«Газпромбанк» (Открытое акционерное общество)
(ГПБ (ОАО)

УТВЕРЖДАЮ
Заместитель Председателя
Правления ГПБ (ОАО)
_____ Ф.М. Канцеров
« 27» июля 2011 г.

Рег. № И/42

ЧАСТНАЯ ПОЛИТИКА
защиты персональных данных
в «Газпромбанк»
(Открытое акционерное общество)

(С изменениями от 11.04.2012 № И/18 и от 16.01.2014 № И/1)

МОСКВА

2011

Содержание

1. Общие положения

1.1. Настоящая Частная политика определяет политику обработки персональных данных ГПБ (ОАО), а также детализирует положения «Политики информационной безопасности «Газпромбанк» (Открытое акционерное общество)», утвержденной решением Правления ГПБ (ОАО) от 24.09.2008 (протокол № 35) (с изменениями от 30.09.2009 (протокол № 41), от 10.11.2010 (протокол № 49), от 22.03.2012 (протокол № 11), применительно к вопросам обеспечения безопасности персональных данных. Настоящая Частная политика разработана с учетом положений внешних нормативных документов, регламентирующих порядок обеспечения безопасности персональных данных, указанных в приложении к настоящей Частной политике.

1.2. Целью настоящей Частной политики являются определение особенностей обработки и обеспечения безопасности персональных данных, а также минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности персональных данных.

1.3. Организация обработки и обеспечения безопасности персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.4. Настоящая Частная политика распространяется на все технологические процессы «Газпромбанк» (Открытое акционерное общество) (далее – Банк), связанные с обработкой персональных данных субъектов, и обязательна для применения всеми работниками Банка.

1.5. Самостоятельным структурным подразделением Банка, осуществляющим разработку и реализацию мероприятий по обеспечению безопасности персональных данных субъектов, является Департамент защиты информации (далее - Ответственное подразделение). При необходимости к работам по защите персональных данных могут привлекаться другие самостоятельные структурные подразделения Банка.

1.6. Работники Банка должны быть ознакомлены со внутренними нормативными документами, локальными актами Банка, устанавливающими правила обработки и обеспечения безопасности персональных данных, в соответствии с порядком, изложенным в этих внутренних нормативных документах. Контроль за ознакомлением осуществляет Ответственное подразделение.

1.7. Требования настоящей Частной политики при необходимости могут детализироваться иными внутренними нормативными документами Банка.

1.8. В филиалах Банка могут быть в установленном порядке (включая согласование с Ответственным подразделением головного офиса) разработаны внутренние нормативные документы, уточняющие порядок применения настоящей Частной политики с учетом специфики работы филиала.

1.9. В соответствии с требованиями ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» настоящая Частная политика подлежит опубликованию в информационно-телекоммуникационной сети «Интернет».

2. Список терминов и определений

2.1. **Автоматизированная банковская система -** автоматизированная система, реализующая технологию выполнения функций Банка.

2.2. **Автоматизированная система**[1] **–** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную поддержку выполнения установленных функций.

2.3. **Акт определения требуемого уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)** – внутрибанковский документ, в котором фиксируется результат определения требуемого уровня защищенности персональных данных при их обработке в ИСПДн Банка.

2.4. **Банковский информационный технологический процесс** – часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования Банка и не являющихся платежной информацией.

2.5. **Банковский платежный технологический процесс** – часть банковского технологического процесса, реализующая банковские операции с информационными активами Банка, связанные с перемещением денежных средств с одного счета на другой и (или) контролем этих операций.

2.6. **Банковский технологический процесс** – технологический процесс, осуществляющий операции по изменению и (или) определению состояния активов Банка, используемых при его функционировании или необходимых для реализации банковских услуг.

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

2.8. **Владелец ИСПДн** – владелец информационной системы персональных данных, выполняющий функции в соответствии с «Порядком предоставления и контроля доступа к ИТ-ресурсам ГПБ (ОАО)», утвержденным приказом от 07.05.2008 № 71.

2.9. **Информационный актив –** информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Банка, находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

2.10. **Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[2]. К информационным системам персональных данных относятся автоматизированные банковские системы, целью создания и использования которых является обработка персональных данных. Автоматизированные банковские системы, реализующие банковские платежные технологические процессы, не относятся к информационным системам персональных данных[3].

2.11. **Информационно-технологический блок (ИТ-блок)** – совокупность самостоятельных структурных подразделений Банка, ответственных за развитие, эксплуатацию и сопровождение автоматизированных систем.

2.13. **Комплекс БР ИББС** – взаимоувязанная совокупность документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации[4]».

---

[1] Согласно стандарту Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2010), утвержденному распоряжением Банка России от 21.06.2010 № Р-705.

[2] Согласно п. 10 ст. 3 главы 1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

[3] Согласно п. 7.10.9 стандарта Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организации банковской системы Российской Федерации», утвержденного распоряжением Банка России от 21.06.2010 № Р-705.

[4] Перечень документов, входящих в состав Комплекса БР ИББС, приведен в п. 4-7 приложения.

2.14. **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.15. **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.

2.16. **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.

2.16[1]. **Определение требуемого уровня защищённости персональных данных при их обработке в ИСПДн** - определение одного из четырёх уровней защищённости персональных данных, в соответствии с критериями, установленными постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», которые требуется обеспечить при обработке персональных данных в ИСПДн Банка.

2.17. **Ответственное подразделение** – Департамент защиты информации, руководитель которого[5] является ответственным за организацию обработки персональных данных в ГПБ (ОАО) и в функции ответственного входит:

- организация обработки персональных данных в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», требованиями, установленными иным законодательством Российской Федерации, документами Банка России и локальными актами Банка о персональных данных;
- осуществление внутреннего контроля за соблюдением Банком и его работниками законодательства Российской Федерации и внутренних нормативных документов Банка о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников Банка в месячный срок положения законодательства Российской Федерации, требований Банка России, локальных актов, внутренних нормативных документов Банка по вопросам обработки персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов.

2.18. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[6].

2.18[1]. **Пользователь сайта** – лицо, предоставляющее Банку для обработки свои персональные данные с использованием средств web-сайта Банка.

2.19. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

---

[5] Приказ от 17.09.2013 № 151 «О назначении ответственных за организацию обработки персональных данных в ГПБ (ОАО)».

[6] Согласно п. 1 ст.3 главы 1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2.20. **Система обеспечения безопасности персональных данных** – система правовых, организационных, технических и иных мер по обеспечению доступности, целостности и конфиденциальности персональных данных.

2.21. **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.22. **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.

3. Перечень сокращений

АБС	-	автоматизированная банковская система;
Банк	-	ГПБ (ОАО);
БР ИББС	-	Банк России – информационная безопасность банковской системы;
ВДЛ	-	высшее должностное лицо Банка;
ВНД	-	внутренний нормативный документ Банка;
ИСПДн	-	информационная система персональных данных;
ИБ	-	информационная безопасность;
ОРД	-	организационно – распорядительный документ;
ПДн	-	персональные данные;
ССП	-	самостоятельное структурное подразделение Банка;
ЮД	-	Юридический департамент.

4. Общие положения по организации обработки и обеспечению безопасности ПДн

4.1. Основными принципами обработки ПДн в Банке являются:

- законность целей и способов обработки ПДн и добросовестность Банка, как оператора, что достигается путем установления требований к обработке ПДн и неукоснительного их соблюдения;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Банка;
- соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн;

- хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и уничтожение ПДн по достижении целей обработки или в случае утраты необходимости в их достижении.

4.2. Банк, как оператор, осуществляет обработку ПДн физических лиц в рамках требований законодательства Российской Федерации в целях:

- осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: от 02.12.1990 № 395-1 «О банках и банковской деятельности», от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг», от 25.02.1999 № 40-ФЗ «О несостоятельности (банкротстве) кредитных организаций», от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации», от 30.12.2004 № 218-ФЗ «О кредитных историях», от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», нормативными актами Банка России, а также Уставом Банка (в действующей редакции) и ВНД;

- заключения договоров, сторонами которых являются субъекты персональных данных, при этом персональные данные субъектов не распространяются, а также не предоставляются третьим лицам без согласия субъектов персональных данных и используются Банком исключительно для исполнения указанных договоров и заключения договоров с субъектами персональных данных;

- организации учета работников Банка (кандидатов на работу) для обеспечения соблюдения требований законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, добровольном страховании всех видов, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Законом № 152-ФЗ, а также Уставом Банка (в действующей редакции) и ВНД;

- обеспечения пропуска субъектов ПДн на территорию Банка или в иных аналогичных целях;

- выполнения трудового законодательства Российской Федерации.

4.3. Банк обрабатывает ПДн, осуществляя свою деятельность в соответствии с требованиями Гражданского кодекса Российской Федерации, Трудового кодекса Российской Федерации, Налогового кодекса Российской Федерации, федеральных законов, положений и инструкций Банка России и ФСФР России, Устава Банка (в действующей редакции), а также Генеральной лицензии Банка России и других лицензий на осуществляемые виды деятельности.

4.4. В Банке используется смешанная обработка ПДн. Под смешанной обработкой понимается автоматизированная и неавтоматизированная обработка ПДн (согласно приказу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 16 июля 2010 г. № 482 «Об утверждении образца формы уведомления об обработке персональных данных»). При этом полученная в ходе обработки ПДн информация может:

- передаваться получателю по внутренней сети Банка;
- передаваться получателю с использованием сети общего пользования Интернет;

- не передаваться.

4.5. В соответствии со степенью тяжести последствий потери свойств безопасности ПДн для субъектов ПДн Банк выделяет следующие категории ПДн:

- ПДн, отнесенные в соответствии с Законом № 152-ФЗ к специальным категориям ПДн;
- ПДн, отнесенные в соответствии с Законом № 152-ФЗ к биометрическим ПДн;
- ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим ПДн, к общедоступным ПДн;
- ПДн, отнесенные в соответствии с Законом № 152-ФЗ к общедоступным ПДн.

4.7. В случае достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации, Банк прекращает обработку и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение ПДн, которые обрабатывались третьими лицами на основании договора с Банком, в порядке, установленном законодательством Российской Федерации. Уничтожение ПДн и материальных носителей ПДн в Банке осуществляется в согласованном с Ответственным подразделением порядке и документируется. Детально соответствующий порядок определяется в иных ВНД, регламентирующих порядок уничтожения информации, в отношении которой установлено требование обеспечения конфиденциальности, и материальных носителей такой информации.

4.8. Ответственное подразделение определяет необходимость направления в уполномоченный орган по защите прав субъектов ПДн уведомления об обработке (о намерении осуществлять обработку) ПДн в соответствии с требованиями законодательства Российской Федерации. В случае установления необходимости направления такого уведомления, ответственным за его составление, направление, уточнение и изменение является Ответственное подразделение. ССП информируют Ответственное подразделение об изменении включенной в такое уведомление информации по направлениям своей деятельности.

5. Основные требования к процедурам обработки ПДн

5.1. Обработка ПДн в Банке должна осуществляться с согласия субъекта ПДн кроме случаев, установленных законодательством Российской Федерации, когда такое согласие не требуется.

5.2. В Банке запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн, или иным образом затрагивающих его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации.

5.3. Банк осуществляет трансграничную передачу ПДн в случаях, предусмотренных законодательством Российской Федерации, а также на основе соответствующих соглашений с международными и иностранными организациями, закрепляющих адекватную защиту прав субъектов ПДн, в том числе в части обеспечения конфиденциальности ПДн как составной части конфиденциальной информации, обмен которой производится.

5.4. Предоставление ПДн Банком третьему лицу, кроме случаев, предусмотренных законодательством Российской Федерации, должно осуществляться с согласия субъекта ПДн. В случае если Банк на основании договора поручает обработку ПДн третьему лицу, существенным условием договора (или заключенного с таким лицом соглашения о конфиденциальности) должна являться обязанность указанного лица по обеспечению конфиденциальности ПДн и безопасности ПДн при их обработке (в том числе, как составной части конфиденциальной информации, обмен которой производится), а также выполнение им требований, предъявляемых к защите ПДн в соответствии со статьей 19 Закона № 152-ФЗ и несение ответственности перед Банком за обработку таких ПДн.

5.5. Руководители ССП, обеспечивающих достижение целей обработки ПДн, указанных в п. 4.2, готовят проекты утверждаемых в установленном порядке ВНД и/или ОРД, устанавливающих для каждой такой цели:

- объем и содержание ПДн;
- сроки обработки ПДн, в том числе сроки хранения;
- правовые основания для обработки ПДн, в том числе необходимость, форму и порядок получения согласия субъектов ПДн;
- источники получения ПДн, виды и способы обработки ПДн, состав получателей (пользователей) ПДн.

5.6. В случаях, установленных законодательством Российской Федерации, обработка ПДн в Банке осуществляется с согласия субъекта ПДн в письменной форме, оформляемого в соответствии с требованиями статьи 9 Закона № 152-ФЗ.

5.7. Рекомендации к порядку получения согласия субъекта ПДн и требования к виду и составу такого согласия устанавливаются в иных ВНД.

5.8. В Банке ведется учет работников, осуществляющих обработку ПДн, в том числе с использованием ИСПДн. Учет ведет Ответственное подразделение совместно с Владельцами ИСПДн и ИТ-блоком в виде электронного перечня и/или списка на основании ОРД и согласованных и исполненных в установленном порядке заявок на доступ в ИСПДн. Учет ведется на основе списков доступа работников и/или установленных ролей в соответствии с занимаемой должностью.

5.9. Порядок допуска и доступа к работе в ИСПДн устанавливается согласно «Положению о режиме конфиденциальности информации в ГПБ (ОАО)», утвержденному приказом от 27.05.2011 № 47. Доступ к ПДн и обработку таких данных работники Банка должны осуществлять только для выполнения должностных обязанностей.

5.10. Работники Банка, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими ПДн и категориях обрабатываемых ПДн при предоставлении доступа к ИСПДн, а также должны быть ознакомлены под личную подпись со всей содержащейся в должностных инструкциях и соответствующих ВНД совокупностью требований Банка по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

5.11. Во избежание несанкционированного доступа к ПДн рекомендуется:

- исключать фиксацию на одном материальном носителе ПДн и иной информации (в т.ч. других ПДн), если материальный носитель не позволяет осуществлять обработку ПДн отдельно от другой зафиксированной на том же носителе информации (ПДн);
- для каждой категории ПДн использовать отдельный материальный носитель.

5.12. При обработке ПДн на бумажных носителях следует руководствоваться «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

5.13. Обработка ПДн, получаемых Банком через web-сайт:

5.13.1. Обработка ПДн Пользователей сайта, осуществляется в целях предварительного рассмотрения обращений на предоставление различных видов банковских услуг, сбора резюме для подбора работников на вакантные должности, а также уточнения обстоятельств, указанных в обращениях по поводу услуг, предоставляемых Банком и информирования Пользователей сайта о результатах их рассмотрения.

5.13.2. Согласие Пользователей сайта на обработку их ПДн при рассмотрении обращений на предоставление различных видов банковских услуг, сбора резюме для подбора работников на вакантные должности осуществляется в виде отметки в соответствующем поле

во время заполнения web-форм, содержащих текст согласия. С целью установления достоверности предоставленных в web-формах данных Пользователями сайта Банк может проводить дополнительные проверочные мероприятия, по установлению факта направления ими ПДн. В случае несогласия Пользователи сайта обязаны прекратить ввод своих персональных данных.

6. Основные мероприятия по обеспечению безопасности ПДн

6.1. Объектами защиты являются ПДн, банковские платежные и информационные технологические процессы и АБС, обрабатывающие ПДн.

6.2. Безопасность ПДн достигается путем реализации комплекса мероприятий, позволяющих минимизировать риск нарушения информационной безопасности Банка.

6.2[1]. Безопасность персональных данных при их обработке в ИСПДн Банка обеспечивается с помощью системы защиты персональных данных.

Система защиты персональных данных включает организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в ИСПДн.

6.3. При обработке ПДн Банк обеспечивает их безопасность и принимает необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, путем установления в отношении таких данных режима конфиденциальности и контроля за его соблюдением, а также путем внедрения дополнительных мер защиты, реализующих требования законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов, стандартов и лучших международных практик.

6.4. При обеспечении защиты ПДн Банк руководствуется требованиями законодательства Российской Федерации и Комплекса БР ИББС. В качестве базовой модели угроз безопасности ПДн Банка принята «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» из состава Комплекса БР ИББС.

6.5. Все разрабатываемые в Банке и касающиеся обработки и/или защиты ПДн проекты документов многократного применения (в том числе форм анкет и согласий на обработку ПДн), а также проекты ВНД и ОРД должны быть согласованы с Ответственным подразделением и ЮД. Также обязательному согласованию с Ответственным подразделением подлежат мероприятия по сбору и защите ПДн.

6.6. В Банке в установленном порядке создается комиссия по определению требуемого уровня защищённости ПДн при их обработке в ИСПДн. В функции комиссии входит определение требуемого уровня защищённости ПДн при их обработке в ИСПДн, а также утверждение актов определения требуемого уровня защищённости ПДн при их обработке в ИСПДн. При отсутствии такой комиссии указанные функции возлагаются на Ответственное подразделение. Ответственное подразделение также ведет перечень обрабатывающих ПДн АБС на основе обследования АБС Банка и перечень ИСПДн на основе утвержденных актов определения требуемого уровня защищённости ПДн при их обработке в ИСПДн Банка.

6.7. В Банке устанавливается следующий подход к отнесению АБС к ИСПДн:

- вопрос об отнесении АБС к ИСПДн рассматривается комиссией, назначаемой в соответствии с п. 6.6 настоящей Частной политики по представлению Ответственного подразделения;

- решение об отнесении АБС к ИСПДн принимается с учетом целей создания и использования АБС, вида реализуемого АБС технологического процесса и обрабатываемых в АБС ПДн;
- к ИСПДн должны быть отнесены как минимум АБС, целью создания и использования которых является обработка ПДн;
- решение об отнесении АБС к ИСПДн отражается в акте определения требуемого уровня защищённости ПДн при их обработке в ИСПДн;
- решение о неотнесении АБС к ИСПДн отражается в отдельном акте.

6.8. Банковские информационные технологические процессы, в рамках которых ПДн обрабатываются в ИСПДн, документируются Владельцами ИСПДн в разрабатываемых в установленном порядке ВНД, регламентирующих работу с указанными ИСПДн.

6.9. Для каждой ИСПДн ее Владелец определяет и фиксирует в Акте определения требуемого уровня защищенности ПДн при их обработке в ИСПДн:

- цели обработки ПДн;
- объем и содержание обрабатываемых ПДн, соответствующие целям обработки;
- перечень действий с ПДн и способы их обработки для достижения указанных целей.

6.10. Выбор требований по обеспечению безопасности ПДн осуществляется в соответствии с требованиями законодательства Российской Федерации в области ПДн и документов Банка России в зависимости от установленного уровня защищённости ПДн, зафиксированного в соответствующем Акте определения требуемого уровня защищенности ПДн при их обработке в ИСПДн и в соответствии с базовой моделью угроз безопасности ПДн Банка.

6.11. Ответственными за обеспечение безопасности ПДн при их обработке в ИСПДн являются руководители эксплуатирующих (Владельцы ИСПДн) и обслуживающих ИСПДн (ИТ-блок и Ответственное подразделение) подразделений Банка. Распределение функций и зон ответственности между указанными подразделениями устанавливается в регламентирующих эксплуатацию ИСПДн ВНД и ОРД.

6.12. В документации на внедряемые ИСПДн Банка должны быть отражены вопросы обеспечения безопасности обрабатываемых ПДн. Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн должны осуществляться по согласованию и под контролем Ответственного подразделения.

6.13. Ответственное подразделение должно:

6.13.1. Разработать систему обеспечения безопасности ПДн, обеспечивающую нейтрализацию предполагаемых угроз. При этом ввод в эксплуатацию и использование средств и систем защиты информации должны осуществляться в соответствии с документацией на них.

6.13.2. Осуществлять проверку готовности средств защиты информации, а также контроль их использования.

6.13.3. Проводить анализ происходящих нарушений порядка обработки и защиты ПДн, разработку и принятие мер по предотвращению возможных опасных последствий.

6.13.4. Совместно с Департаментом по работе с персоналом проводить обучение лиц, использующих средства защиты информации, применяемые в автоматизированных системах, правилам работы с ними.

6.14. Требования по обеспечению безопасности ПДн средствами антивирусной защиты и порядок проведения контроля реализации этих требований аналогичны общим требованиям по обеспечению антивирусной защиты конфиденциальной информации Банка, установленным в соответствующих ВНД.

6.15. В Банке вводятся ограничения на доступ в помещения, в которых проводится обработка ПДн, и устанавливаются требования к учету, хранению и уничтожению

материальных носителей ПДн, аналогичные общим ограничениям и требованиям по обеспечению информационной безопасности конфиденциальной информации Банка, установленным в соответствующих ВНД (Положение о режиме конфиденциальности информации в ГПБ (ОАО) (утверждено приказом от 27.05.2011 № 47) и Инструкции по работе с документами, содержащими конфиденциальную информацию, в ГПБ (ОАО) (утверждена приказом от 12.04.2013 № 53).

6.16. Обеспечение конфиденциальности ПДн не требуется в случае обезличивания ПДн и в отношении общедоступных ПДн.

6.17. Координацию работ по созданию системы обеспечения безопасности персональных данных и взаимодействие с регуляторами[5] по вопросам безопасности ПДн в Банке осуществляет Ответственное подразделение. Руководитель Ответственного подразделения является ответственным за организацию обработки персональных данных.

7. Основные мероприятия по обеспечению прав субъектов ПДн при обработке их ПДн

7.1. Субъект ПДн, обрабатываемых Банком как оператором, имеет право:

- на получение сведений о Банке как об операторе, о месте нахождения Банка, о наличии у Банка ПДн, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими ПДн;
- требовать от Банка уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- принимать предусмотренные законодательством Российской Федерации меры по защите своих прав.

7.2. Банк в обязательном порядке рассматривает все обращения субъектов ПДн, в том числе если субъект ПДн считает, что Банк осуществляет обработку его ПДн с нарушением требований законодательства Российской Федерации или иным образом нарушает его права и свободы.

7.3. Порядок обработки обращений и запросов субъектов ПДн (или их законных представителей) по вопросам обработки их ПДн и действий в случае запросов уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн, устанавливается в ВНД, разрабатываемых Ответственным подразделением в соответствии с настоящей Частной политикой.

7.4. Отказ субъекта предоставить свои ПДн Банку для обработки в определенных целях влечет невозможность достижения этих целей.

7.5. Предоставление ПДн не должно нарушать конституционные права и свободы других лиц, в т.ч. работников Банка, и в предоставляемых данных не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

7.6. В случае отзыва субъектом ПДн согласия на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации, Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если ПДн обрабатываются третьими лицами по договору с Банком). В случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если ПДн обрабатываются

[5] Банк России, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий без ознакомления с ПДн субъектов.

третьими лицами по договору с Банком) в порядке, установленном законодательством Российской Федерации о защите персональных данных.

8. Обязанности работников, допущенных к обработке ПДн

8.1. Работники, допущенные к обработке ПДн, обязаны:

- знать и неукоснительно выполнять требования настоящей Частной политики;
- обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;
- не разглашать ПДн, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия других лиц, которые могут привести к разглашению (уничтожению, искажению) ПДн;
- выявлять факты разглашения (уничтожения, искажения) ПДн и информировать об этом Ответственное подразделение.

8.2. Обязанности работников, допущенных к обработке ПДн, регламентируются ВНД, устанавливающими правила обращения с конфиденциальной информацией в Банке.

9. Контроль за соблюдением требований настоящей Частной политики

9.1.Контроль за обеспечением безопасности ПДн и соблюдением требований настоящей Частной политики осуществляет Ответственное подразделение.

9.2.Контроль осуществляется путем проведения мониторинга ИБ и менеджмента инцидентов ИБ, по результатам оценки состояния ИБ, а также в рамках иных контрольных мероприятий.

10. Ответственность за несоблюдение положений настоящей Частной политики

10.1.Ответственность работников Банка за несоблюдение требований настоящей Частной политики, повлекшее за собой разглашение, утрату или нарушение целостности ПДн, определяется законодательством Российской Федерации, ВНД, а также трудовыми договорами и должностными инструкциями работников Банка.

11. Заключительные положения

11.1.ВДЛ/руководители ССП осуществляют ознакомление штатных работников подчиненных подразделений с настоящей Частной политикой под личную подпись и обеспечивают хранение подписанных листов ознакомления, их сканирование и направление отсканированных копий в Ответственное подразделение. Ознакомление вновь принимаемых штатных работников с настоящей Частной политикой осуществляет Департамент по работе с персоналом.

11.2.В филиалах и представительствах Банка функции подразделений головного офиса выполняют соответственно:

- в части функций ВДЛ – управляющие филиалами и главы представительств;
- в части функций руководителей ССП – начальники управлений/отделов филиала / соответствующие работники по решению глав представительств;

- в части функций Ответственного подразделения - подразделения, осуществляющие функции по вопросам безопасности;
- в части функций ИТ-блока - подразделения, осуществляющие функции сопровождения автоматизированных систем;
- в части функций ЮД - юридическая служба (юрист) филиала или представительства;
- в части функций Департамента по работе с персоналом – кадровые службы или лица, ответственные за организацию работы с персоналом в филиалах или представительствах.

Прочие функции осуществляются работниками филиалов и представительств в соответствии с решением управляющих филиалами и глав представительств.

11.3. Ответственность за поддержание настоящей Частной политики в актуальном состоянии возлагается на руководителя Ответственного подразделения.

11.4. В случае изменения законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативно-методических рекомендаций, требований уполномоченных органов настоящая Частная политика применяется в части, не противоречащей вновь принятым нормативным правовым документам. При необходимости Ответственное подразделение незамедлительно инициирует внесение соответствующих изменений в настоящую Частную политику в порядке, установленном «Положением о внутренних нормативных документах ГПБ (ОАО)» от 25.12.2013 № И/95.

11.5.Внесение изменений в настоящую Частную политику должно осуществляться на периодической и внеплановой основе:

- периодическое внесение изменений не реже одного раза в 3 года;
- внеплановое внесение изменений может производиться в случае изменения законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов, а также по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, по результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.

Приложение

к «Частной политике защиты персональных данных в «Газпромбанк» (Открытое акционерное общество)»
от _____ № ___

Перечень внешних нормативных документов, используемых при подготовке настоящей Частной политики

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

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

3^1. «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержден приказом Минкультуры России от 25.08.2010 № 558.

3^2. Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн. Зарегистрирован Минюстом России от 14.5.2013 № 28375.

3^3. «Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных», утверждены приказом Роскомнадзора от 19.08.2011 № 706.

4. Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», утвержден распоряжением Банка России от 21.06.2010 № Р-705.

5. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» (СТО БР ИББС-1.2-2010), утвержден распоряжением Банка России от 21.06.2010 № Р-705.

5^1. Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, утвержден приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 01.12.2009 № 630.

6. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.3-2010), утверждены распоряжением Банка России от 21.06.2010 № Р-705.

7. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.4-2010), утверждены распоряжением Банка России от 21.06.2010 № Р-705.

8. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации, разработанные совместно Банком России, Ассоциацией российских банков и Ассоциацией региональных банков России (Ассоциация «Россия») и опубликованные в совместном письме от 28.06.2010 № 01-23/3148 «О введении в действие Стандартов и Рекомендаций в области стандартизации Банка России по вопросам информационной безопасности банковской организации Российской Федерации».