УТВЕРЖДЕНО
Общим собранием участников
ООО КБ «Альба Альянс»
(Протокол заседания от 23 декабря 2016 года)

ПОЛОЖЕНИЕ
об организации и обеспечении защиты персональных данных ООО КБ «Альба Альянс»

Москва, 2016

1. Назначение и область применения

1.1. Положение об организации и обеспечении защиты персональных данных в ООО КБ «Альба Альянс» предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных в соответствии с требованиями Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных в ООО КБ «Альба Альянс».

1.3. Положение является локальным нормативным правовым актом ООО КБ «Альба Альянс» (далее – Банк). Требования Положения обязательны для выполнения всеми работниками, которые допущены к обработке персональных данных.

2. Термины и сокращения

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
КЗ	Контролируемая зона
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средство защиты информации
СЗПДн	Система (подсистема) защиты персональных данных
СКЗИ	Средство криптографической защиты информации
ФЗ	Федеральный закон

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

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с Перечнем присвоенных идентификаторов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления

таких процессов и методов.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Материальный носитель персональных данных (далее – материальный носитель) – материальный объект, используемый для закрепления и хранения информации. В рамках настоящего Положения под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т. п.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или с другими лицами организующие и/или осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы информационной системы, осуществляемое с использованием вредоносных программ.

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

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

Ресурс информационной системы – именованный элемент системного прикладного или аппаратного обеспечения функционирования информационной системы.

Средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Общие положения

3.1. Необходимость проведения мероприятий по защите персональных данных в Банке определяется:

– Федеральным законом РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.2. Целью защиты ПДн является предотвращение возможной утечки информации и/или несанкционированного и непреднамеренного изменения или разрушения ПДн.

3.3. Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

3.4. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

3.5. Все работники, обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под роспись.

4. Нормативные ссылки

Настоящее Положение разработано в соответствии с правовыми актами РФ:

– Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным Законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– «Составом и содержанием организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн», утвержденными приказом ФСТЭК России от 18.02.2013 г. № 21;

– «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», утвержденной Заместителем директора ФСТЭК России 15.02.2008 г.;

– «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утвержденной Заместителем директора ФСТЭК России 15.02.2008 г.;

– Приказом ФСБ России от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5. Персональные данные, подлежащие защите

5.1. Персональные данные, подлежащие защите, утверждаются приказом Президента Банка в виде Перечня обрабатываемых персональных данных ООО КБ «Альба Альянс».

5.2. Персональные данные, подлежащие защите в Банке, обрабатываются без использования средств автоматизации, а также в информационных системах персональных данных (ИСПДн).

6. Организационная система обеспечения безопасности ПДн

6.1. В состав организационной системы обеспечения безопасности ПДн Банка входят:

– Президент;
– лицо, ответственное за организацию обработки персональных данных;
– работники Отдела защиты информации;
– работники Управления информационных технологий;
– начальник Управления по работе с персоналом;
– руководители подразделений, работникам которых предоставлен доступ к ПДн;
– работники, которым предоставлен доступ к ПДн (пользователи ИСПДн).

6.2. Общее руководство организацией работ по защите ПДн осуществляет Президент Банка.

6.3. Лицо, ответственное за организацию обработки персональных данных, в рамках обеспечения безопасности ПДн выполняет следующие функции:

– организует процессы разработки, утверждения и корректировки локальных правовых актов по обеспечению безопасности ПДн;

– организует внутренний контроль за соблюдением Банком и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– организует доведение до сведения работников Банка положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

6.4. Руководство и контроль за обеспечением безопасности ПДн при их обработке в ИСПДн, организацию работ по разработке документации по защите ПДн, разработке СЗПДн, по проведению организационных и технических мероприятий по защите ПДн при их обработке в ИСПДн осуществляет начальник Отдела защиты информации.

6.5. Из числа работников Управления информационных технологий назначаются администраторы безопасности. Обязанности администраторов безопасности, ответственных за защиту информации, определяются Инструкцией администраторам безопасности ИСПДн и включают:

– администрирование, контроль работоспособности и анализ результатов работы средств защиты информации в ИСПДн;

– обнаружение и участие в расследовании попыток НСД, информирование руководства о фактах нарушения установленного порядка обеспечения безопасности и попытках НСД к информационным ресурсам;

– проведение периодических проверок защищенности ИСПДн;

– подготовка предложений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПД.

6.6. Работники отделов, входящих в состав Управления информационных технологий в части, касающейся их деятельности, осуществляют:

– системное администрирование серверов, сетевого оборудования и рабочих станций ИСПДн;

– администрирование прикладных систем ИСПДн.

6.7. Управление информационных технологий в рамках обеспечения защиты ПДн в ИСПДн осуществляет следующие функции:

– вносит изменения в список пользователей ИСПДн и осуществляет соответствующие настройки общесистемного и прикладного ПО;

– обеспечивает подготовку предложений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПДн;

– осуществляет взаимодействие с подразделениями Банка.

6.8. Руководители подразделений, работникам которых предоставлен доступ к ПДн:

– формируют заявки на допуск пользователей к обработке ПДн в ИСПДн;

– организуют соблюдение требований безопасности ПДн и выполнение мероприятий по защите в подразделениях Банка;

– готовят предложения по внесению изменений или дополнений в Перечень обрабатываемых персональных данных, Перечень подразделений и сотрудников, осуществляющих обработку ПДн, Перечень ИСПДн Банка, Перечень материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, необходимые для выполнения функций и задач подразделений по обработке ПДн.

6.9. Работники, которым предоставлен доступ к ПДн в рамках обработки без использования средств автоматизации, непосредственно реализуют организационные меры по обеспечению сохранности носителей ПДн и соблюдению порядка обработки ПДн в соответствии с локальными правовыми актами Банка.

6.10. Пользователи ИСПДн непосредственно реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил безопасности информации.

6.11. При определении полномочий пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн Банка, рекомендуется соблюдать принцип разделения ролей.

6.12. Перечень лиц, ответственных за обеспечение безопасности ПДн, устанавливается Приказом Президента Банка.

7. Защита ПДн при обработке без использования средств автоматизации

7.1. Требования к обеспечению безопасности ПДн при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

7.2. Порядок обработки ПДн без использования средств автоматизации устанавливается Положением об обработке персональных данных в ООО КБ «Альба Альянс».

7.3. Данный способ обработки ПДн (а также состав ПДн и перечень лиц, допущенных к обработке) указывается в Перечне обрабатываемых персональных данных и Перечне подразделений и сотрудников, осуществляющих обработку

персональных данных.

7.4. Защита ПДн, обрабатываемых без использования средств автоматизации, обеспечивается выполнением следующих мероприятий:

– определением мест хранения персональных данных (материальных носителей) и перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечением раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях в соответствии с Положением об обработке персональных данных в ООО КБ «Альба Альянс» и Перечень мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации;

– соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

– установлением порядка прекращения обработки и уничтожения или обезличивания ПДн.

7.5. Уничтожение персональных данных должно проводиться в соответствии с Регламентом уничтожения персональных данных в ООО КБ «Альба Альянс».

8. Защита ПДн при обработке в информационных системах персональных данных

8.1. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

– моделирование угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе частной модели угроз и нарушителя;

– определение требуемого уровня защищенности ПДн при их обработке в ИСПДн;

– разработку на основе частной модели угроз и нарушителя с учетом требуемого уровня защищенности ПДн системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– описание системы защиты персональных данных;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;

– учет лиц, допущенных к обработке персональных данных в информационной системе;

– контроль соблюдения мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных, включая контроль условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения машинных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– принятие мер в случае обнаружения фактов несанкционированного доступа к персональным данным;

– восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8.2. Методы и способы защиты персональных данных включают в себя:

– реализацию разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрацию действий пользователей, контроль несанкционированного доступа и действий пользователей, посторонних лиц;

– учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;

– управление изменениями конфигурации ИСПДн и системы защиты персональных данных;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, только в пределах охраняемой территории (рабочие станции, серверы, коммутационное оборудование, сетевые принтеры);

– организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку персональных данных;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок с использованием средств антивирусной защиты.

8.3. Моделирование угроз безопасности и выбор уровня защищенности

8.3.1. Частная модель нарушителя и угроз безопасности персональных данных при их обработке в информационных системах персональных данных разрабатывается с использованием методических документов ФСТЭК России и/или ФСБ России. Результаты определения типа актуальных угроз безопасности ПДн при их обработке в ИСПДн и их состава утверждаются Приказом Президента Банка.

8.3.2. Частная модель нарушителя и угроз безопасности ПДн при их обработке в ИСПДн должна включать:

– исходные данные для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

– совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

– тип и перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн;

– описание потенциального нарушителя;

– требуемый класс СКЗИ, позволяющих обеспечить безопасность ПДн.

8.3.3. Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

8.3.4. Частная модель нарушителя и угроз безопасности ПДн должна периодически пересматриваться в соответствии с Планом внутренних проверок состояния защиты ПДн.

8.3.5. Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется в случае изменения:

– технологических процессов обработки ПДн;

– состава средств защиты информации в ИСПДн;

– характеристик ИСПДн, влияющих на уровень защищенности (изменения типа ИСПДн, количества субъектов ПДн в ИСПДн, изменения категории обрабатываемых ПДн в ИСПДн).

8.3.6. На основе определенного типа угроз безопасности ПДн и характеристик ИСПДн в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности ПДн при их обработке в ИСПДн.

8.4. Порядок разработки, ввода в действие и эксплуатации СЗПДн

8.4.1. Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

8.4.2. Требования по защите ПДн для каждой ИСПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

8.4.3. При формировании требований к СЗПДн должны быть учтены:

– положения законодательства РФ и руководящих документов ФСТЭК России и ФСБ России, актуальных на момент разработки требований;

– результаты разработки частной модели нарушителя и угроз, в частности, выполнение требований должно обеспечивать нейтрализацию предполагаемых актуальных угроз безопасности ПДн;

– необходимость обеспечения определенного уровня защищенности ПДн при их обработке в ИСПДн.

8.4.4. Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн, проводятся следующие мероприятия:

– обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн;

– проектирование и реализация ИСПДн и СЗПДн в её составе;

– ввод в действие СЗПДн, включающий опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.

8.4.5. Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случаях, если:

- изменился состав обрабатываемых ПДн;
- изменился состав или структура самой ИСПДн, или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн), или технологический процесс обработки ПДн, вследствие чего произошли изменения в структуре ИСПДн;
- изменился состав угроз безопасности ПДн в ИСПДн.

8.4.6. В случае изменения характеристик ИСПДн, влияющих на уровень защищенности ИСПДн, проводится пересмотр уровня защищенности ПДн при их обработке в ИСПДн и повторная оценка эффективности принимаемых мер по обеспечению безопасности ПДн.

8.5. Разрешительная система допуска пользователей к информационным ресурсам

8.5.1. Разграничение доступа пользователей к ИСПДн, должно осуществляться на основании Перечня подразделений и сотрудников ООО КБ «Альба Альянс», осуществляющих обработку персональных данных.

8.5.2. Пользователям, администраторам и администраторам безопасности ИСПДн должны назначаться минимально необходимые права и привилегии в ИСПДн.

8.5.3. Допуск работника к ПДн, уровень прав доступа для каждой ИСПДн должны оформляться в виде заявки от руководителей подразделений Банка. Форма заявки приведена в Приложении 1.

8.5.4. Заявка передается Лицу, ответственному за организацию обработки ПДн, на утверждение. Заявка должна храниться в Управлении информационных технологий в течение всего срока эксплуатации ИСПДн.

8.5.5. В случае изменения организационно-штатной структуры, при увольнении или изменении должности работника на основании информации Управления по работе с персоналом и руководителей подразделений проводится актуализация Перечня подразделений и сотрудников ООО КБ «Альба Альянс», осуществляющих обработку персональных данных.

8.5.6. На периодической основе или после каждого изменения в ИСПДн работники Отдела защиты информации должны проводить проверку соответствия прав пользователей, определенных Перечнем подразделений и сотрудников ООО КБ «Альба Альянс», осуществляющих обработку персональных данных, с действующими правами доступа к ИСПДн.

8.6. Регистрация действий пользователей

8.6.1. Регистрация действий пользователей должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

8.6.2. Подлежат обязательной регистрации следующие операции, осуществляемые в ИСПДн:

- регистрация входа (выхода) пользователей в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа;

– регистрация действий администраторов системы.

8.7. Обеспечение безопасности при хранении носителей информации ПДн

8.7.1. Учет защищаемых съемных носителей ПДн – компакт-дисков, flash-накопителей – должен осуществляться в Журналах учета электронных носителей ПДн (типовая форма журнала приведена в Положении об обработке персональных данных в ООО КБ «Альба Альянс»).

8.7.2. Обязанность по ведению учета защищаемых съемных носителей ПДн возлагается на Управление информационных технологий.

8.7.3. В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых съемных носителей ПДн необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с защищаемых съемных носителей ПДн должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя в соответствии с Регламентом уничтожения персональных данных в ООО КБ «Альба Альянс».

8.8. Резервирование технических средств, дублирование массивов и носителей информации

8.8.1. Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты информации при их случайной или намеренной модификации должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

8.8.2. Для обеспечения целостности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие механических повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

8.9. Использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия

В качестве СЗИ, прошедших процедуру оценки соответствия, используются СЗИ, сертифицированные в системах сертификации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации в пределах их полномочий.

При использовании средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией;

– проведение обучения лиц, использующих средства защиты информации, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и

технической документации к ним. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 2. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним приведена в Приложении 3;

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

– периодическое тестирование средств защиты в соответствии с эксплуатационной документацией на СЗИ. Форма журнала проведения периодического тестирования СЗИ приведена в Приложении 4;

– разбирательство и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению целостности, конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

8.10. Использование защищенных каналов связи

8.10.1. При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) 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.

8.10.2. Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена дополнительно должны применяться 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 данных;

– управление доступом к защищаемым персональным данным информационной сети;

– использование атрибутов безопасности.

8.10.3. Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем

и проверка подлинности пользователей и целостности передаваемых данных.

8.10.4. Защита каналов связи реализуется следующими организационно-техническими способами:

– размещение линий связи и сетевого оборудования в пределах контролируемой зоны;

– использование волоконно-оптических линий связи, затрудняющих или исключающих возможность перехвата передаваемой информации;

– использование средств криптографической защиты, если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации.

8.11. Физическая защита помещений и технических средств

8.11.1. Размещение ИСПДн и охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.11.2. Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) Банка.

8.11.3. Границами КЗ могут являться:

– периметр охраняемой территории Банка;

– ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории;

– стены помещений Банка.

8.11.4. В состав КЗ должны входить:

– помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;

– помещения, в которых проходят кабельные линии связи ИСПДн;

– помещения, в которых хранятся бумажные носители ПДн (архивы, помещения работников Банка).

8.11.5. Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

8.11.6. Доступ посторонних лиц (посетителей, работников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников Банка.

8.11.7. Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8.11.8. Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны сдаваться под роспись работникам охранной организации.

8.11.9. Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и/или носители ключевой, аутентифицирующей и парольной информации СКЗИ, оснащаются

входными дверьми и техническими средствами контроля доступа. Работники обеспечивают постоянное закрытие дверей помещений и их открытие только для санкционированного прохода по электронным пропускам, а также постановку помещения на охранную сигнализацию по окончании рабочего дня.

8.11.10. В нерабочее время доступ в КЗ Банка должен быть исключен следующими мерами:

– заключением договора с охранным предприятием, обязательными условиями которого являются следующие обязанности:

o организация и обеспечение контроля доступа в помещения работников и посетителей в рабочее время;

o организация и обеспечение охраны помещений в нерабочее время, а также в выходные и праздничные дни;

o не допускать проникновения и пребывания посторонних лиц в помещениях в нерабочее время, а также в выходные и праздничные дни. При необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом;

o внос и вынос материальных ценностей в помещения и из помещений осуществляется только в присутствии ответственного лица.

8.11.11. В случае заключения договора с арендодателем для реализации мер по организации доступа в КЗ Банка обязательным условием является обязательное присутствие работников банка при предоставлении доступа сотрудников арендодателя в помещения серверных, к коммутационному оборудованию.

8.12. Использование средств антивирусной защиты

8.12.1. Подсистема антивирусной защиты реализуется путем внедрения специального антивирусного программного обеспечения на рабочих станциях и серверах ИСПДн.

8.12.2. Средства антивирусной защиты предназначены для реализации следующих функций:

– антивирусное сканирование;

– блокирование вредоносных программ;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

8.12.3. Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять работников Управления информационных технологий.

8.13. Управление изменениями конфигурации информационной системы и системы защиты персональных данных

8.13.1. Действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных разрешены только работникам Управления информационных технологий под контролем администраторов безопасности.

8.13.2. До внесения изменений в состав технических и программных средств ИСПДн проводится экспертный анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных.

8.14. Порядок оценки эффективности принимаемых мер по обеспечению безопасности ПДн в ИСПДн

8.14.1. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн в ИСПДн может проводиться в виде внутренней оценки (рабочей группой по информационной безопасности в соответствии с требованиями нормативных правовых актов) или добровольной аттестации на соответствие требованиям безопасности информации.

8.14.2. Оценка эффективности (в любой выбранной форме) проводится до ввода в действие новых ИСПДн, в случае изменений в ИСПДн, существенно влияющих на эффективность защиты ПДн, а также периодически, не реже 1 раза в 3 года.

8.14.3. Для ИСПДн, оценка эффективности принимаемых мер которых проводится в виде внутренней оценки, необходимо выполнять следующие требования:

- оценка эффективности принимаемых мер осуществляется на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии;
- в случае проведения оценки на основе собственных доказательств рабочая группа самостоятельно формирует комплект документов, послуживших мотивированным основанием для подтверждения соответствия информационной системы персональных данных всем необходимым требованиям;
- результаты оценки эффективности принимаемых мер должны содержать:
  - наименование и местонахождение ИСПДн;
  - информацию об объекте подтверждения соответствия;
  - наименование документов, на соответствие требованиям которых оценивается ИСПДн;
  - сведения о принятых мерах по обеспечению соответствия ИСПДн необходимым требованиям;
  - сведения о документах, послуживших основанием для подтверждения соответствия ИСПДн требованиям;
  - срок действия оценки и условия повторной оценки.

8.14.4. Добровольная аттестация ИСПДн на соответствие требованиям безопасности информации проводится в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утвержденным председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г., а также ГОСТ РО 0043-003-2012. Организация, проводящая добровольную аттестацию ИСПДн, должна быть лицензирована уполномоченным федеральным органом исполнительной власти на проведение работ по технической защите информации.

8.15. Защита персональных данных при трансграничной передаче

8.15.1. Защита персональных данных при их передаче, обработке на территории иностранных государств осуществляется в соответствии с положениями Конвенции о защите физических лиц при автоматизированной обработке персональных данных ETS N 108 (Страсбург, 28 января 1981 г.) (с изменениями от 15 июня 1999 г.), Директивы Европейского парламента и Совета Европейского союза N 95/46/ЕС «О защите физических лиц в условиях автоматизированной обработки персональных данных и о свободном обращении этих данных», а также с учетом национальных законодательств, нормативных актов и административных положений государств-участников, в которых располагаются используемые средства обработки персональных данных.

8.15.2. До начала осуществления трансграничной передачи Банк обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.

9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных

9.1. Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

9.2. Контроль состояния защиты ПДн должен осуществляться в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных. Форма журнала учета проведения мероприятий приведена в Приложении 5.

9.3. Проведение контроля состояния защиты включает в себя мероприятия по оценке:

– соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знания и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

9.4. Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

10. Принятие мер в случае обнаружения фактов нарушения требований (несанкционированного доступа к ПДн), разбирательство и составление заключений по фактам нарушения требований безопасности

10.1. Лицо, обнаружившее факт нарушения требований безопасности информации, незамедлительно уведомляет подразделение информационной безопасности о факте нарушения.

10.2. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения, и принять меры к их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

10.3. Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

10.4. Порядок проведения расследования причин и условий возникновения нарушения требований (НСД к ПДн) определяется отдельными локальными правовыми актами Банка.

10.5. В случае если вследствие НСД ПДн были модифицированы или уничтожены, осуществляется восстановление ПДн из резервной копии.

11. Требования к персоналу по обеспечению защиты ПДн

11.1. При вступлении в должность нового работника непосредственный руководитель подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн (Положением об обработке персональных данных в ООО КБ «Альба Альянс», настоящим положением). Работники Отдела защиты информации организуют проведение обучения навыкам выполнения процедур, необходимых для работы в ИСПДн Банка и выполнения требований по

защите ПДн, и знакомят под роспись с Инструкцией работнику по обеспечению безопасности при работе с персональными данными.

11.2. Работники должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки персональных данных, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

11.3. Работники должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн в момент заключения трудового договора с начальником Управления по работе с персоналом.

12. Порядок внесения изменений

12.1. Настоящее Положение пересматривается Отделом защиты информации совместно и (или) по согласованию с Управлением информационных технологий, подразделениями Банка, в зоне компетенции которых находятся вопросы выполнения банковских технологических процессов по обработке персональных данных.

12.2. Плановый пересмотр положений настоящего Положения должен осуществляться не реже одного раза в три года. При необходимости, в случае изменения законодательства в области защиты ПДн, инициируется внесение соответствующих изменений.

12.3. Измененное Положение утверждается в установленном порядке.