Утверждено Правлением
ПАО «Томскпромстройбанк»
протокол № б/н от 12.04.2017г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАО «ТОМСКПРОМСТРОЙБАНК»

1. Общие положения.

1.1.Политика информационной безопасности ПАО «Томскпромстройбанк» (далее по тексту - Политика) разработана в соответствии с нормами законодательства Российской Федерации в области обеспечения информационной безопасности и учитывает требования нормативных документов Банка России, федерального органа исполнительной власти, уполномоченного в области безопасности (ФСБ России), федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России).

1.2. Политика является общедоступным документом, который отражает систему взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в ПАО «Томскпромстройбанк».

1.3. Действие настоящей Политики распространяется на деятельность всех сотрудников головной организации и филиалов ПАО «Томскпромстройбанк» (далее по тексту - Банк).

1.4. В соответствии с Уставом Банка и рекомендациями Банка России «Методические рекомендациями по документированию в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» (РС БР ИББС-2.0) Политика является корпоративным документом первого уровня и утверждается Правлением Банка.

1.5. Пересмотр настоящей Политики может осуществляться в следующих случаях:

– если произошли изменения в составе банковских технологических процессов;

– если произошли изменения требований по информационной безопасности в законодательстве Российской Федерации (РФ) и/или нормативных документах Банка России, ФСБ России, ФСТЭК России;

– если выявлены новые актуальные угрозы и/или нарушители информационной безопасности;

– если обнаружены несовершенства в процедурах обеспечения и/или управления информационной безопасностью.

1.6. В Политике используются термины, в соответствии со Стандартом Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

2. Цель, задачи и принцип обеспечения информационной безопасности в Банке.

2.1. Цель обеспечения информационной безопасности в Банке – защита активов от возможного их несанкционированного использования, которое может привести к нанесению ущерба Банка, его клиентам, акционерам, сотрудникам и партнерам.

2.2. Для достижения поставленной цели в Банке решаются следующие задачи:

– анализ и оценка актуальных угроз и нарушителей информационной безопасности;

– оценка рисков информационной безопасности;

– внедрение организационных, программно-аппаратных и технических мер защиты информации;

– создание условий для оперативного реагирования на угрозы информационной безопасности.

2.3. Принципы обеспечения информационной безопасности в Банке:

– законность;

– процессный подход;

– непрерывность функционирования;

– персональная ответственность.

2.4. Законность функционирования системы обеспечения информационной безопасности в Банке достигается путем соответствия внедряемых защитных мер требованиям:

– законодательства РФ о банковской тайне и стандартов безопасности;

– законодательства РФ о национальной платежной системе и нормативных документов Банка России, регламентирующих вопросы защиты информации при осуществлении переводов денежных средств;

– законодательства РФ в области обработки персональных данных и нормативных документов ФСБ России и ФСТЭК России, регламентирующих вопросы обеспечения безопасности персональных данных при их обработке в информационных системах Банка.

2.5. Процессный подход к обеспечению информационной безопасности заключается в построении системы обеспечения информационной безопасности через призму анализа бизнес-процессов, функционирующих в Банке.

2.6. Непрерывность функционирования системы обеспечения информационной безопасности достигается Банком путем применения циклической модели Демминга к процессу обеспечения информационной безопасности «….планирование – реализация – проверка – совершенствование….».

2.7. Персональная ответственность достигается путем установления ответственности каждого сотрудника Банка, вовлеченного в процесс обеспечения информационной безопасности.

3. Общие сведения об активах, подлежащих защите в Банке.

3.1. В качестве активов Банка, информационную безопасность которых необходимо обеспечивать, рассматриваются следующие типы активов:

– информационные активы – информация, содержащая сведения, относящиеся к банковской тайне, коммерческой тайне клиентов, к персональным данным субъектов персональных данных, к платежной информации, в том числе при осуществлении переводов денежных средств, а так же информация, определяющая параметры конфигурирования и эксплуатации средств защиты информации, независимо от формы представления такой информации;

– программные активы – прикладное и системное программное обеспечение, а так же среда разработки прикладного программного обеспечения;

– физические активы – автоматизированные рабочие места (персональные компьютеры, серверы), коммуникационное оборудование (маршрутизаторы, коммутаторы, модемы), периферийная техника (принтеры, сканеры), устройства самообслуживания и торговые терминалы.

4. Модель угроз и нарушителей информационной безопасности.

4.1. В качестве возможных угроз нарушения информационной безопасности в Банке рассматриваются три основных класса угроз:

– угрозы нарушения конфиденциальности информации;

– угрозы нарушения целостности информации;

– угрозы нарушения доступности информации.

4.2. Каждая угроза информационной безопасности расписывается и анализируется следующим образом: «источник угрозы информационной безопасности» - «способ несанкционированного доступа к активу» - «несанкционированные действия с активом» -

«уровень реализации угрозы информационной безопасности» - «нарушение характеристики безопасности актива».

4.3. В качестве одного из основных источников угроз информационной безопасности в Банке рассматриваются лица, которые могут получить несанкционированный доступ к активам Банка (нарушители информационной безопасности).

4.4. С учетом разделения нарушителей информационной безопасности на внешних, внутренних и комбинированных в качестве возможных потенциальных нарушителей информационной безопасности могут выступать:

4.4.1 Внешние нарушители информационной безопасности:

– клиенты Банка;

– лица, случайно или намеренно, получившие доступ к информационным активам Банка через внешние телекоммуникационные каналы связи;

– конкурирующие кредитные организации;

– программисты-разработчики программных компонент, не являющиеся сотрудниками Банка;

– компании, обеспечивающие поставку и ремонт компьютерной техники;

– спецслужбы и представители силовых ведомств, имеющие возможность применять специальные средства и способы атак на информационные активы Банка.

4.4.2. Внутренние нарушители информационной безопасности:

– сотрудники Банка, имеющие легальный доступ к ресурсам автоматизированной банковской системы;

– сотрудники Банка, осуществляющие доступ к информационным активам с использованием технологии удаленного доступа;

– сотрудники Банка, имеющие полномочия системного администратора или администратора информационной безопасности;

– программисты-разработчики программных компонент, являющиеся сотрудниками Банка.

4.4.3 Комбинированные нарушители информационной безопасности - сотрудники Банка, действующие в сговоре с внешними нарушителями информационной безопасности.

4.5. В зависимости от цели, квалификации, технического оснащения и прав доступа к информационным системам Банка нарушители информационной безопасности могут реализовывать атаки на уровне сетевого оборудования, операционных систем, систем управления базами данных, сетевых приложений и сервисов, банковских приложений и сервисов, используя следующие способы несанкционированного доступа:

– внедрение вредоносного программного обеспечения;
– кража носителей информационных активов;
– кража технических средств обработки информационных активов;
– несанкционированное повышение привилегий сотрудника Банка в системе;
– несанкционированные действия сотрудников Банка в системе;
– физическое подключение к каналу связи с целью перехвата информации;
– внесение недекларированных возможностей и/или программных закладок;
– внедрение ложных сетевых сервисов;
– подмена доверенного объекта;
– навязывание ложного сетевого маршрута;
– удаленный запуск приложений и т.д.

4.6. Все способы несанкционированного доступа к активам могут быть направлены на преднамеренное или случайное копирование, модификацию, удаление, передачу по каналам связи и/или передачу на материальных носителях, с целью нарушения конфиденциальности, целостности и/или доступности актива.

4.7. Детальная модель угроз и нарушителей информационной безопасности для информационных систем Банка формируется в отдельных внутренних документах Банка.

5. Процесс обеспечения информационной безопасности.

5.1. Построение системы обеспечения информационной безопасности (далее по тексту - СОИБ) с использованием модели Демминга заключается в цикличном выполнении следующей группы процессов:

– планирование СОИБ;

– реализация СОИБ;

– проверка СОИБ;

– совершенствование СОИБ.

5.2. На этапе планирования СОИБ в Банке осуществляется:

5.2.1. Анализ требований законодательства РФ и нормативных документов Банка России в области обеспечения информационной безопасности.

5.2.2. Определение и распределение ролей сотрудников Банка в области обеспечения информационной безопасности.

5.2.3. Анализ и оценка рисков информационной безопасности:

– идентификация информационных, программных и физических активов Банка;

– определение потенциальных нарушителей информационной безопасности для Банка (модель нарушителя);

– определение значимых для Банка угроз информационной безопасности (модель угроз информационной безопасности);

– оценка вероятности возникновения угроз информационной безопасности;

– оценка степени влияния угроз информационной безопасности на деятельность Банка;

– оценка рисков нарушения информационной безопасности в Банке;

– рассмотрение различных вариантов применения средств защиты информации, в целях минимизации выявленных рисков информационной безопасности;

– оценка затрат на реализацию средств защиты.

5.2.4. Формирование требований к системе информационной безопасности по следующим направлениям:

– комплексная антивирусная защита информационных систем Банка;

– управление логическим доступом к активам Банка;

– управление средствами криптографической защиты и их ключевыми системами;

– использование сотрудниками Банка сети Интернет и корпоративной электронной почты;

– межсетевое взаимодействие информационных систем Банка;

– управление физическим доступом сотрудников в помещения Банка;

– аудит событий информационной безопасности.

5.2.5. Определение и закрепление ответственности сотрудников Банка, принимающих участие в процессе обеспечения информационной безопасности, осуществляется во внутренних документах Банка и должностных инструкциях сотрудников.

5.3. На этапе реализации СОИБ в Банке осуществляется:

5.3.1. Внедрение внутренних распорядительных документов, регламентирующих требования к системе обеспечения информационной безопасности в информационных системах Банка по направлениям, указанным в п.5.2.4 настоящей Политики.

5.3.2. Внедрение и конфигурирование программных, программно-аппаратных и технических средств защиты информации.

5.3.3. Внедрение процедур управления инцидентами информационной безопасности.

5.3.4. Повышение осведомленности сотрудников Банка в вопросах обеспечения информационной безопасности.

5.3.5. Обеспечение непрерывности функционирования информационных систем Банка и возможности восстановления их после сбоя.

5.4. На этапе проверки СОИБ в Банке осуществляется:

5.4.1. Контроль корректности функционирования программных, программно-аппаратных и технических средств защиты информации.

5.4.2. Контроль исполнения сотрудниками Банка внутренних документов Банка, регламентирующих вопросы обеспечения информационной безопасности.

5.4.3. Проведение оценки соответствия системы обеспечения информационной безопасности требованиям к защите информационных активов Банка, установленных законодательством РФ, нормативными документами Банка России, ФСБ России и/или ФСТЭК России.

5.5. На этапе совершенствования СОИБ в Банке осуществляется:

– анализ результатов проверки СОИБ;

– внесение оперативных изменений в состав и конфигурацию средств защиты информации;

– внесение изменений в документы, регламентирующие деятельность по обеспечению информационной безопасности;

– разработка планов по тактическим улучшениям СОИБ.

6. Организационная составляющая процесса обеспечения информационной безопасности.

6.1. Для достижения цели обеспечения информационной безопасности в Банке выделены следующие роли:

– Куратор – Заместитель Председателя Правления;

– Подразделение по информационной безопасности – сектор по информационной безопасности;

– Ответственный сотрудник филиала Банка;

– Сотрудник Банка.

6.2. Сотрудники, выполняющие роли, указанные в п.6.1. настоящей Политики, определяются приказом по Банку (филиалу).

6.3. К основным задачам, решаемым Куратором, относятся:

– определение и согласование лиц, ответственных за обеспечение информационной безопасности;

– координация работ по построению системы обеспечения информационной безопасности;

– согласование внутренних документов по направлению обеспечения информационной безопасности Банка.

6.4. К основным задачам, решаемым Подразделением по информационной безопасности, относятся:

– организация и выполнения работ по выполнению требований законодательства Российской Федерации в области обеспечения информационной безопасности, нормативных документов Банка России, ФСБ России, ФСТЭК России и стандартов безопасности (СТО БР ИББС);

– анализ и оценка рисков нарушения информационной безопасности, в разрезе банковских технологических процессов;

– выработка требований и механизмов защиты информации, участвующей в процессе функционирования банковских технологических процессов;

– определение состава внутренних документов Банка, регламентирующих деятельность по обеспечению информационной безопасности, а так же внесение в них изменений и/или дополнений;

– работа с сотрудниками Банка, в части повышения их уровня осведомленности в вопросах обеспечения информационной безопасности;

– выявление и реагирование на инциденты информационной безопасности;

– мониторинг, контроль и оценка эффективности принятых мер по обеспечению информационной безопасности и применяемых средств защиты информации.

6.5. К основным задачам, решаемым Ответственным сотрудником филиала Банка, относятся:

– организация работ по выполнению требований внутренних документов Банка, в области обеспечения информационной безопасности;

– регистрация и информирование, в установленном порядке, об инцидентах информационной безопасности.

6.6. К основным задачам, решаемым Сотрудником Банка, в рамках выполнения деятельности по информационной безопасности относятся:

– соблюдение требований законодательства и внутренних документов Банка, регламентирующих деятельность по информационной безопасности;

– выявление, регистрация и информирование, в установленном порядке, об инцидентах информационной безопасности на своем участке работ.

7. Контроль и ответственность.

7.1. Сотрудник Банка несет ответственность за несоблюдение требований настоящей Политики.

7.2. Ответственность за поддержание Политики в актуальном состоянии несет начальник подразделения по информационной безопасности.

7.3. Контроль за выполнением требований Политики осуществляется:

– подразделением по информационной безопасности - постоянно, в рамках мероприятий по мониторингу и контролю защитных мер, а так же в рамках проведения внутренних проверок, оценки соответствия требованиям нормативных документов Банка России и стандартов безопасности;

– ответственным сотрудником филиала Банка - постоянно, в рамках мероприятий по соблюдению процедур обеспечения информационной безопасности филиала Банка;

– службой внутреннего аудита - ежегодно в головной организации и в ходе комплексных проверок в филиалах Банка.