пионерская, 276

Я, _____
(ФИО полностью)
_____,
(номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе)

_____

_____
(адрес регистрации по месту жительства)

_____

не возражаю против обработки (автоматизированным и неавтоматизированным способом) Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), распространение, использование моих персональных данных, необходимых для осуществления нижеследующих целей (*нужное отметить знаком √*):

☐ идентификация руководителя юридического лица, иного лица, обладающего полномочиями на открытие банковского счета от имени юридического лица, и заключение сопутствующих договоров;

☐ идентификация индивидуального предпринимателя, иного лица, обладающего полномочиями на открытие банковского счета от имени индивидуального предпринимателя, и заключение сопутствующих договоров;

☐ идентификация лица, указанного в карточке, на распоряжение денежными средствами, находящимися на банковском счете, открытом в АКБ "МАЙКОПБАНК" (ЗАО);

√ осуществление возложенных на АКБ "МАЙКОПБАНК" (ЗАО) законодательством РФ функций в соответствии с Налоговым кодексом РФ, федеральными законами: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;

√ оформление и исполнение договоров и иных документов, оформляемых во исполнение договоров, заключенных между Банком и Клиентом (в случае, если заключение договоров от имени Клиента производится субъектом персональных данных, указанным в настоящем согласии).

срок действия согласия: с момента подписания настоящего согласия и действительно в течение пяти лет после исполнения договорных обязательств по последнему, заключенному с Банком договору .

Банк может проверить достоверность предоставленных мной персональных данных, в том числе с использованием услуг других операторов при рассмотрении вопросов о предоставлении других услуг и заключении новых договоров.

В вышеизложенных целях АКБ "МАЙКОПБАНК" (ЗАО) производит обработку следующих персональных данных, предоставленных мной добровольно: фамилия, имя, отчество (при наличии), паспортные данные, гражданство, год, месяц, дата и место рождения, сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса, телефона организации, и времени работы в этой организации).

Настоящее согласие может быть отозвано мной после исполнения договорных обязательств, путем направления письменного заявления в АКБ "МАЙКОПБАНК" (ЗАО), если иное не установлено законодательством Российской Федерации.

_____
Дата

_____ /_____/
Подпись *Фамилия инициалы*

Приложение 1в
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма при открытии картсчета либо счета по вкладу

Согласие на обработку персональных данных
Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество)
г. Майкоп, ул. Пионерская, 276

Я, _____
(ФИО полностью)
_____,
(номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе)
_____
_____
(адрес регистрации)
_____

не возражаю против обработки (автоматизированным и неавтоматизированным способом) Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение моих персональных данных, необходимых для осуществления нижеследующих целей (*нужное отметить знаком √*):

☐ идентификация Клиента при открытии счета для расчетов с использованием банковской пластиковой карты «Золотая Корона» в АКБ "МАЙКОПБАНК" (ЗАО);

☐ идентификация Клиента при открытии счета по вкладу в АКБ "МАЙКОПБАНК" (ЗАО);

☐ идентификация Клиента при совершении им в АКБ "МАЙКОПБАНК" (ЗАО) операций по получению либо отправлению перевода денежных средств без открытия банковского счета;

√ осуществление возложенных на АКБ "МАЙКОПБАНК" (ЗАО) законодательством РФ функций в соответствии с Налоговым кодексом РФ, федеральными законами: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О персональных данных», «О страховании вкладов физических лиц в банках Российской Федерации», нормативными актами Банка России, а также Уставом и нормативными актами Банка;

√ оформление и исполнение договоров и иных документов, оформляемых во исполнение договоров, заключенных между Банком и Клиентом.

срок действия согласия: с момента подписания настоящего согласия и действительно в течение пяти лет после исполнения договорных обязательств по последнему заключенному договору.

Банк может проверить достоверность предоставленных мной персональных данных, в том числе с использованием услуг других операторов при рассмотрении вопросов о предоставлении других услуг и заключении новых договоров.

В вышеизложенных целях АКБ "МАЙКОПБАНК" (ЗАО) производит обработку следующих персональных данных, предоставленных мной добровольно: фамилия, имя, отчество (при наличии), паспортные данные, гражданство, адрес регистрации, адрес фактического проживания, год, месяц, дата и место рождения, индивидуальный налоговый номер (при наличии), данные миграционной карты и(или) документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации, в случае если их наличие предусмотрено законодательством РФ.

Настоящее согласие может быть отозвано мной, после исполнения договорных обязательств, путем направления письменного заявления в АКБ "МАЙКОПБАНК" (ЗАО), если иное не установлено законодательством Российской Федерации.

_____
Дата

_____ /_____/
Подпись *Фамилия инициалы*

Приложение 1г
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма для заемщиков

Согласие на обработку персональных данных
Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество)
г. Майкоп, ул. Пионерская, 276

Я, _____
(ФИО полностью)
_____,
(номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе)
_____
(адрес регистрации)

не возражаю против обработки (автоматизированным и неавтоматизированным способом) Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу в Бюро кредитных историй при наличии отдельного согласия) моих персональных данных, необходимых для осуществления
нижеследующих целей (*нужное отметить знаком √*):
☐ принятие Банком решения о выдаче / отказе в выдаче кредита по моему заявлению- анкете о получении кредита в АКБ "МАЙКОПБАНК" (ЗАО);
☐ принятие Банком решения о заключении договора поручительства по моему заявлению- анкете о предоставлении поручительства АКБ "МАЙКОПБАНК" (ЗАО);
☐ принятие Банком решения о заключении договора залога по моему заявлению- анкете о предоставлении залога АКБ "МАЙКОПБАНК" (ЗАО);
√ осуществление возложенных на АКБ "МАЙКОПБАНК" (ЗАО) законодательством РФ функций в соответствии с Налоговым кодексом РФ, федеральными законами: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О государственной регистрации прав на недвижимое имуществом и сделок с ним», «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;
√ оформление и исполнение договоров и иных документов, оформляемых во исполнение договоров, заключенных между Банком и Клиентом.
срок действия согласия: с момента подписания настоящего согласия и действительно в течение пяти лет после исполнения договорных обязательств по последнему заключенному договору.

Банк может проверить достоверность предоставленных мной персональных данных, в том числе с использованием услуг других операторов при рассмотрении вопросов о предоставлении других услуг и заключении новых договоров.

В вышеизложенных целях АКБ "МАЙКОПБАНК" (ЗАО) производит обработку следующих персональных данных, предоставленных мной добровольно: фамилия, имя, отчество (при наличии), паспортные данные, гражданство, адрес регистрации, адрес фактического проживания, год, месяц, дата и место рождения, семейное, социальное, имущественное положение, образование, профессия, сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса, телефона организации, и времени работы в этой организации), доходы, абонентский номер телефона (мобильного и домашнего), индивидуальный налоговый номер (при наличии), сведения об имущественном положении, сведения о номере и серии страхового свидетельства государственного пенсионного страхования, сведения из страховых полисов обязательного (добровольного) медицинского страхования.

Настоящее согласие может быть отозвано мной, после исполнения договорных обязательств, путем направления письменного заявления в АКБ "МАЙКОПБАНК" (ЗАО), если иное не установлено законодательством Российской Федерации.

_____
Дата

_____ /_____/
Подпись *Фамилия инициалы*

Приложение 1д
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма для сотрудников Банка

Согласие на обработку персональных данных
Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество)
г. Майкоп, ул. Пионерская, 276

Я, _____
(ФИО полностью)

_____,
(номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем его органе)

_____

_____
(адрес регистрации)

_____

не возражаю против обработки (автоматизированным и неавтоматизированным способом) Акционерным коммерческим банком "МАЙКОПБАНК" (Закрытое акционерное общество), включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение моих персональных данных, необходимых для осуществления нижеследующих целей:

√ осуществление возложенных на АКБ "МАЙКОПБАНК" (ЗАО) законодательством РФ функций в соответствии с Налоговым кодексом РФ, Трудовым кодексом РФ, федеральными законами, в том числе «О банках и банковской деятельности» №395-I от 02.12.1990г., «Об акционерных обществах» №208-ФЗ от 26.12.1995г., «О рынке ценных бумаг», «О кредитных историях» №218-ФЗ от 30.12.2004г., «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» №115-ФЗ от 07.08.2001г., «О персональных данных» №152-ФЗ от 27.07.2006г., «О государственной регистрации прав на недвижимое имущество и сделок с ним» №122-ФЗ от 21.07.1997г., нормативными актами Банка России, а также Уставом и локальными нормативными актами АКБ "МАЙКОПБАНК" (ЗАО) при исполнении трудового договора и должностной инструкции;

срок действия согласия: согласие предоставлено на срок действия трудового договора. Срок хранения документов, содержащих персональные данные, определяется законодательством Российской Федерации об архивном деле.

В вышеизложенных целях АКБ "МАЙКОПБАНК" (ЗАО) производит обработку следующих персональных данных, предоставленных мной добровольно: фамилия, имя, отчество (при наличии), паспортные данные, гражданство, адрес регистрации, адрес фактического проживания, год, месяц, дата и место рождения, индивидуальный налоговый номер (при наличии), данные о трудовой деятельности (образовании, профессии, ранее занимаемой должности, наименовании предприятия, на котором ранее осуществлялась трудовая деятельность), сведения о почетных и специальных званиях и поощрениях, абонентский номер телефона (мобильного и домашнего телефона, зарегистрированного на имя субъекта персональных данных), номер и серия страхового свидетельства государственного пенсионного страхования, сведения из страховых полисов обязательного (добровольного) медицинского страхования.

Настоящее согласие может быть отозвано мной, после исполнения договорных обязательств, путем направления письменного заявления в АКБ "МАЙКОПБАНК" (ЗАО), если иное не установлено законодательством Российской Федерации.

_____
Дата

_____ /_____/
Подпись *Фамилия инициалы*

Приложение 2
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма

Журнал лиц, допущенных к работе с персональными данными в рамках своих должностных обязанностей

Журнал начат «____» _____ 20__ г.

Должность _____

_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__ г.

Должность _____

_____ / ФИО должностного лица /

№ п/п	ФИО сотрудника	Должность	Категория обрабат -ых ПДн	Доступ к ПДн в ИСПДн разрешен в целях	Осуществляет обработку персональных данных в ИСПДн	Дата и подпись ознаком-ся с документами, устанавлив-ми порядок обработки ПДн	Основание для прекращения допуска к работе с ПДн	Дата прекращения допуска

Приложение 3а
к Положению о порядке
обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма

Журнал
учета электронных носителей персональных данных

Журнал начат «____» _____ 20__ г. Журнал завершен «____» _____ 20__ г.

Должность Должность

_____ / ФИО должностного лица / _____ / ФИО должностного лица /

№ п/п	Учетный номер (регистрационный / серийный номер) либо наименование организации (лица) владельца носителя	Тип / емкость носителя	Дата поста-новки на учет	Отметка о постановке на учет (ФИО, подпись)		Дата снятия с учета	Отметка о снятии с учета (ФИО, подпись)		Сведения об уничтожении носителя / стирании информации / возврате носителя
				Сдал	Принял		Сдал	Принял	

Приложение 3б
к Положению о порядке
обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма

Журнал
учета электронных носителей, содержащих списки на зачисление денежных средств

Журнал начат «____» _____ 20__ г. Журнал завершен «____» _____ 20__ г.

Должность Должность

_____ / ФИО должностного лица / _____ / ФИО должностного лица /

Наименова-ние организа-ции	Номер и дата списка	Сумма списка	Дата поступ-ления списка	Принес список и электр. носитель (Подпись)	Забрал список (Подпись)	Номер и дата платежного поручения	Сумма платеж-ного поруче-ния	Дата поступле-ния платеж-ного поручения	Дата зачисле-ния	Отметка о возврате эл.носи-теля (Дата и подпись)

Приложение 4
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Перечень мест хранения материальных носителей персональных данных и ответственных за хранение

№ п/п	Наименование подразделения	Перечень категорий ПДн	Ответственный за хранение	место хранение
1	Кадровая служба	ПДн работников банка	Немкина О.В.	Головной офис, каб.14
2	Юридическая служба	ПДн клиентов, в отношении которых ведется работа, связанная с принудительным взысканием задолженности	Перегудова О.П.	Головной офис, каб.16
3	Отдел автоматизации банковских операций	Все категории ПДн, содержащиеся в АБС	Ткаченко С.В.	Головной офис, каб.21
4	Отдел экономического анализа и денежного обращения	ПДн заемщиков для передачи в НБКИ	Поликова Е.Е.	Головной офис, каб.16
5	Отдел ценных бумаг и вкладных операций	ПДн клиентов, содержащихся в кредитных досье физ.лиц. юр.дела клиентов, держателей пластиковых карт	Шмырева А.А.	Головной офис, каб.20
6	Отдел кредитования	Пдн содержащиеся в кредитных досье ИП и юр.лиц	Бедрина Т.В.	Головной офис, каб.15
7	Сектор валютных операций	ПДн клиентов, обращающихся в банк в рамках осуществления переводов, без открытия счета и валютного контроля, ПОД/ФТ	Дрожина Н.В.	Головной офис, каб.20
8	Бухгалтерия	Юридические дела ИП и юр.лиц	Сысоева Л.Ф.	Головной офис, каб.12
9	Операционный отдел	ПДн, содержащиеся в анкетах и доверенностях юр. лиц и ИП	Семенихина Н.И.	Головной офис, каб.22
10	Касса	ПДн клиентов вкладчиков и лиц осуществляющих переводы, без открытия счета	Тащева И.В.	Головной офис, помещение кассы
11	Дополнительный офис	ПДн клиентов вкладчиков и лиц осуществляющих переводы, без открытия счета	Канаева Н.Н.	Помещение доп.офиса

Приложение 5
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма

Разрешаю уничтожить
<руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных>
ФИО

_____
«___» _____20__ г.

Акт об уничтожении материальных носителей персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению носителей

(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем

_____.

(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

_____.

(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Приложение 6
к Положению о порядке обработки
персональных данных в
АКБ «МАЙКОПБАНК» (ЗАО)

Форма

Журнал учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных в АКБ «МАЙКОПБАНК» (ЗАО)

Журнал начат «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответст-венного лица	Примечание
1	2	3	4	5	6	7	8