УТВЕРЖДАЮ:

Президент
ПАО «Банк «Екатеринбург»
_____/ С.Н. Викторов
« 05 » февраля 2016 г.

ПОЛИТИКА

в отношении обработки персональных данных

2016г.

Содержание

1. **Назначение** 3
2. **Определения** 3
3. **Перечень условных обозначений и сокращений** 6
4. **Построение защиты персональных данных** 7
5. **Состав подсистем СЗПДн** 8
6. **Подсистема организационных мер защиты** 8
7. **Подсистема физической защиты** 9
8. **Подсистема защиты каналов связи** 9
9. **Подсистема управления логическим доступом** 9
10. **Подсистема защиты от воздействия вредоносных программ** 9
11. **Подсистема межсетевого экранирования** 9
12. **Подсистема защиты информационного взаимодействия через сети связи общего пользования** 10
13. **Подсистема обнаружения вторжений** 10
14. **Подсистема инструментального анализа защищенности** 10
15. **Подсистема конфиденциального делопроизводства** 10
16. **Подсистема обеспечения целостности** 11
17. **Подсистема обеспечения непрерывности** 11
18. **Подсистема очистки памяти** 11
19. **Подсистема защиты от наличия недекларированных возможностей** 11
20. **Подсистема защиты от утечки по техническим каналам** 11
21. **Подсистема подтверждения соответствия требованиям по безопасности** 12
22. **Персонал** 12
23. **Ответственный за организацию обработки ПДн** 12
24. **Администратор информационной безопасности ИСПДн** 13
25. **Администратор ИСПДн** 13
26. **Пользователь ИСПДн** 13

1. Назначение

1.1. Целью настоящей Политики в отношении обработки персональных данных (далее Политика) является обеспечение соответствия обработки и защиты персональных данных, обрабатываемых в ПАО «Банк «Екатеринбург», требованиям Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных», нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных».

1.2. Политика разработана в соответствии с требованиями:

— Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных»;

— Постановления Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— Постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Политика содержит сведения о реализуемых требованиях к защите персональных данных.

1.4. Политика должна быть опубликована или иным образом должен быть обеспечен неограниченный доступ к ней.

2. Определения

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

2.2. Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

2.3. Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

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

2.5. 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.

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

2.7. Доступ к информации – возможность получения информации и ее использования.

2.8. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

2.10. Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.11. Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

2.12. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их раскрытие третьим лицам или их распространение без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.13. Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.14. Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

2.15. Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

2.17. Носитель персональных данных – материальный объект, в котором информация, содержащая персональные данные, находит свое отражение в виде символов, образов, сигналов, количественных характеристик физических величин. Выделяются следующие типы носителей персональных данных:

- бумажный носитель персональных данных – носитель на бумажной основе, содержащий персональные данные;
- машинный носитель персональных данных – электронный, магнитный, магнитооптический, оптический носитель, содержащий персональные данные (дискета, CD-диск, DVD-диск, жесткий диск, USB устройства, позволяющие хранить информацию, и т.д.).

2.18. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.19. 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.

2.20. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно 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.

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

2.22. Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

2.24. Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

2.25. Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

2.27. Технические средства – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (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).

2.28. Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

2.29. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.30. Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.31. 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.

2.32. Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

2.33. Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

2.35. Шифровальные (криптографические) средства – криптосредства:

- средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;
- средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
- средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
- ключевые документы (независимо от вида носителя ключевой информации).

3. Перечень условных обозначений и сокращений

ИСПДн — информационные системы персональных данных ПАО «Банк «Екатеринбург»

ПДн — персональные данные

СЗПДн — система защиты персональных данных, обрабатываемых в информационных системах персональных данных ПАО «Банк «Екатеринбург»

СЗИ — средство защиты информации

4. Построение защиты персональных данных

4.1. В локальном акте ПАО «Банк «Екатеринбург» – «Положении об обработке и защите персональных данных», определяются:

— порядок взаимодействия с Роскомнадзором;

— перечень оснований для обработки персональных данных (далее ПДн);

— порядок получения ПДн;

— порядок поручения обработки ПДн;

— порядок предоставления, распространения ПДн;

— порядок трансграничной передачи ПДн;

— порядок прекращения обработки ПДн, уничтожения ПДн;

— порядок рассмотрения запросов субъектов ПДн на предоставление информации;

— порядок рассмотрения запросов на уточнение ПДн;

— порядок рассмотрения запросов на устранение нарушений законодательства, допущенных при обработке ПДн, блокирование или уничтожение ПДн;

— порядок принятия решений на основании исключительно автоматизированной обработки ПДн;

— порядок защиты ПДн.

4.2. Защита ПДн, обрабатываемых без использования средств автоматизации, строится на основании требований Постановления Правительства РФ от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.3. Система защиты ПДн, обрабатываемых в информационных системах персональных данных ПАО «Банк «Екатеринбург» (далее СЗПДн), строится на основании требований нормативных правовых актов, принятых в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», а также:

— Перечня ПДн, обрабатываемых в ИСПДн;

— Актов определения уровня защищенности ПДн при их обработке в далее ИСПДн;

— Модели угроз безопасности ПДн при их обработке в ИСПДн.

4.4. Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется в соответствии с порядком, установленным Постановлением

Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5. Состав подсистем СЗПДн

5.1. СЗПДн включает в себя следующие подсистемы:

— организационных мер защиты;

— физической защиты;

— защиты каналов связи;

— управления логическим доступом;

— защиты от воздействия вредоносных программ;

— межсетевого экранирования;

— защиты информационного взаимодействия через сети связи общего пользования;

— обнаружения вторжений;

— инструментального анализа защищенности;

— конфиденциального делопроизводства;

— обеспечения целостности;

— обеспечения непрерывности;

— очистки памяти;

— защиты от наличия недекларированных возможностей;

— защиты от утечки по техническим каналам;

— подтверждения соответствия требованиям по безопасности.

5.2. Состав требований, реализуемых каждой из подсистем СЗПДн, зависит от:.

— Уровня защищенности ПДн при их обработке в ИСПДн;

— Структурно-функциональных характеристик и особенностей функционирования ИСПДн;

— Состава актуальных угроз безопасности ПДн при их обработке в ИСПДн.

6. Подсистема организационных мер защиты

6.1. Состоит из лиц, выполняющих функции по:

— администрированию программных, программно-аппаратных, аппаратных средств ИСПДн;

— администрированию средств защиты информации ИСПДн (далее СЗИ);

— защите ПДн.

6.2. Также в данную подсистему входят локальные акты ПАО «Банк «Екатеринбург» по вопросам обработки и защиты ПДн.

7. Подсистема физической защиты

7.1. Данная подсистема предназначена для обеспечения физической охраны технических средств ИСПДн, эксплуатационной и технической документации к СЗИ, ключевых документов, носителей ПДн.

7.2. Данная подсистема реализуется путем применения инженерно-технических средств охраны, надежных хранилищ, мер мо обеспечению необходимого уровня физической укрепленности помещений.

8. Подсистема защиты каналов связи

8.1. Данная подсистема предназначена для исключения несанкционированного доступа к защищаемой информации ИСПДн (ПДн, служебная информация СЗИ) при ее передаче по каналам связи, выходящим за пределы контролируемой зоны ПАО «Банк «Екатеринбург».

8.2. Данная подсистема реализуется путем применения криптосредств, защищенных коробов и защищенных телекоммуникационных шкафов совместно со средствами контроля за их вскрытием.

9. Подсистема управления логическим доступом

9.1. Данная подсистема предназначена для идентификации, проверки подлинности пользователей и администраторов ИСПДн, разграничения и контроля доступа в ИСПДн, регистрации действий пользователей и администраторов ИСПДн.

9.2. Данная подсистема реализуется путем применения СЗИ от несанкционированного доступа, встроенных механизмов защиты применяемых программных, программно-аппаратных, аппаратных средств ИСПДн (операционных систем, систем управления базами данных, приложений).

10. Подсистема защиты от воздействия вредоносных программ

10.1. Данная подсистема предназначена для защиты от воздействия на ИСПДн вредоносных программ.

10.2. Данная подсистема реализуется путем применения средств антивирусной защиты, периодического обновления антивирусных баз на рабочих местах и серверах ИСПДн, подключенных к сетям связи общего пользования, а также ИСПДн, при функционировании которых предусмотрено использование съемных носителей информации.

11. Подсистема межсетевого экранирования

11.1. Данная подсистема предназначена для фильтрации трафика, передаваемого в/из ИСПДн.

11.2. Данная подсистема реализуется путем применения межсетевых экранов при подключении ИСПДн к сетям связи общего пользования, локальным вычислительным сетям ПАО «Банк «Екатеринбург».

12. Подсистема защиты информационного взаимодействия через сети связи общего пользования

12.1. Данная подсистема предназначена для защиты ПДн при подключении ПДн к сетям связи общего пользования в целях:

- получения общедоступной информации;
- удаленного доступа к ИСПДн через сети связи общего пользования,
- межсетевого взаимодействия отдельных ИСПДн ПАО «Банк «Екатеринбург» через сети связи общего пользования;
- межсетевого взаимодействии отдельных ИСПДн ПАО «Банк «Екатеринбург» с ИСПДн других операторов через сети связи общего пользования.

12.2. Данная подсистема реализуется путем:

- применения электронных замков, носителей информации для надежной идентификации и проверки подлинности пользователей;
- применения средств централизованного управления СЗПДн;
- анализа принимаемой по сетям связи общего пользования информации (в том числе на наличие компьютерных вирусов);
- проверки подлинности взаимодействующих ИСПДн;
- проверки подлинности пользователей;
- проверки целостности данных, передаваемых по сетям связи общего пользования;
- предотвращения возможности отрицания пользователем факта отправки ПДн другому пользователю;
- предотвращения возможности отрицания пользователем факта получения ПДн от другого пользователя.

13. Подсистема обнаружения вторжений

13.1. Данная подсистема предназначена для защиты от воздействия на ИСПДн сетевых атак.

13.2. Данная подсистема реализуется путем применения средств обнаружения вторжений при подключении ИСПДн к сетям связи общего пользования.

14. Подсистема инструментального анализа защищенности

14.1. Данная подсистема предназначена для периодического тестирования функций СЗПДн в целях выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на ИСПДн.

14.2. Данная подсистема реализуется путем применения средств анализа защищенности как периодически, так и при изменении программной среды или состава пользователей ИСПДн.

15. Подсистема конфиденциального делопроизводства

15.1. Данная подсистема предназначена для исключения несанкционированного доступа к носителям ПДн.

15.2. Данная подсистема реализуется путем учета носителей ПДн, исключения хищения, подмены или уничтожения съемных носителей ПДн.

16. Подсистема обеспечения целостности

16.1. Данная подсистема предназначена для обеспечения целостности программной среды ИСПДн, программных компонент СЗИ.

16.2. Данная подсистема реализуется путем:

— обеспечения отсутствия средств модификации объектного кода программ в процессе обработки и (или) хранения ПДн;

— проверки целостности программных компонентов СЗПДн;

— оборудования аппаратных средств, с которыми осуществляется штатное функционирование программных криптосредств, а также аппаратных и аппаратно-программных криптосредств средствами контроля за их вскрытием.

17. Подсистема обеспечения непрерывности

17.1. Данная подсистема предназначена для обеспечения возможности восстановления ПДн, работоспособности СЗПДн.

17.2. Данная подсистема реализуется путем применения средств дублирования массивов ПДн, ведения копий программных компонентов СЗПДн.

18. Подсистема очистки памяти

18.1. Данная подсистема предназначена для исключения несанкционированного доступа к ПДн, находящимся в оперативной памяти ИСПДн, на внешних накопителях.

18.2. Данная подсистема реализуется путем применения в ИСПДн средств очистки (обнуления, обезличивания) освобождаемых областей оперативной памяти ИСПДн, внешних накопителей.

19. Подсистема защиты от наличия недекларированных возможностей

19.1. Данная подсистема предназначена для исключения наличия недекларированных возможностей в программных компонентах СЗПДн.

19.2. Данная подсистема реализуется путем применения в ИСПДн программного обеспечения СЗИ, соответствующего 4 уровню контроля отсутствия недекларированных возможностей.

20. Подсистема защиты от утечки по техническим каналам

20.1. Данная подсистема предназначена для исключения утечки ПДн по техническим каналам.

20.2. Данная подсистема реализуется путем:

— размещения устройств вывода информации (мониторов) таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

21. Подсистема подтверждения соответствия требованиям по безопасности

21.1. Данная подсистема предназначена для обеспечения соответствия требованиям по безопасности ПДн.

21.2. Данная подсистема реализуется путем:

— применения СЗИ, прошедших в установленном порядке процедуру оценки соответствия;

— оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.

22. Персонал

22.1. Выделяются следующие группы лиц, участвующих в обработке и защите ПДн:

— ответственный за организацию обработки ПДн;

— администратор информационной безопасности ИСПДн;

— администратор ИСПДн;

— пользователи ИСПДн.

23. Ответственный за организацию обработки ПДн

23.1. Ответственный за организацию обработки ПДн – сотрудник ПАО «Банк «Екатеринбург» или специализированной организации, имеющей необходимые лицензии ФСТЭК России и ФСБ России, ответственный за:

— подготовку локальных актов ПАО «Банк «Екатеринбург» по вопросам обработки и защиты ПДн;

— осуществление внутреннего контроля за соблюдением ПАО «Банк «Екатеринбург» и его работниками законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПДн;

— проведение инструктажа работников в целях доведения до данных работников положений законодательства Российской Федерации, локальных актов по вопросам обработки и защиты ПДн;

— организацию приема и обработки запросов (обращений, заявлений) субъектов ПДн или их представителей.

23.2. Ответственным за организацию обработки ПДн назначается лицо, имеющее высшее профессиональное образование и (или) переподготовку (повышение квалификации) в области информационной безопасности, а также производственный стаж в области информационной безопасности не менее одного года.

23.3. Ответственный за организацию обработки ПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией ответственного за организацию

обработки ПДн» или соответствующим договором со специализированной организацией.

24. Администратор информационной безопасности ИСПДн

24.1. Администратор информационной безопасности ИСПДн – сотрудник ПАО «Банк «Екатеринбург» или специализированной организации, имеющей необходимые лицензии ФСТЭК России и ФСБ России, ответственный за установку, настройку и сопровождение СЗИ.

24.2. Администратором информационной безопасности ИСПДн назначается лицо, имеющее высшее профессиональное образование и (или) переподготовку (повышение квалификации) в области информационной безопасности, а также производственный стаж в области информационной безопасности не менее одного года.

24.3. Администратор информационной безопасности ИСПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией администратора информационной безопасности ИСПДн» или соответствующим договором со специализированной организацией.

25. Администратор ИСПДн

25.1. Администратор ИСПДн – сотрудник ПАО «Банк «Екатеринбург» или работник специализированной организации, ответственное за установку, настройку и сопровождение программных, программно-аппаратных, аппаратных средств ИСПДн.

25.2. Администратором ИСПДн назначается лицо, имеющее производственный стаж в области создания, обслуживания локальных вычислительных сетей не менее одного года.

25.3. Администратор ИСПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией администратора ИСПДн» или соответствующим договором со специализированной организацией или соответствующим договором с физическим лицом.

26. Пользователь ИСПДн

26.1. Пользователь ИСПДн – сотрудник ПАО «Банк «Екатеринбург», осуществляющее обработку ПДн в ИСПДн.

26.2. Пользователь ИСПДн несет ответственность за некачественное, неполное, несвоевременное исполнение или неисполнение своих обязанностей, предусмотренных «Инструкцией пользователя ИСПДн» или соответствующим договором с контрагентом или соответствующим договором с физическим лицом.

27. Заключительные положения

Политику в отношении обработки персональных данных от 17.12.2013 г. считать утратившей силу с момента подписания настоящей Политик Президентом ПАО «Банк «Екатеринбург».