Акционерное общество коммерческий банк
«Михайловский Промжилстройбанк»

У Т В Е Р Ж Д Е Н О

Правлением АО КБ «Михайловский ПЖСБ»

Протокол № 247 от « 29 » декбря 2017 г.

Председатель Правления

_____ В.Г. Прохорова

ЧАСТНАЯ ПОЛИТИКА
обеспечения безопасности персональных данных в информационных системах в АО КБ «Михайловский ПЖСБ»

город Михайловка Волгоградской области

2017

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Частная политика обеспечения безопасности персональных данных в информационных системах АО КБ «Михайловский ПЖСБ» (далее – Частная политика, Политика) определяет стратегию защиты персональных данных, обрабатываемых в ИСПДн Банка, и формулирует основные принципы и механизмы защиты ПДн. Политика является основным руководящим документом Банка, определяющим требования, предъявляемые к обеспечению безопасности ПДн.

1.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.3. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.4. Сокращения, условные обозначения, термины, используемые в целях Политики:

Банк -	АО КБ «Михайловский ПЖСБ»
ВП -	Вредоносная программа
ГРИИБ -	Группа реагирования на инциденты информационной безопасности
ИБ -	Информационная безопасность
ИС -	Информационные системы
ИСПДн -	Информационные системы персональных данных
ЛВС -	Локальная вычислительная сеть
МЭ -	Межсетевой экран
НСД -	Несанкционированный доступ
ОИОАОиПД -	Отдел информационного обеспечения, автоматизации обработки и передачи данных
ОС -	Операционная система
ПДн -	Персональные данные
ПМВ -	Программно-математические воздействия
ПО -	Программное обеспечение
РД -	Руководящий документ
САЗ -	Средство анализа защищенности
СВТ -	Средства вычислительной техники
СЗИ -	Средства защиты информации
СЗПДн -	Система защиты персональных данных
СОВ -	Система (средство) обнаружения вторжения
ФСТЭК -	Федеральная служба по техническому и экспортному контролю России

2. ЦЕЛИ, ЗАДАЧИ И ОБЛАСТЬ ПРИМЕНЕНИЯ ПОЛИТИКИ

2.1. Цель настоящей Частной политики - обеспечение безопасности информации, содержащей персональные данные, циркулирующей в Банке, а также реализация положений законодательных актов Российской Федерации и нормативных требований по защите персональных данных и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения персональных данных, их незаконного использования и нарушения работы информационно-телекоммуникационной системы Банка.

2.2. Основными целями обеспечения безопасности персональных данных являются:

2.2.1. предотвращение нарушений прав субъекта персональных данных (физического лица) на сохранение конфиденциальности информации, циркулирующей в ИСПДн Банка;

2.2.2. предотвращение искажения или несанкционированной модификации, уничтожения, блокирования информации, содержащей персональные данные, циркулирующей в ИСПДн Банка;

2.3. Для решения поставленных целей предполагается решение следующих задач:

2.3.1. определение принципов обработки ПДн;

2.3.2. определение требований и рекомендаций к процедурам обработки ПДн;

2.3.3. определение мероприятий по обеспечению безопасности ПДн;

2.3.4. определение мероприятий по обеспечению прав субъектов ПДн;

2.3.5. определение порядка контроля соблюдения Политики.

2.4. Требования настоящей Частной политики обязательны для всех структурных и обособленных подразделений Банка и распространяются на:

2.4.1. автоматизированные системы Банка;

2.4.2. средства телекоммуникаций;

2.4.3. информационные ресурсы и носители информации;

2.4.4. помещения;

2.4.5. работников Банка.

2.5. Внутренние документы Банка, затрагивающие вопросы, рассматриваемые в данном документе, должны разрабатываться с учетом положений настоящей Частной политики и не противоречить им.

3. КЛАССИФИКАЦИЯ ИНФОРМАЦИОНЫХ СИСТЕМ

3.1. В Банке устанавливается следующий подход отнесения информационной системы к ИСПДн:

3.1.1. решение об отнесении информационной системы к ИСПДн принимается с учетом целей создания и использования информационной системы, вида реализуемого информационной системой технологического процесса и обрабатываемых в информационной системе ПДн;

3.1.2. к ИСПДн относятся информационные системы, одной из целей создания и использования которых является обработка ПДн;

3.2. В Банке устанавливается следующий подход к классификации ИСПДн:

3.2.1. классификация ИСПДн Банка производится в соответствии с требованиями законодательства Российской Федерации;

3.2.2. классификация ИСПДн производится на основе категорий, обрабатываемых ПДн и количества субъектов ПДн, обрабатываемых в ИСПДн;

3.2.3. для ИСПДн банка актуальны угрозы безопасности ПДн 2-го типа, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

3.2.4. для ИСПДн банка необходимо обеспечивать 2-й уровень защищенности ПДн.

4. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В информационной системе Банка осуществляется обработка, передача, накопление и хранение информации, содержащей персональные данные, которая в соответствии с действующим законодательством РФ, подлежит защите.

4.2. В Банке определены следующие основания для обработки информации, содержащей персональные данные:

4.2.1. ст. 5 Федерального Закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»;

4.2.2. ст. 7 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»;

4.2.3. Положение Банка России от 15.10.2015 № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», разработанное на основании Федерального закона № 115-ФЗ.

4.3. Цель обработки информации, содержащей персональные данные:

4.3.1. Предоставление услуг в банковской сфере;

4.3.2. Взаимодействие с государственными органами для обмена данными (Пенсионный Фонд, ФОМС, ФНС и т.д.).

4.4. Определен следующий перечень категорий персональных данных физических лиц, обрабатываемых в ИСПДн Банка:

4.4.1. Персональные данные, предоставляемые Банку физическими лицами-субъектами персональных данных (определены в Приложении №1 к настоящей Частной политике).

4.4.2. Общедоступные персональные данные;

4.4.3. Специальные категории персональных данных (ст. 10 Федерального закона «О персональных данных»), а также биометрические персональные данные (ст. 11 Федерального закона «О персональных данных») Банком не обрабатываются.

4.5. Персональные данные, предоставляемые физическими лицами Банку, в зависимости от цели предоставления подразделяются на:

4.5.1. ПД лиц, обратившихся за получением кредита на условиях, объявленных Банком;

4.5.2. ПД лиц, обратившихся в Банк с предложением предоставить обеспечение по кредитным договорам;

4.5.3. ПД лиц, заключивших с Банком договор банковского вклада;

4.5.4. ПД лиц, заключивших с Банком договор банковского счета;

4.5.5. ПД лиц, осуществляющих перевод денежных средств без открытия счета.

4.5.6. ПД лиц, осуществляющих перечисление денежных средств без открытия счета по системам денежных переводов («Вестерн Юнион», «Золотая Корона», «Лидер» и т.п.).

4.5.7. ПД лиц, с которыми Банк заключил договор на поставку товара, оказание услуг, выполнение работ с целью обеспечения финансово-хозяйственной деятельности;

4.5.8. ПД лиц, обратившихся в Банк с запросом любого характера и предоставившие при этом свои персональные данные;

4.5.9. ПД работников Банка, заключивших с Банком трудовой договор;

4.5.10. ПД лиц, обратившихся в Банк с целью трудоустройства.

4.6. Субъектами обрабатываемых персональных данных выступают:

4.6.1. Клиенты Банка (их представители);

4.6.2. Контрагенты Банка (их представители);

4.6.3. Работники Банка.

4.7. Период обработки и хранения персональных данных соответствует требованиям, установленным целями обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

4.8. Перечень категорий персональных данных, обрабатываемых в подразделениях Банка, а также ответственные лица, определены в Приложении №2 к настоящей Частной политике.

5. ОБЩИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Организационная структура по обеспечению безопасности персональных данных.

5.1.1. Должностной обязанностью каждого работника, имеющего доступ к персональным данным, в том числе является соблюдение требований законодательства и внутренних документов Банка о защите персональных данных, ставших ему известными в процессе выполнения своих обязанностей. Эта обязанность включена в должностную инструкцию, с которой каждый сотрудник знакомится под роспись.

5.1.2. Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляет Администратор информационной безопасности. К числу его функциональных обязанностей относится:

5.1.2.1. Общеметодологическое руководство;

5.1.2.2. Определение принципов защиты информации;

5.1.2.3. Контроль выполнения мер и мероприятий по защите информации.

5.1.2.4. Организация и проведение мероприятий по обеспечению безопасности ПДн;

5.1.2.5. Организация эксплуатации технических и программных средств защиты информации;

5.1.2.6. Отслеживание всех возможностей несанкционированного доступа к информации, а также возможностей нарушения работы программно-аппаратных комплексов ИСПДн третьими лицами;

5.1.2.7. Проведение мониторинга защищённости всех компонент ИСПДн;

5.1.2.8. Расследование зафиксированных случаев как успешных, так и предотвращенных попыток НСД (в составе ГРИИБ);

5.1.2.9. Выработка рекомендаций по повышению уровня защищённости ресурсов ИСПДн;

5.1.2.10. Настройка и сопровождение программных и аппаратных систем защиты ПДн;

5.1.3. Настройку и поддержание нормального функционирования информационных систем Банка осуществляет ОИОАОиПД. В обязанности работников данного подразделения входит:

5.1.3.1. Обеспечение безотказного функционирования технических средств ИСПДн;

5.1.3.2. Обеспечение штатного режима функционирования программного обеспечения серверов и рабочих станций ИСПДн;

5.1.3.3. Осуществление мониторинга состояния ресурсов и компонент ИСПДн;

5.1.3.4. Осуществление резервного копирования информации и обеспечение оперативного восстановления систем при сбоях;

5.1.3.5. Своевременная модернизация программного и аппаратного обеспечения.

5.1.3.6. Контроль ПО в течение всего жизненного цикла для всех типов платформ (включая инсталляцию, поддержку и удаление ПО);

5.1.3.7. Установка, настройка и поддержка работоспособности баз данных;

5.1.3.8. Участие в расследованиях зафиксированных случаев как успешных, так и предотвращенных попыток НСД (в составе ГРИИБ);

5.1.4. Обработка персональных данных осуществляется работниками, в соответствии с их должностными обязанностями. Работники обязаны соблюдать положения данной Политики, а также своих должностных инструкций, организационно-распорядительных документов по обеспечению ИБ и правил работы в ИС в рамках выполнения своих должностных полномочий по обработке ПДн.

5.2. Требования к организационным мероприятиям по обеспечению безопасности персональных данных.

5.2.1. Основой организационных мероприятий по обеспечению безопасности ПДн является набор регламентирующих документов по защите ПДн и настоящая Частная политика, в частности. Данные документы определяют стратегию и требования по защите ПДн. Положения данных документов должны быть доведены до всех работников, ответственных за безопасность ПДн.

5.2.2. Мероприятия по обеспечению безопасности ПДн должны проводиться в соответствии с требованиями нормативно-правовых документов, в частности:

5.2.2.1. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

5.2.2.2. Конституция РФ;

5.2.2.3. Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные Постановлением Правительства РФ от 01.11.2012 г. № 1119.

5.2.2.4. Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утв. Постановлением Правительства РФ от 15 сентября 2008 г. № 687.

5.2.2.5. Стандарта Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения»

5.2.3. Обеспечение безопасности персональных данных, а также разработка и внедрение СЗПДн, основывается на выявленных актуальных угрозах безопасности.

5.2.4. Система управления информационной безопасности ПДн, строится с учетом контроля выполнения мероприятий по обеспечению безопасности ПДн, их полноту и достаточность для обеспечения необходимого уровня защищенности.

5.2.5. Работники Банка под роспись ознакамливаются с положениями настоящей Частной политики, а также иных нормативных документов, регламентирующих работу с персональными данными и ответственностью за нарушение данных положений.

5.2.6. Отдельно регламентируются процессы предоставления информации третьим лицам и процессы обеспечения безопасности ПДн при их передаче. Должны быть назначены работники, ответственные за обеспечение безопасности ПДн при их передаче, определены их обязанности и ответственность.

5.2.7. Четко регламентируются меры по обеспечению физической безопасности ПДн.

5.2.8. Четко регламентируется использование носителей информации, содержащих ПДн.

5.2.9. На постоянной основе производятся обучения и тренинги работников Банка, ответственных за обеспечение безопасности ПДн.

5.2.10. Четко регламентируются процессы эксплуатации и контроля средств защиты ПДн.

5.3. Требования к мероприятиям по технической защите персональных данных.

5.3.1. Для защиты ПДн, обрабатываемых в ИСПДн Банка внедрена система защиты персональных данных (СЗПДн) – комплекс информационных систем обеспечения информационной безопасности, позволяющий обеспечить конфиденциальность, целостность и доступность ПДн, хранящихся и обрабатываемых в Банке.

5.3.2. Обоснование комплекса мероприятий по обеспечению безопасности ПДн в ИСПДн производится с учетом результатов оценки опасности угроз, согласно частной модели угроз и определения уровня защищенности персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства от 01.11.2012 г. № 1119.

5.3.3. СЗПДн включает в себя следующие системы обеспечения безопасности ПДн:

5.3.3.1. система управления доступом;

5.3.3.2. система регистрации и учета в ИСПДН;

5.3.3.3. система обеспечения целостности данных;

5.3.3.4. система антивирусной защиты;

5.3.3.5. система обнаружения вторжений;

5.3.3.6. система криптографической защиты.

5.3.4. Защита ПДн обеспечивается на всех технологических этапах передачи, обработки и хранения ПДн и при всех режимах работы ИСПДн, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе средства защиты от НСД не должны ухудшать основные функциональные характеристики системы.

5.3.5. Обеспечивается непрерывное функционирование подсистем защиты ПДн с установленными параметрами, позволяющими обеспечивать безопасность ПДн в соответствии с заданными требованиями.

5.3.6. Реализуется защищенная среда хранения и обработки ПДн, позволяющая предоставлять доступ к ПДн только авторизованным для этого работникам Банка.

5.3.7. Обеспечивается защита ПДн от разглашения или утечки.

5.3.8. Реализуется защита ПДн от подмены или модификации.

5.3.9. Реализуется система резервного копирования данных, позволяющая восстановить утерянную информацию.

5.3.10. Внедряемые системы защищаются от сбоев в работе и в случае их отказа защищённость ПДн не нарушается.

5.3.11. Используемые технические и программные средства удовлетворяют устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

6. ТРЕБОВАНИЯ ПО РЕАЛИЗАЦИИ ОРГАНИЗАЦИОННЫХ МЕР

6.1. Все работники Банка, ответственные за обеспечение безопасности ПДн, ознакамливаются под роспись с регламентирующими документами по обеспечению безопасности ПДн.

6.2. Все регламентирующие документы поддерживаются в актуальном состоянии с учетом положений и возможных изменений законодательных актов в области защиты ПДн, изменений структуры ИСПДн, режима обработки ПДн, организационных и иных изменений в структуре Банка.

6.3. Утвержденная в Банке частная модель угроз безопасности отражает актуальное состояние защищенности ИСПДн и актуальные угрозы безопасности ПДн. Разработка модели угроз безопасности осуществляется на основании анализа

существующих угроз безопасности и возможности их реализации в обследуемой ИСПДн, в соответствии с уровнем её защищенности, используемым средствам обеспечения ИБ и моделью нарушителя.

6.4. Разработка модели актуальных угроз безопасности ПДн осуществляется в соответствии со следующими документами:

6.4.1. «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», утв. ФСТЭК от 15 февраля 2008 г.

6.4.2. «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утв. ФСТЭК от 14 февраля 2008 г.

6.5. Система управления обеспечением безопасности ПДн представляет собой комплекс организационных мероприятий, позволяющих производить контроль и оценку СЗПДн и обеспечения безопасности ПДн в целом.

6.6. В рамках управления обеспечением безопасности ПДн решаются следующие задачи:

6.6.1. Контроль осуществления имеющихся мер по обеспечению безопасности ПДн.

6.6.2. Контроль выполнения требований нормативных документов по обеспечению безопасности ПДн.

6.6.3. Определение полноты и достаточности имеющихся мер по обеспечению безопасности ПДн.

6.6.4. Осуществление и контроль информирования работников Банка о вопросах защиты ПДн.

6.6.5. Сбор и анализ информации о событиях ИБ.

6.6.6. Совершенствование существующей СЗПДн и процессов обеспечения безопасности ПДн.

6.7. Устанавливается режим обработки ПДн, определяющий:

6.7.1. Порядок отнесения информации к ПДн;

6.7.2. Определение срока хранения информации в ИСПДн;

6.7.3. Порядок получения доступа работниками Банка к ПДн;

6.7.4. Соответствие ролей и обязанностей работников назначаемым им правам доступа к ПДн;

6.7.5. Определение средств обработки ПДн;

6.7.6. Определение порядка обработки ПДн (включая инструкции по хранению, обработке и передаче ПДн с использованием СВТ);

6.7.7. Определение порядка неавтоматизированной обработки ПДн;

6.7.8. Определение порядка удаления ПДн и безопасного уничтожения/очистки носителей информации;

6.7.9. Процесс передачи ПДн третьим лицам, с которыми ведется обмен ПДн, четко регламентируется. При регламентировании процесса передачи ПДн третьим лицам необходимо установить:

- Тип и объем передаваемых данных;
- Формат передаваемых данных;
- Порядок согласования передачи данных (лицо, предоставляющее право на передачу ПДн, оформление заявки на передачу ПДн, обоснование необходимости передачи ПДн);
- Работников, ответственные за осуществление передачи данных;
- Каналы передачи ПДн;
- Средства передачи ПДн;
- Меры по обеспечению безопасности ПДн при передаче третьим лицам.

6.8. Устанавливается ответственность третьих лиц за обеспечение конфиденциальности ПДн при её передаче им.

6.9. Процесс получения согласия субъекта персональных данных на обработку его ПДн, регламентируется в соответствии с 152-ФЗ, в том числе разработаны формы

такого согласия, которые включаются в используемые договора и соглашения с субъектами ПДн для ознакомления и подписи.

6.10. Физическая безопасность ИСПДн, включает в себя:

6.10.1. Контроль доступа на защищаемую территорию. Должен быть реализован пропускной режим доступа на территорию Банка. Доступ должен предоставляться работникам Банка в соответствии с выданными пропусками, позволяющими осуществлять персональную идентификацию.

6.10.2. Контроль вноса и выноса средств вычислительно техники. Для вноса и выноса средств вычислительно техники должно оформляться персональное разрешение с указанием целей проноса и выноса и описанием СВТ или носителей информации.

6.10.3. Контроль доступа в помещения, в которых располагается техническое оборудование, участвующее в хранении, обработке и передаче ПДн, а также носители данных, содержащие ПДн с возможностью персональной идентификации субъектов доступа.

6.10.4. Предотвращение несанкционированного доступа к оборудованию, участвующему в хранении, обработке и передаче ПДн.

6.10.5. Оборудование размещается в помещениях со строгим контролем доступа и журналом аудита доступа, в закрытых шкафах. Оборудование опечатывается.

6.10.6. Защита носителей информации, содержащих ПДн от несанкционированного доступа, хищения и подмены.

6.11. Носители информации, содержащие ПДн, размещаются в защищаемых помещениях, в сейфах.

6.12. Обеспечивается безопасность каналов передачи данных.

6.13. Каналы передачи данных защищаются от возможных угроз несанкционированного съема информации, внедрения или подмены объектов сети, а также от нарушения целостности и доступности.

6.14. Учитываются все точки подключения и блокируются неиспользуемые.

6.15. Обеспечивается контроль каналов передачи данных, располагающихся на контролируемой защищаемой территории, постоянно осуществляется контроль их состояния.

6.16. Используются системы охранной сигнализации.

6.17. Используются системы пожарной сигнализации.

6.18. Используются системы видеонаблюдения.

6.19. Размещение и установка технических средств исключает возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения.

6.20. Уборка или иные работы в помещениях, которых осуществляется хранение или обработка ПДн, производится в присутствии ответственного работника Банка с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

6.21. Контролируются действия гостей, клиентов и иных лиц, имеющих временный доступ на защищаемую территорию.

6.22. Четко регламентируется процесс предоставления доступа третьим лицам на защищаемую территорию.

6.23. Ведется журнал учета доступа третьих лиц на защищаемую территорию.

6.24. Для каждого гостя или группы гостей назначается ответственный работник Банка, который должен сопровождать во время их пребывания на защищаемой территории.

6.25. Гости не имеют возможности доступа в помещения, в которых размещается оборудование, участвующее в обработке и хранении ПДн, а также носители информации, содержащие ПДн, за исключением случаев, когда данная необходимость обусловлена оказанием специальных услуг. В данном случае ответственный работник Банка постоянно контролирует действия гостей.

6.26. При использовании электронных материальных носителей информации, содержащих ПДн, реализованы следующие меры:

6.26.1. Все материальные носители имеют маркировку, определяющую содержащуюся в них информацию и режим её обработки: для ПДн должна быть маркировка «Конфиденциально - ПДн».

6.26.2. Определен срок использования материальных носителей информации и хранимой на них информации.

6.26.3. Ведется реестр материальных носителей ПДн и проводится их регулярная инвентаризация.

6.26.4. Обеспечивается безопасное хранение материальных носителей ПДн.

6.27. При хранении материальных носителей ПДн соблюдаются условия, обеспечивающие сохранность персональных данных. Хранение материальных носителей ПДн осуществляется в шкафах (сейфах) в помещениях, исключающих несанкционированный доступ к ним.

6.28. Ответственность за обеспечение безопасности информации, хранящейся на материальных носителях ПДн, несут работники Банка, использующие материальные носители.

6.29. Работники Банка, осуществляющие обработку ПДн и ответственные за обеспечение её безопасности, ознакамливаются со всеми требованиями по обеспечению безопасности ПДн под личную роспись.

6.30. Все изменения в порядке осуществления защиты ПДн и работы с ИСПДн, своевременно доводятся до работников Банка.

6.31. Работники Банка, осуществляющие обработку ПДн и ответственные за обеспечение её безопасности, проходят обучение по вопросам обеспечения безопасности ПДн:

6.31.1. при приеме на работу;

6.31.2. при необходимости в соответствии с Положением об обучении и проверке знаний по вопросам информационной безопасности.

6.32. Эксплуатация средств защиты ПДн осуществляется работниками Банка, в соответствии с их ролями и обязанностями, а также рабочими инструкциями.

6.33. Эксплуатация средств защиты ПДн осуществляется в соответствии с требованиями обеспечения безопасности.

6.34. Администратором информационной безопасности осуществляется контроль эксплуатации и администрирования средств защиты ПДн.

6.35. Обеспечение безопасности ПДн осуществляется в соответствии с регламентирующими документами по защите ПДн в ИСПДн Банка.

7. ТРЕБОВАНИЯ ПО РЕАЛИЗАЦИИ МЕР ТЕХНИЧЕСКОЙ ЗАЩИТЫ

7.1. Система управления доступом.

7.1.1. идентификация и проверка подлинности субъектов доступа осуществляется:

7.1.1.1. при входе в операционную систему ИСПДн по паролю (или с использованием иного механизма аутентификации) условно–постоянного действия длиной не менее восьми буквенно-цифровых символов;

7.1.1.2. при входе в прикладную систему ИСПДн по паролю (или с использованием иного механизма аутентификации) условно–постоянного действия длиной не менее восьми буквенно-цифровых символов.

7.1.2. Предусматриваются механизмы блокирования доступа к ИС при выполнении 3-х неудачных попыток ввода пароля.

7.1.3. Проводится идентификация:

7.1.3.1. файлов,

7.1.3.2. каталогов,

7.1.3.3. томов,

7.1.3.4. внешних устройств,

7.1.3.5. используемых средств защиты,

7.1.3.6. терминалов,

7.1.3.7. технических средств обработки ПДн,

7.1.3.8. ИСПДн,

7.1.3.9. каналов связи,

по их логическим именам или адресам (номерам).

7.1.4. Запрещается любой доступ пользователей к ресурсам, кроме явно разрешённого.

7.1.5. Система контроля доступа по умолчанию запрещает любой доступ.

7.1.6. Осуществляется сокрытие субъектов (объектов) и/или прикладных функций защищаемой сети.

7.1.7. Осуществляется трансляции внешних сетевых адресов и портов.

7.1.8. Осуществляется блокирование доступа, не идентифицированного субъекта или субъекта, не имеющего соответствующих прав доступа.

7.1.9. Фильтрация трафика осуществляется в соответствии:

7.1.9.1. с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

7.1.9.2. независимо для каждого сетевого пакета;

7.1.9.3. с учетом любых значимых полей сетевых пакетов;

7.1.9.4. на транспортном уровне запросов на установление виртуальных соединений;

7.1.9.5. на прикладном уровне запросов к прикладным сервисам;

7.1.9.6. с учетом даты/времени, с возможностью аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети;

7.1.9.7. для пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

7.1.10. На МЭ используется проверка соединений с запоминанием состояния (динамическая фильтрация пакетов, stateful inspection), при которой допускаются только «установленные» входящие соединения.

7.1.11. Осуществляется регистрация и учет запрашиваемых сервисов прикладного уровня и запросов на установление виртуальных соединений.

7.1.12. Обеспечивается возможность дистанционного управления компонентами средств межсетевого экранирования, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

7.1.13. Осуществляется идентификация и аутентификация администратора МЭ при его локальных запросах на доступ с помощью идентификатора и пароля условно-постоянного действия;

7.1.14. Осуществляется регистрация входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

7.1.15. Для управления МЭ используются только защищённые протоколы, исключающие передачу данных в открытом виде.

7.2. Система регистрации и учета.

7.2.1. Осуществляется регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или остановка не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются:

7.2.1.1. дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы,

7.2.1.2. результат попытки входа (успешная или неуспешная – несанкционированная),

7.2.1.3. идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа,

7.2.1.4. код или пароль, предъявленный при неуспешной попытке.

7.2.2. Проводится учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема).

7.2.3. Осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

7.2.3.1. дата и время запуска;

7.2.3.2. имя (идентификатор) программы (процесса, задания);

7.2.3.3. идентификатор субъекта доступа, запросившего программу (процесс, задание);

7.2.3.4. результат запуска (успешный, неуспешный - несанкционированный).

7.2.4. Осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

7.2.4.1. дата и время попытки доступа к защищаемому файлу;

7.2.4.2. указание результата (успешная, неуспешная – несанкционированная);

7.2.4.3. идентификатор субъекта доступа;

7.2.4.4. спецификация защищаемого файла.

7.2.5. Осуществляется регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа:

7.2.5.1. терминалам,

7.2.5.2. рабочим станциям,

7.2.5.3. узлам сети ИСПДн,

7.2.5.4. линиям (каналам) связи,

7.2.5.5. внешним устройствам рабочих станций,

7.2.5.6. программам,

7.2.5.7. томам,

7.2.5.8. каталогам,

7.2.5.9. файлам,

7.2.5.10. записям,

7.2.5.11. полям записей.

7.2.6. В параметрах регистрации указываются:

7.2.6.1. дата и время попытки доступа к защищаемому объекту;

7.2.6.2. указание ее результата (успешная, неуспешная – несанкционированная);

7.2.6.3. идентификатор субъекта доступа;

7.2.6.4. спецификация защищаемого объекта - логическое имя (номер).

7.2.7. Осуществляется очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

7.3. Система обеспечения целостности.

7.3.1. Внедрены системы обеспечения целостности программных средств защиты в составе СЗПДн, а также неизменность программной среды.

7.3.2. Проводятся проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.

7.3.3. Реализуются механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.

7.3.4. Обеспечивается возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности.

7.3.5. Осуществляется резервное копирование ПДн.

7.3.6. Реализуется физическая охрана ИСПДн (устройств и носителей информации), предусматривающая:

7.3.6.1. контроль доступа в помещения ИСПДн посторонних лиц,

7.3.6.2. наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время.

7.4. Система анализа защищенности.

7.4.1. Должно проводиться тестирование функций СЗПДн:

7.4.1.1. регулярно, раз в год,

7.4.1.2. при изменении ИСПДн,

7.4.1.3. при изменениях в СЗПДн;

7.4.1.4. при смене персонала, ответственного за обеспечение безопасности ИСПДн.

7.4.2. Анализ защищенности должен проводиться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) анализа защищенности (САЗ).

7.4.3. Для ИСПДн САЗ должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

7.4.4. Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).

7.4.5. Должны использоваться последние обновления сигнатурных баз для обнаружения актуальных уязвимостей.

7.5. Подсистема антивирусной защиты.

7.5.1. В системе антивирусной защиты на всех технических средствах ИСПДн проводится непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.

7.5.2. Выполняются проверка на предмет наличия ВП:

7.5.2.1. при первом запуске средств защиты ПДн от ПМВ,

7.5.2.2. еженедельно.

7.5.3. При выявлении факта ПМВ, инициируется автоматическая проверка ИСПДн на предмет наличия ВП.

7.5.4. Проводится автоматическая проверка на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.

7.5.5. Реализуются механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.

7.6. Система криптографической защиты.

7.6.1. При передаче ПДн по общим каналам передачи данных используются средства криптографической защиты информации

7.6.2. Рекомендуется осуществлять шифрование ПДн, записываемых на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах

связи, а также на съемные носители данных (диски, ленточные кассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию.

7.6.3. Доступ субъектов к операциям шифрования и криптографическим ключам дополнительно контролируется системой управления доступом.

7.6.4. По возможности используются сертифицированные средства криптографической защиты.

8. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ БАНКА ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Требования настоящей Частной политики обязательны для всех работников Банка, допущенных к работе с ПДн.

8.2. Работники Банка, нарушившие положения настоящей Частной политики, несут административную и иную ответственность в соответствии с законодательством Российской Федерации.

8.3. Работники Банка, разгласившие информацию, включающую ПДн, обрабатываемую в ИСПДн Банка, а также работники, по вине которых произошла утрата документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними нормативными документами Банка и условиями трудового соглашения (контракта).

8.4. При обнаружении нарушений порядка предоставления ПДн дальнейшее предоставление персональных данных пользователям информационной системы приостанавливается до выявления причин нарушений и устранения этих причин.

9. ПЕРЕСМОТР ПОЛИТИКИ

9.1. Развитие системы информационной безопасности и совершенствование методов и средств защиты является непрерывным процессом, в связи с чем возникает необходимость пересмотра положений Частной политики. Внесение изменений в Политику может носить как регламентный характер, так и быть вызванным изменениями в системе информационной безопасности или нормативных документах.

9.2. Пересмотр положений Частной политики безопасности производится в следующих случаях:

9.2.1. При изменении законодательства в области защиты ПД.

В случае внесения изменений в законодательства в области защиты ПДн необходимо провести пересмотр положений Частной политики для оценки её соответствия новым положениям.

9.2.2. При регламентном пересмотре Частной политики.

Регламентный пересмотр Частной политики производится раз в год и обусловлен необходимостью соответствия положений Частной политики текущему состоянию ИСПДн и используемых методов защиты ПДн.

9.2.3. При внесении изменений в регламентные документы Банка.

Частная политика разрабатывается на основе концептуальных документов по информационной безопасности. В случае изменения взглядов на проблему защиты ПДн или целей обеспечения безопасности ПДн изменения вносятся в концептуальные нормативные документы и, как следствие, требуется пересмотр положений Частной политики.

9.2.4. При внесении изменений в информационную систему персональных данных.

9.2.4.1. В случае внесения изменений в ИСПДн положения Частной политики должны быть дополнены и/или исправлены, чтобы отвечать текущему состоянию ИСПДн.

9.2.4.2. При внесении изменений в Частную политику проводятся мероприятия по обследованию и анализу изменений:

9.2.4.2.1. В ИСПДн в целом;

9.2.4.2.2. В СЗПДн;

9.2.4.2.3. В системе нормативных и регламентных документов.

9.2.4.2.4. При внесении изменений в перечень защищаемых объектов и ресурсов (при необходимости).

9.2.4.2.5. При формулировке и описании дополнительных (изменённых) требований к СЗПДн, мер и процедур защиты ПДн.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Настоящая Частная политика, а также все изменения и дополнения к ней утверждается Правлением Банка.

10.2. Настоящая Частная политика подлежит опубликованию на официальном сайте Банка в сети Интернет.

10.3. Сотрудника Банка, имеющие доступ к персональным данным, должны быть ознакомлены с настоящей Частной политикой под роспись.

10.4. В случае вступления отдельных пунктов настоящей Частной политики в противоречие с новыми законодательными актами, они утрачивают юридическую силу и до момента внесения изменений в Политику, Банк руководствуется действующим законодательством Российской Федерации и нормативными актами Банка России.

10.5. С момента вступления в силу настоящей Частной политики признаются утратившими силу:

- Политика АО КБ «Михайловский ПЖСБ» в отношении обработки персональных данных, утвержденная Правлением 15.09.2016 г., протокол № 171;
- Перечень персональных данных, обрабатываемых в ОАО КБ «Михайловский ПЖСБ», утвержденный Правлением 28.06.2011 г., протокол № 117.

Приложение № 1
к Частной политике
обеспечения безопасности персональных
данных в информационных системах
в АО КБ «Михайловский ПЖСБ»

Перечень персональных данных, обрабатываемых Банком

Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному, или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, в том числе:

1.Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (в том числе видеозаписи внутренних систем охранного видеонаблюдения и банковских терминальных устройств, фотографии работника Банка на личном листке по учету кадров, на удостоверении сотрудника Банка и в общедоступных источниках Банка (в т.ч. в электронном виде), ксерокопии с документов, удостоверяющих личность и имеющих фотографию владельца).

2. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

3. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

5. Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).

6. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).

7. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения).

8. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения).

9. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

10. Содержание и реквизиты трудового договора с работником Банка или гражданско-правового договора с гражданином.

11. Сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их пластиковых карт, данные по окладу, надбавкам, налогам и другие сведения).

12. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный

билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения).

13. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

14. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);

- недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения);

- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, пластиковых карт, вид, срок размещения, сумма, условия вклада и другие сведения);

- кредиты (займы), банковские счета (в том числе пластиковые карты), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, номера банковских карт, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения).

15. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

16. Сведения об идентификационном номере налогоплательщика.

17. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

18. Сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним.

19. Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников Банка.

20. Материалы по аттестации и оценке работников Банка.

21. Материалы по внутренним служебным расследованиям в отношении работников Банка.

22. Внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

23. Сведения о временной нетрудоспособности работников Банка.

24. Табельный номер работника Банка.

25. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

Приложение № 2
к Частной политике
обеспечения безопасности персональных
данных в информационных системах
в АО КБ «Михайловский ПЖСБ»

Места хранения персональных данных, обрабатываемых без использования средств автоматизации и подразделения, осуществляющие их обработку

Категория ПДн	Документ	Место хранения	Ответственное лицо	Подразделения, осуществляющие обработку
ПД лиц, обратившихся за получением кредита на условиях, объявленных Банком. ПД лиц, обратившихся в Банк с предложением предоставить обеспечение по кредитным договорам.	1) Подлинные экземпляры кредитных договоров, договоров по обеспечению кредита в период действия кредитного договора.	Сейфовая комната Банка/	Заведующий кассой	Отдел кредитования
	2) Кредитные досье - копии кредитных договоров, договоров залога, поручительства, вся информация о заемщике, и документы, послужившие основанием для предоставления кредита.	Специально отведенные металлические шкафы в помещении отдела кредитования	Начальник отдела кредитования	Отдел Кредитования
ПД лиц, заключивших с Банком договор банковского вклада. ПД лиц, заключивших с Банком договор банковского счета	1) Юридические дела клиентов - юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой.	Специально отведенные металлические шкафы, запирающиеся на ключ в помещении юридического отдела.	Ведущий юрисконсульт	Юридический отдел, Отдел финансового мониторинга
	2) Юридические дела клиентов - физических лиц.	Специально отведенные шкафы в помещении операционного управления.	Главный специалист операционного управления.	ОПЕРУ
	3) Договора по вкладам (депозитам) юридических лиц и	Специально отведенные шкафы в	Начальник операционного управления.	ОПЕРУ

	индивидуальных предпринимателей	помещении операционного управления.		
ПД лиц, осуществляющих перевод денежных средств без открытия счета	Заявления и другие документы по переводам без открытия счета.	Помещение кассового узла. Специально отведенные шкафы в помещении отдела бухгалтерского учета и отчетности	Заведующий кассой. Ведущий специалист ОБУиО.	ОПЕРУ
ПД лиц, осуществляющих перечисление денежных средств без открытия счета по системам денежных переводов («Вестерн Юнион», «Золотая Корона», «Лидер» и т.п.)	Заявления и другие документы по системным переводам без открытия счета.	Помещение кассового узла. Специально отведенные шкафы в помещении операционного управления (в части заявлений и отчетов по переводам) Специально отведенные шкафы в помещении отдела бухгалтерского учета и отчетности	Заведующий кассой. Главный специалист операционного управления. Ведущий специалист ОБУиО.	ОПЕРУ
ПД лиц, с которыми Банк заключил договор на поставку товара, оказание услуг, выполнение работ с целью обеспечения финансово-хозяйственной деятельности	Договора	Специально отведенные шкафы в помещении отдела бухгалтерского учета и отчетности.	Главный бухгалтер	ОБУиО
ПД лиц, обратившихся в Банк с запросом любого характера и предоставившие при этом свои персональные данные	Обращения	В зависимости от характера обращения	В зависимости от места хранения	В зависимости от характера обращения
ПД работников Банка, заключивших с Банком трудовой договор.	Персональные данные сотрудников Банка.	Специально отведенные шкафы, запирающиеся на ключ, и металлические	Делопроизводитель	Делопроизводитель

		сейфы секретариата		
ПД лиц, обратившихся в Банк с целью трудоустройства.	Персональные данные соискателей.	Специально отведенные шкафы, запирающиеся на ключ, и металлические сейфы секретариата	Делопроизводитель	Делопроизводитель