Положение
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.

с изменениями: №1 -12

1. Общие положения.

1.1. Настоящее Положение устанавливает требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных в АО«БАЛАКОВО-БАНК» (далее Банк).

1.2. Настоящее Положение разработано на основе Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», стандарта Банка России СТО БР ИББС-1.0-2014

Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Банке, определяются с учетом:

- нормативно-методических документов Банка.
- модели угроз и нарушителей информационной безопасности Банка.
- нормативных документов Банка в области обеспечения информационной безопасности.
- основных направлений Политики информационной безопасности Банка.
- актуальными для Банка угрозами информационной безопасности, определенными в модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Банка (далее – Отраслевая модель угроз).

1.3. В Положении используются следующие основные термины и определения:

- **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Указано в перечне персональных данных Банка.

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

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- **оператор** – Банк, осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **информационная безопасность -** состояние защищенности интересов (целей) Банка в условиях угроз в информационной сфере.

Защищенность достигается обеспечением совокупности свойств информационной безопасности - доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств информационной безопасности определяется ценностью указанных активов для интересов (целей) организации банковской системы Российской Федерации.

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных»;

1.4. К информационным системам персональных данных Банка (далее – ИСПДн) относятся подсистемы, целью создания и использования которых является обработка персональных данных (Приложение №1).

1.5. Банк не осуществляет трансграничную передачу персональных данных. Все технические средства ИСПДн Банка находятся в пределах Российской Федерации.

1.6. Согласно Указанию Банка России от 10.12.2015 г. № 3889-У "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных, в информационных системах персональных данных" выделена Типовая модель угроз безопасности персональных данных, актуальная при их обработке в информационных системах персональных данных (Приложение №2).

В соответствии со спецификой ИСПДн Банка, угрозы утечки персональных данных по техническим каналам являются для Банка не актуальными.

В соответствии со спецификой ИСПДн Банка, угрозы утечки персональных данных по техническим каналам являются для Банка не актуальными.

1.7 Банк с целью выполнения обязанностей работодателя в связи с возникновением трудовых отношений между Банком и его работником, а так же по оказанию банковских услуг в пределах устава Банка осуществляет обработку: фамилия, имя, отчество, число, месяц и год рождения, место рождения, адресные данные, сведения о доходах, имущественное положение, образование, профессия, семейное положение, социальное положение, паспортные данные, данные свидетельства о рождении, данные страховых свидетельств (пенсионное и медицинское), ИНН, данные воинского учета, принадлежащих работникам, состоящим в трудовых отношениях с Банком, а так же физическим лицам (клиентам), которым оказываются банковские услуги и акционерам Банка.

1.8. Обработка персональных данных осуществляется в режиме смешанной обработки персональных данных.

1.9. Срок или условие прекращения обработки персональных данных: ликвидация либо реорганизация Банка.

1.10 В случае предоставления физическим лицом - заполнение анкет заемщика, поручителя, на трудоустройство и т.д., с указанием в них персональных данных членов семьи (ст.2 Семейного Кодекса РФ), в соответствии с требованиями Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных», физическое лицо должно предоставить согласие на обработку персональных данных членов семьи, данные которых они указывают. Согласие предоставляется на отдельном, для каждого члена семьи, листе по утверждённым формам (Приложения № 8,9,10). При невозможности получения согласия на обработку персональных данных от членов семьи, в их адрес Банком (отделом который запрашивает персональные данные) направляется «Уведомление об обработке Банком их персональных данных» по утверждённым формам (Приложения № 11, 12).

В случае выявления неправомерной обработки персональных данных, осуществляемой Банком, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить, в произвольной форме, субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных.

2. Требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, доступ к которым должен быть ограничен.

2.1. Требования по обеспечению безопасности персональных данных, реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

Реализация и выполнение требований по обеспечению безопасности персональных данных должны осуществляться по согласованию и под контролем службы безопасности Банка в рамках их полномочий.

Организационно-распорядительная, проектная и эксплуатационная документация (например, концепции, технические задания, технические проекты и рабочая документация, акты ввода в опытную и постоянную эксплуатацию, положения, инструкции) по указанным ИСПДн Банка в части вопросов информационной безопасности должна согласовываться службой безопасности Банка, отделом автоматизации, службой внутреннего контроля.

2.2. Все информационно-вычислительные ресурсы ИСПДн Банка защищаются от воздействий вредоносного кода.

2.3. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению антивирусной защиты возлагаются приказами (распоряжениями) Председателя Правления Банка на сотрудников согласно Инструкции по антивирусной защите Банка.

Администратор информационной безопасности Банка руководствуется в своей деятельности инструкцией администратора информационной безопасности, Положением об отделе, в штате которого он состоит, а также инструкциями, входящих в состав эксплуатационной документации на ИСПДн Банка.

2.4. Технические средства, их составные части, включая корпус, блоки, задействованные в обработке персональных данных, и отдельные, не используемые в технологическом процессе элементы указанных технических средств (например, порты, дисководы, разъемы), должны быть, оборудованы средствами контроля их вскрытия или должна использоваться система контроля доступа, позволяющая осуществлять полноценный контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации. В случае использования системы контроля доступа применение специальных защитных знаков существенно ограничивается, при этом опечатыванию подлежит исключительно корпус технического средства.

2.5. Сотрудники, осуществляющие обработку персональных данных в ИСПДн Банка, должны соблюдать требования нормативных и иных актов (регламенты, инструкции) в области информационной безопасности.

2.6. К ИСПДн требования по защите информации от утечки по техническим каналам, в том числе, по каналам побочных электромагнитных излучений и наводок не предъявляются, в соответствии с Отраслевой моделью угроз.

2.7. Процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн Банка в проектной и эксплуатационной документации.

2.8. Эталонные копии ПО учитываются, доступ к ним ограничен.

2.9. Восстановление ИСПДн Банка в случае нештатной ситуации должно осуществляться администратором отдела автоматизации с обязательным привлечением администратора информационной безопасности (при необходимости – с привлечением специалистов разработчиков ИСПДн.

2.10. Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн Банка обеспечивается по периодически (не реже 1 раз в год) обновляемому паролю длиной не менее шести буквенно-цифровых символов.

При наличии технической возможности количество последовательных неудачных попыток ввода пароля ограничивается - от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты блокируют 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 Банка в эксплуатационной документации в соответствии с требованиями к организации парольной защиты (Приложение №3).

2.11. Пользователям ИСПДн Банка запрещается осуществление несанкционированного копирования персональных данных. С этой целью в помещениях, в которых размещаются технические средства обработки персональных данных, запрещается осуществление несанкционированного копирования, в том числе, с использованием отчуждаемых носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующие различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов и т.д.), а также устройств фото- и видеосъемки.

2.12. Передача персональных данных производится государственным органам или по официальному запросу в рамках законодательства. А также на основании официально заключенного договора на передачу персональных данных (бюро кредитных историй). По телекоммуникационным каналам и линиям связи между подразделениями Банка, с одной стороны, и внешними организациями, с другой стороны, передача осуществляется с использованием сертифицированных средств криптографической защиты или иных защитных механизмов.

2.13. Сохранность и целостность программных средств обеспечения информационной безопасности, персональных данных, а также других программных средств ИСПДн Банка является обязательной и обеспечивается, в том числе, за счет создания резервных копий.

Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, использования (для восстановления) резервных копий, осуществляется согласно Регламенту проведения резервного копирования Банка.

3. Контроль обеспечения безопасности персональных данных при их обработке в ИСПДн

3.1. Контроль обеспечения безопасности персональных данных при их обработке в ИСПДн Банка (далее – Контроль) является неотъемлемой частью общего комплекса мер обеспечения безопасности и защиты информации в Банке России.

3.2. Контроль должен осуществляться на всех этапах обработки персональных данных.

3.3. Выделяется внутренний и внешний контроль.

3.3.1. **Внешний контроль** осуществляется в рамках следующих контрольных мероприятий:

- контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке ИСПДн, осуществляемый ФСТЭК России и ФСБ России в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн;
- внешние оценки соответствия информационной безопасности требованиям Стандарта Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

3.3.2. **Внутренний контроль** осуществляется в рамках следующих контрольных мероприятий:

- мониторинг и контроль защитных мер;
- внутренние проверки (и самооценки) соответствия требованиям настоящего документа, проводимые подразделениями безопасности и защиты информации в подразделениях Банка;
- самооценки соответствия информационной безопасности требованиям стандарта Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

3.4. Методическое руководство и контроль выполнения требований настоящего Порядка осуществляется Службой безопасности, Службой внутреннего контроля.

3.5. Самооценка соответствия информационной безопасности требованиям стандарта Банка России СТО БР ИББС-1.0 проводится в соответствии с рекомендациями в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014, стандарта Банка России СТО БР ИББС-1.2-2014.

3.6. Внешние оценки соответствия информационной безопасности требованиям стандарта Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» проводится в соответствии со стандартом Банка России СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности», со стандартом Банка России СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-2014.

3.7. Поддержание на должном уровне системы обеспечения информационной безопасности (далее - СОИБ) организаций банковской системы Российской Федерации и снижения степени тяжести последствий от нарушений ИБ определены в Рекомендациях в области стандартизации Банка России РС БР ИББС-2.5-2014.

3.8. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем определены в Рекомендациях в области стандартизации Банка России РС БР ИББС-2.6-2014.

4. Порядок хранения материальных носителей ПД от несанкционированного доступа:

4.1. К носителям ПД в Банке относятся:

- бумажные (любой документ, содержащий в себе ПД сотрудника или клиента позволяющий идентифицировать его)
- электронные внутренние / стационарные, (HDD-диски ПК, серверов)
- электронные внешние / съёмные (CD, Flash-накопители, дискеты 3,5” и т.д.)

4.2. Хранение информации на бумажных или на электронных носителях происходит в сейфах и архиве банка, а также в помещениях оборудованных ОПС и сдаваемых под охрану;

4.3. Хранение отчуждаемых (съемных) носителей ИСПДн допускается в одном хранилище с другими документами, в отдельном контейнере, опечатываемом самим Пользователем, либо его руководителем, исключающем их непреднамеренное уничтожение.

4.4. Помещения, где обрабатываются ИСПДн, оборудуются сигнализацией и по окончанию рабочего дня и сдаются под расписку посту охраны банка (для сектора расчетных операций с клиентами другой порядок) обеспечивая сохранность конфиденциальной информации, СКЗИ, ключевых документов и исключают возможность неконтролируемого проникновения или пребывания в них посторонних лиц во внерабочее время.

4.5. Ограничен круг лиц, имеющих парольный доступ к электронным базам данных, содержащих персональные данные;

4.6. Места хранения материальных носителей ПД определены в рабочих кабинетах и архивах Банка. (Приложение №14).

5. Обязанности Банка по уточнению, блокированию и уничтожению персональных данных.

5.1. В случае выявления неправомерной обработки или при выявлении неточностей в обрабатываемых персональных данных субъектом персональных данных или его представителем необходимо, чтобы было составлено по данному случаю заявление (Приложение №13). Банк обязан осуществить уточнение обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование в случае неправомерной обработки (в том числе, если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) с момента получения данного заявления на время проверки полученной информации.

В случае подтверждения факта неточности персональных данных Банк на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных

осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.2. В случае подтверждения факта неточности персональных данных Банк на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

5.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Банка. В случае, если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Банк обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5.4. В случае достижения цели обработки персональных данных Банк обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банк) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено:

- договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- соглашением между Банком и субъектом персональных данных;
- иными Федеральными законами (в том числе Федеральным законом № 218 – ФЗ «О кредитных историях» от 30.12.2004 г.).

Персональные данные, полученные Банком при рассмотрении заявок на получение кредита, в случае отрицательного решения, подлежат уничтожению в срок, не превышающий трёх рабочих дней с даты принятия решения, в случае если Заёмщик в указанный срок не забрал предоставленные им документы, содержащие персональные данные.

Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 218 – ФЗ «О кредитных историях» от 30.12.2004 г. или другими федеральными законами.

5.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Банк обязан прекратить их обработку, а также в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не

предусмотрено договором, стороной которого, выгодоприобретателем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. Способы уничтожения персональных данных

6.1. Физическое уничтожение носителя
6.2. Уничтожение информации с носителя

- **Бумажный носитель.** Уничтожение происходит через шредирование (измельчение) или уничтожение через термическую обработку (сжигание).

- **Электронный носитель.** Уничтожение заключается в удалении информации с носителя путём многократной перезаписи в секторах магнитного диска или уничтожение самого носителя путём нанесения ему неустранимых физических повреждений, исключающих возможность его использования или восстановления ключевой информации.

6.3. Уничтожение персональных данных проводится комиссией в количестве не менее трех человек. После уничтожения составляется акт (Приложение № 4).

7. Порядок реагирования на запросы со стороны субъектов ПДн.

7.1. При обращении физических лиц за предоставлением информации по вопросам обработки своих персональных данных факт обращения и характер запроса фиксируется в регистрационном журнале установленной формы (Приложение № 5).
7.2. В срок, не превышающий тридцати дней с даты получения запроса субъекта персональных данных или его представителя, подготавливается ответ по типовой форме (Приложение № 6) о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его представителя.
7.3. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, по форме (Приложение № 7) в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.
7.4. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
7.4. Ответственность за ненадлежащую подготовку информации, её несанкционированную передачу несет должностное лицо, результатом деятельности которого явились нарушения.

Приложение №1
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных.

Перечень информационных подсистем, в которых обрабатываются персональные данные.

№ п/п	Наименование системы	Эксплуатирующие подразделения
1	Diasoft FA # Beans (Автоматическая банковская система).	1. Отдел ценных бумаг и отчетности 2. Отдел денежного обращения и пластиковых карт 3. Отдел бухгалтерского учета и отчетности 4. Служба безопасности 5. Отдел финансового мониторинга и валютного контроля 6. Кредитный отдел 7. Отдел информационных технологий 8. Служба управления рисками. 9. Иванов И.И. 10. Разъякашина Е.В. 11. Кириллов Е.Ю. 12. Служба внутреннего контроля 13. Служба внутреннего аудита.
2	WF card WorkFlow (Система учета операций произведенных с использованием пластиковых карт)	1. Отдел денежного обращения и пластиковых карт 2. Отдел информационных технологий 3. Отдел бухгалтерского учета и отчетности 4. Служба внутреннего контроля 5. Служба внутреннего аудита.
3	1С Предприятие 8.2 «Зарплата – кадры»	1. Отдел бухгалтерского учета и отчетности 2. Отдел кадров 3. Отдел информационных технологий 4. Служба внутреннего контроля 5. Служба внутреннего аудита.
4	1С Предприятие 7.7 «Торговля и склад»	1. Операционные кассы вне кассового узла (ОКВКУ) 2. Отдел информационных технологий
5	Contact (Система денежных переводов)	1. Операционные кассы вне кассового узла (ОКВКУ) 2. Отдел информационных технологий 3. Отдел кассовых операций

6	«Контур-экстерн» (Программа для обмена сообщениями по налоговой и бухгалтерская отчетность)	1. Отдел бухгалтерского учета и отчетности 2. Отдел информационных технологий
7	KOMITA (Система финансового мониторинга)	1. Отдел финансового мониторинга и внутреннего контроля 2. Отдел информационных технологий 3. Служба внутреннего контроля 4. Служба внутреннего аудита
8	«Персонифицированный учёт» (формирование данных для пенсионного фонда)	1. Отдел бухгалтерского учета и отчетности 2. Отдел кадров 3. Отдел информационных технологий
9	АРМ «Контракты» (система таможенного банковского контроля ТБ СВК)	1. Отдел финансового мониторинга и внутреннего контроля 2. Отдел информационных технологий
10	DOCPSN (формирование данных для пенсионного фонда)	1. Юридический отдел (юрист консульт по кадрам) 2. Отдел информационных технологий 3. Отдел бухгалтерского учета и отчетности
11	ПТК ПСД (отчетность в ГУ по ценным бумагам, По противодействию легализации отмыванию доходов)	1. Отдел ценных бумаг и отчетности 2. Отдел финансового мониторинга валютного контроля 3. Отдел информационных технологий 4. Служба управления рисками 5. Служба безопасности 6. Отдел бухгалтерского учета и отчетности 7. Отдел денежного обращения и пластиковых карт 8. Служба внутреннего контроля 9. Служба внутреннего аудита.
12	2НДФЛ (Налоговая и бухгалтерская отчетность)	1. Отдел ценных бумаг и отчетности 2. Отдел бухгалтерского учета и отчетности 3. Отдел денежного обращения и пластиковых карт 4. Отдел информационных технологий
13	НБКИ (Формирование, отправка и получение сообщений по кредитным историям)	1. Кредитный отдел 2. Служба безопасности 3. Отдел информационных технологий 4. Кириллов Е.Ю.
14	Киберплат (платежи МТС)	1. Операционные кассы вне кассового узла (ОКВКУ) 2. Отдел информационных технологий 3. Служба безопасности 4. Отдел бухгалтерского учета и отчетности
15	КБ «Юнистрим Банк» (Система денежных переводов)	1. Операционные кассы вне кассового узла (ОКВКУ) 2. Отдел кассовых операций 3. Отдел информационных технологий 4. Служба безопасности

Приложение №2
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных

**Типовая модель угроз безопасности персональных данных,
актуальная при их обработке в информационных системах персональных данных:**

1. угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;
2. угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
3. угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
4. угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
5. угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
6. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
7. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
8. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;
9. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;
10. угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации.

Приложение №3
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных

Требования к организации парольной защиты
АО «БАЛАКОВО-БАНК».

1. Пароли формируются сотрудником, выполняющим функции администратора информационной безопасности.
2. Не допускается использование единого пароля для доступа к различным информационным ресурсам Банка.
3. К структуре паролей предъявляются следующие требования:
   - пароль должен состоять не менее чем из 6 символов;
   - в числе символов пароля обязательно должны присутствовать буквы и цифры;
   - пароль не должен включать легко вычисляемые сочетания символов (например, имена, фамилии, наименования АРМ), какую- либо личную информацию о пользователе, а также общепринятые сокращения (например, ЭВМ, ЛВС, SYSOP);
4. при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 4 символа.
5. Свой пароль пользователь не имеет права сообщать никому. Запрещается оставлять пароли в легкодоступном или на видном месте.
6. Резервная копия каждого пароля с фиксацией даты формирования пароля храниться в Службе безопасности.
7. В случае необходимости использования учетной записи отсутствующего сотрудника оформляется заявка на предоставление временного пароля - Приложение №4 к Положению об эксплуатации электронно-вычислительной техники и распределении доступа пользователей к ресурсам локальной вычислительной сети АО“БАЛАКОВО-БАНКА”.
8. Полная плановая смена паролей должна проводиться не реже одного раза в год.
9. Внеплановые удаление или смена пароля пользователя ИСПДн Банка в случае прекращения или любого изменения его полномочий должны производиться немедленно после окончания последнего сеанса работы данного пользователя. При этом должна быть также выполнена безотлагательная корректировка прав доступа на всех средствах вычислительной техники в соответствии с изменившимися полномочиями сотрудника.
10. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий администраторов (увольнение, переход на другую работу внутри банка и другие обстоятельства) и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.
11. В случае компрометации пароля (подсматривание его кем-либо, разглашение пароля и др.) пароль необходимо сменить.

Приложение №4
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных

РАЗРЕШАЮ УНИЧТОЖИТЬ

Председатель Правления
АО «БАЛАКОВО-БАНК»

_____Н.Е. Рожкова

“____” _____ 20__г

Акт об уничтожении персональных данных

Комиссия, назначенная приказом по банку № ___ от _____ ___ г. для уничтожения персональных данных, в составе:

Председатель комиссии: _____ ;
Члены комиссии: _____ ;
_____ .

провела отбор носителей персональных данных _____ для уничтожения по реестру от «__» _____ ___ г. и установила, что персональные данные, полученные в результате обработки _____,
(наименование отделов)
в соответствии с требованиями руководящих документов по защите информации, подлежат уничтожению, в связи с _____ .
(цель обработки данных достигнута, утрата необходимости в достижении целей обработки и т.д.)

№ п/п	Дата	Тип носителя	Кол-во листов
1.			
2.			
3.			

Всего подлежит уничтожению: _____ (_____) носителей.
цифрами прописью

Комиссия установила, что после утверждения Акта об уничтожении персональных данных перечисленные носители сверены с записями в Акте и уничтожены путем

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

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

Приложение №5
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных.

Журнал учета обращений граждан (субъектов персональных данных)

по вопросам обработки персональных данных АО «БАЛАКОВО-БАНК».

№ п/п	Сведения о запрашивающем лице.	Краткое содержание обращения.	Цель получения информации.	Дата предоставления ответа и отметка о предоставлении (какая именно информация была передана) или отказе в предоставлении информации.	Подпись запрашиваю щего лица.	Ф.И.О. Подпись сотрудника предоставив шего ответ на запрос.

Приложение №8
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
(Заполняется в случае предоставления в анкете ПД членов семьи Заёмщика).

Согласие члена семьи Заёмщика на обработку персональных данных.

Я _____
(Ф.И.О.)

_____
(адрес)

_____
(серия и номер паспорта, когда и кем выдан)

осведомлен(а) и согласен(а) с тем, что в соответствии со статьёй 6 и статьёй 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» АО«БАЛАКОВО-БАНК» находящийся по адресу: Саратовская обл., г. Балаково, ул. Факел Социализма,21 осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ в интересах Банка), обезличивание, блокирование, удаление, уничтожение персональных данных, передачу, как с использованием средств автоматизации, так и без использования таких средств, указанных в настоящей анкете, состоящих из: фамилия, имя, отчество, дата рождения, место работы, адрес места регистрации / проживания, номера телефонов в целях заключения и исполнения кредитного договора между АО «БАЛАКОВО-БАНК» и

_____
(Ф.И.О. Заёмщика)

В целях урегулирования просроченной задолженности Заёмщика Банк вправе осуществлять передачу данных, указанных в настоящей анкете и данных, полученных в течение срока действия Кредитного договора, для их обработки юридическими лицами, исполняющими функции коллекторских агентств и / или предоставляющими Банку иные услуги по урегулированию просроченной задолженности Заёмщика, на основании заключённых с ними договоров.

Я заявляю, что указанная в настоящем Согласии информация является достоверной и может быть мной подтверждена в случае необходимости документально.

Я ознакомлен(а) с тем, что АО«БАЛАКОВО-БАНК» осуществляет обработку моих персональных данных лично, без поручения их обработки другому лицу.

Своё согласие на обработку персональных данных я предоставляю на неограниченный срок до моего письменного уведомления о его отзыве и в соответствии с п.5 со ст.21 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прекратить обработку моих персональных данных.

«___»_____20__ г. _____ (_____)

Приложение №9
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
(Заполняется в случае предоставления в анкете ПД членов семьи Поручителя).

Согласие члена семьи Поручителя на обработку персональных данных.

Я _____
(Ф.И.О.)

_____
(адрес)

_____
(серия и номер паспорта, когда и кем выдан)

осведомлен(а) и согласен(а) с тем, что в соответствии со статьёй 6 и статьёй 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» АО«БАЛАКОВО-БАНК» находящийся по адресу: Саратовская обл., г. Балаково, ул. Факел Социализма,21 осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ в интересах Банка), обезличивание, блокирование, удаление, уничтожение персональных данных, передачу, как с использованием средств автоматизации, так и без использования таких средств, указанных в настоящей анкете, состоящих из: фамилия, имя, отчество, дата рождения, место работы, адрес места регистрации / проживания, номера телефонов в целях заключения и исполнения Договора поручительства между АО«БАЛАКОВО-БАНК» и

_____
(Ф.И.О. Поручителя)

В целях урегулирования просроченной задолженности Поручителя Банк вправе осуществлять передачу данных, указанных в настоящей анкете и данных, полученных в течение срока действия Кредитного договора, для их обработки юридическими лицами, исполняющими функции коллекторских агентств и / или предоставляющими Банку иные услуги по урегулированию просроченной задолженности Поручителя, на основании заключённых с ними договоров.

Я заявляю, что указанная в настоящем Согласии информация является достоверной и может быть мной подтверждена в случае необходимости документально.

Я ознакомлен(а) с тем, что АО«БАЛАКОВО-БАНК» осуществляет обработку моих персональных данных лично, без поручения их обработки другому лицу.

Своё согласие на обработку персональных данных я предоставляю на неограниченный срок до моего письменного уведомления о его отзыве и в соответствии с п.5 со ст.21 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прекратить обработку моих персональных данных.

«___»_____20__ г. _____ (_____)

Приложение №10
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
(Заполняется в случае предоставления в анкете ПД членов семьи Кандидата на трудоустройство).

Согласие члена семьи Кандидата на трудоустройство
на обработку персональных данных.

Я _____
(Ф.И.О.)

_____
(адрес)

_____
(серия и номер паспорта, когда и кем выдан)

осведомлен(а) и согласен(а) с тем, что в соответствии со статьёй 6 и статьёй 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» АО «БАЛАКОВО-БАНК» находящийся по адресу: Саратовская обл., г. Балаково, ул. Факел Социализма,21 осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ в интересах Банка), обезличивание, блокирование, удаление, уничтожение персональных данных, передачу, как с использованием средств автоматизации, так и без использования таких средств, указанных в настоящей анкете, состоящих из: фамилия, имя, отчество, дата рождения, место работы, адрес места регистрации / проживания, номера телефонов в целях проверки информации службой безопасности АО«БАЛАКОВО-БАНК»

_____
(Ф.И.О. Кандидата на трудоустройство)

Я заявляю, что указанная в настоящем Согласии информация является достоверной и может быть мной подтверждена в случае необходимости документально.

Я ознакомлен(а) с тем, что АО «БАЛАКОВО-БАНК» осуществляет обработку моих персональных данных лично, без поручения их обработки другому лицу.

Своё согласие на обработку персональных данных я предоставляю на неограниченный срок до моего письменного уведомления о его отзыве и в соответствии с п.5 со ст.21 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» прекратить обработку моих персональных данных.

«___»_____20__ г. _____ (_____)

Приложение №11
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
(при отправке Уведомления об обработке ПД
членов семьи Клиента).

Кому: _____
ф.и.о.

_____
адрес физ.лица

_____

Уведомление об обработке персональных данных.

АО «БАЛАКОВО-БАНК», место нахождения: 413840, Саратовская обл., г. Балаково, ул. Факел Социализма, 21 (далее – Банк) уведомляет о включении в анкету заемщика/ поручителя -

_____
Ф.И.О.

Ваших персональных данных (фамилия, имя, отчество, дата рождения, место работы, адрес места регистрации / проживания, номер служебного и домашнего телефона) в целях их обработки начиная с _____ (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),
дд/мм/гг- дата подачи анкеты
извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных совершаемых с использованием средств автоматизации или без использования таких средств, для реализации Банком программ кредитования физических лиц, в том числе при сотрудничестве с третьими лицами, принятия решения о предоставлении кредита и заключения с ними кредитного договора, либо договора / поручительства, в случае если Банком будет принято положительное решение о предоставлении ему(ей) кредита.

Основанием обработки Банком Ваших персональных данных является гл.2, гл.4 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», ст. 26 Федерального закона № 395-1 от 02.12.1990 г. «О банках и банковской деятельности», ст. 7 Федерального закона от 25.07.2002 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», локальные нормативные документы АО«БАЛАКОВО-БАНК».

Предполагаемыми пользователями Ваших персональных данных будут являться сотрудники Банка. Сроком окончания обработки персональных данных будет являться достижение целей обработки или в случае утраты необходимости в их достижении. Банк не осуществляет трансграничную передачу персональных данных в процессе обработки и обеспечивает их защиту в соответствии с требованиями, установленными Правительством РФ.

В соответствии с главой 3 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» Вы как субъект персональных данных имеете право на получение информации, касающейся обработки Ваших персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Банком;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Банком способы обработки персональных данных;

4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) иные сведения, предусмотренные указанным Федеральным законом или другими федеральными законами.

С уважением,

Председатель Правления
АО «БАЛАКОВО-БАНК»

Приложение №12
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
(при отправке Уведомления об обработке ПД
членов семьи Кандидата на трудоустройство).

Кому: _____
ф.и.о.

_____
адрес физ.лица

_____

Уведомление об обработке персональных данных.

АО «БАЛАКОВО-БАНК», место нахождения: 413840, Саратовская обл., г. Балаково, ул. Факел Социализма, 21 (далее – Банк) уведомляет о включении в анкету Кандидата на трудоустройство -

_____
Ф.И.О.

Ваших персональных данных (фамилия, имя, отчество, дата рождения, место работы, адрес места регистрации / проживания, номер служебного и домашнего телефона) в целях их обработки начиная с _____ (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),
(дд/мм/гг (*))
извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных совершаемых с использованием средств автоматизации или без использования таких средств, для реализации Банком программ кредитования физических лиц, в том числе при сотрудничестве с третьими лицами, принятия решения о предоставлении кредита и заключения с ними кредитного договора, либо договора / поручительства, в случае если Банком будет принято положительное решение о предоставлении ему(ей) кредита.

Основанием обработки Банком Ваших персональных данных является гл.2, гл.4 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», ст.ст. 57, 65, 85-90 Трудового кодекса Российской Федерации от 30.12.2001г. № 197-ФЗ, локальные нормативные документы АО «БАЛАКОВО-БАНК».

Предполагаемыми пользователями Ваших персональных данных будут являться сотрудники Банка. Сроком окончания обработки персональных данных будет являться достижение целей обработки или в случае утраты необходимости в их достижении. Банк не осуществляет трансграничную передачу персональных данных в процессе обработки и обеспечивает их защиту в соответствии с требованиями, установленными Правительством РФ.

В соответствии с главой 3 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» Вы как субъект персональных данных имеете право на получение информации, касающейся обработки Ваших персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных Банком;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Банком способы обработки персональных данных;

4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) иные сведения, предусмотренные указанным Федеральным законом или другими федеральными законами.

С уважением,

Председатель Правления
АО «БАЛАКОВО-БАНК»

_____
(*)- дата подачи анкеты

Приложение №13
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных

Председателю Правления
АО «БАЛАКОВО-БАНК»

Заявление
о принятии мер по ограничению доступа к информации,
обрабатываемой с нарушением законодательства Российской Федерации
в области персональных данных.

1. Субъект персональных данных (представитель субъекта персональных данных):

_____
(Ф.И.О. полностью)

_____
(данные документа, удостоверяющего личность)

_____

_____
(наименование, реквизиты документа, подтверждающего полномочия)

_____

2. Адрес регистрации по месту жительства субъекта персональных данных:

_____
(полный почтовый адрес)

_____

_____
(номер телефона)

3. Сведения о документах, содержащих ошибочную информацию или обрабатываемую с нарушением законодательства РФ в области персональных данных. Документ (информационный ресурс в сети Интернет), где они были выявлены:

_____

_____

_____

_____

4. Меры необходимые для устранения выявленной ошибки (заблокировать, внести изменение следующего содержания)

_____

_____

«____»_____20___ г. _____
(Подпись)

Подготовил:

Приложение №14
К Положению об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных

Места хранения материальных носителей персональных данных
в АО «БАЛАКОВО-БАНК».

Пояснения:

Информационная система АО «БАЛАКОВО-БАНК», в которой обрабатываются персональные данные (далее - ПД) является информационной системой, обрабатывающей иные категории персональных данных, т.к. в ней не обрабатываются специальные категории персональных данных, т.е. персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных. ПД из общедоступных источников не категорируются.

№ п/п	Место хранения персональных данных .	Материальные носители
1	Руководители. (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
2	Служба внутреннего контроля (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
3	Служба внутреннего аудита (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
4	Отдел по работе с клиентами (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
5	Отдел финансового мониторинга и валютного контроля (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
6	Референт (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
7	Юридический отдел (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
8	Отдел ценных бумаг и отчётности (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).

9	Служба управления рисками (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
10	Кредитный отдел (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
11	Отдел денежного обращения и пластиковых карт (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
12	Отдел информационных технологий (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
13	Отдел бухгалтерского учёта и отчётности (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
14	Отдел кассовых операций (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
15	Хозяйственный отдел (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
16	Отдел по работе с персоналом (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
17	Служба безопасности (Офисная мебель для документов, сейфы)	- Документация, относящаяся к деятельности отдела, содержащая ПД. - Персональные компьютеры. - Накопители информации (съёмные, оптические, магнитные).
18	Архивы (стеллажи, сейфы)	- Документация, относящаяся к деятельности отделов Банка, содержащие ПД.