МОРСКОЙ БАНК

ПРИКАЗ

«31» марта 2014 г. № МБ - 81

Москва

Об утверждении «Политики информационной безопасности МОРСКОГО БАНКА (ОАО)»

В целях утверждения Политики информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с даты подписания настоящего Приказа «Политику информационной безопасности МОРСКОГО БАНКА (ОАО)».
2. Управлению делами (Терентьева Е.Ю.) довести настоящий Приказ до всех сотрудников Банка.
3. Контроль за исполнением настоящего Приказа возложить на Вице-президента по безопасности Школина А.Л.

Председатель Правления **Ю.В. Бардин**

МОРСКОЙ БАНК

УТВЕРЖДЕНО

Приказ Председателя Правления

МОРСКОГО БАНКА (ОАО)

№ МБ- 81 **от «** 31 **»** марта **2014г.**

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОРСКОГО БАНКА (ОАО)

Москва, 2014 г.

СОДЕРЖАНИЕ

1. Общие положения

1.1. «Политика информационной безопасности» (далее – Политика) МОРСКОГО БАНКА (ОАО) (далее – Банк) разработана в соответствии с законодательством Российской Федерации в части обеспечения информационной безопасности и защиты информации, требованиями Центрального банка Российской Федерации, требованиями Федеральных служб, уполномоченных в области безопасности, надзора в сфере связи, информационных технологий и массовых коммуникаций.

1.2. Настоящая Политика является основополагающим документом, определяющим официально принятую руководством Банка систему приоритетов, целей, принципов и методов обеспечения информационной безопасности (далее – ИБ) Банка. Наряду с другими документами системы менеджмента ИБ, Политика определяет взаимосвязанную совокупность общих требований, основополагающих принципов, а также конкретных регламентов и инструкций в области обеспечения ИБ и защиты информации, которыми Банк руководствуется в своей деятельности.

1.3. Соблюдение требований Политики и связанных с ней документов системы менеджмента ИБ (далее – СМИБ) предоставляют Банку конкурентные преимущества в глазах клиентов, соответствие правовым, регулятивным, договорным требованиям, обеспечивают стабильность бизнес-процессов и в конечном итоге ведут к повышению финансовых результатов Банка.

1.4. Руководство Банка осознает важность защиты конфиденциальной информации, необходимость развития, совершенствования принимаемых организационных мер и используемых технических средств обеспечения ИБ в контексте совершенствующегося законодательства, норм регулирования банковской деятельности, развивающихся информационных технологий, а также ожиданий пользователей банковских услуг.

1.5. Требования Политики распространяются на все структурные подразделения Банка и обязательны к исполнению всеми работниками и должностными лицами Банка, а также представителями организаций-контрагентов, в рамках заключаемых договоров при использовании информационных ресурсов Банка.

1.6. Общее руководство обеспечением ИБ Банка выполняет Вице-Президент по безопасности. Ответственность за организацию мероприятий по защите информации, обеспечению ИБ, контролю за соблюдением требований Политики несут выделенные подразделения по обеспечению безопасности в Головном офисе и филиалах, либо ответственные лица, наделенные ролью защиты информации и обеспечения ИБ в филиалах и структурных подразделениях Банка.

1.7. Руководители подразделений Банка ответственны за обеспечение выполнения требований Политики и иных документов СМИБ своими подчинёнными. Работники Банка обязаны соблюдать требования настоящей Политики, других нормативных документов по вопросам ИБ и защиты информации. Невыполнение работниками Банка требований документов СМИБ приравнивается к невыполнению должностных инструкций и влечёт дисциплинарную ответственность.

1.8. Настоящая Политика является корпоративным документом по ИБ первого уровня в соответствии с Рекомендациями в области стандартизации Банка России РС БР ИББС 2.0 2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС 1.0», принятыми и введенными в действие распоряжением Банка России от 28 апреля 2007г. № Р-348.

1.9. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются

документами по ИБ второго уровня. Частные политики оформляются как отдельные внутренние нормативные документы Банка, разрабатываются и согласуются в соответствии с установленным в Банке порядком.

2. *Термины и сокращения*

2.1 **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая заданную технологию.

2.2 **Автоматизированная банковская система (АБС)** – АС, реализующая заданный банковский платежный или информационный процесс.

2.3 **Аудит информационной безопасности (аудит ИБ)** - систематический, независимый и документируемый процесс получения свидетельств деятельности Банка по обеспечению информационной безопасности, установления степени выполнения в Банке критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности Банка.

2.4 **Банковский технологический процесс** – последовательность технологически связанных операций по изменению и (или) определению состояния активов Банка, используемых при функционировании или необходимых для реализации банковских услуг.

2.5 **Информационная безопасность (ИБ)** – состояние защищенности банковских технологических процессов, автоматизированных систем, автоматизированных банковских систем по отношению к угрозам информационной безопасности.

2.6 **Информация** – любые сведения, сообщения, данные независимо от формы их представления.

2.7 **Инцидент информационной безопасности** – проявление одного или нескольких событий, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

2.8 **Конфиденциальная информация** – информация, в отношении которой Банком установлен режим конфиденциальности.

2.9 **Модель угроз информационной безопасности** - описание источников угроз ИБ, методов реализации угроз, объектов реализации угроз, уязвимостей, используемых источниками угроз, масштабов потенциального ущерба.

2.10 **Модель нарушителя информационной безопасности** – описательное представление нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, мотивации действий, способов реализации угроз.

2.11 **Оценка риска нарушения информационной безопасности** - систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести определение величин рисков нарушения ИБ, связанных с использованием информационных активов Банка на всех стадиях их жизненного цикла.

2.12 **Обработка риска нарушения информационной безопасности** - процесс выбора и осуществления защитных мер, снижающих величину риска нарушения ИБ, или использование мер по уходу, переносу или принятию риска.

2.13 **Пользователь информационной системы** - работник Банка, специалист, оказывающий услуги или выполняющий работы для Банка, физическое лицо, обладающее возможностью доступа к информационной системе Банка.

2.14 **Риск нарушения информационной безопасности** - мера, учитывающая вероятность реализации угрозы ИБ или величину ущерба от неё.

2.15 **Система информационной безопасности** - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное обеспечение.

2.16 **Система менеджмента информационной безопасности (СМИБ)** - часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

2.17 **Система обеспечения информационной безопасности (СОИБ)** - совокупность системы информационной безопасности и системы менеджмента информационной безопасности Банка.

2.18 **Угроза информационной безопасности** – операционный риск, влияющий на нарушение одного или нескольких свойств информационной безопасности целостности, доступности или конфиденциальности информационных активов Банка.

3. Область действия

3.1 Основными объектами защиты системы информационной безопасности в Банке являются:

- информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения независимо от формы и вида их представления;
- платежные и информационные технологические процессы;
- сотрудники Банка как пользователи информационных ресурсов;
- технологическая инфраструктура, включающая системы обработки и анализа информации, каналы информационного обмена, телекоммуникационные системы и средства защиты информации, объекты и помещения, в которых размещены информационные системы.

3.2 К объектам, подлежащим защите от потенциальных угроз и противоправных действий в рамках настоящей Политики относятся:

- банковские системы, информационные ресурсы Банка, массивы и базы данных, программные комплексы и рабочие места сотрудников;
- информация с ограниченным доступом, составляющая служебную или банковскую тайну, а также иная конфиденциальная информация на бумажной или иной другой основе;
- средства и системы информатизации – технические средства обработки, передачи информации, линии телеграфной, телефонной, факсимильной связи, средства копирования, вспомогательные технические средства;
- персонал Банка, имеющий непосредственный доступ к финансам, нематериальным ценностям, хранилищам;
- системы дистанционного банковского обслуживания, торговые площадки, используемые Банком в повседневной работе.

4. Задачи обеспечения ИБ

4.1 Целью деятельности по обеспечению ИБ Банка является снижение угроз ИБ до приемлемого в Банке уровня. В процессе достижения цели решаются следующие задачи:

- устойчивое функционирование Банка;
- защита интересов владельцев Банка;
- охрана жизни и здоровья персонала;

- обеспечение доступности информационных ресурсов;
- обеспечение целостности информации;
- обеспечение конфиденциальности информации ограниченного доступа;
- соблюдение требований законодательства в области ИБ;
- поддержание адекватности мер защиты реальным угрозам ИБ Банка;
- повышение доверия клиентов Банку;
- поддержка непрерывности бизнеса;
- своевременное информирование руководства Банка о состоянии ИБ;
- минимизация угроз ИБ;
- снижение рисков и возможного ущерба при их реализации, как для самого Банка, так и для его клиентов.

4.2 В процессе решения поставленных задач проводятся следующие работы:

4.2.1 Анализ циркулирующей в Банке информации, отнесение различных видов информации к различным категориям, организация работ по разграничению доступа и защите информации в соответствии с установленными категориями;

4.2.2 Прогнозирование, своевременное выявление и устранение угроз безопасности ресурсам и персоналу Банка, обнаружение предпосылок и условий, способных привести к финансовому, материальному, репутационному или иному ущербу;

4.2.3 Разработка и внедрение механизмов реагирования на существующие и возможные угрозы ИБ, на проявление негативных тенденций в функционировании Банка на основе правовых, организационных, технических и иных мер и средств обеспечения безопасности;

4.2.4 Принятие мер для максимально возможной локализации возникающего ущерба вследствие реализации угроз ИБ, неправомерных действий физических или юридических лиц, природных или техногенных явлений, ослабление влияния последствий нарушения безопасности на достижение стратегических целей Банка.

4.2.5 Комплексное использование методов и средств защиты, применение разнородных средств для построения целостной системы ИБ, перекрывающей все выявленные каналы реализации угроз.

4.2.6 Непрерывность защиты, предполагающая принятие соответствующих мер на всех этапах жизненного цикла АС.

4.2.7 Обеспечение безопасности и физической защиты персонала, установление режима охраны, пропускного режима на объекты Банка.

4.2.8 Выявление конфиденциальной информации, обоснование уровня её конфиденциальности и документальное оформление в виде перечня сведений, подлежащих защите.

4.2.9 Защита информации, хранимой и обрабатываемой средствами вычислительной техники и связи.

4.2.10 Минимизация полномочий, т.е. предоставление сотрудникам минимальных прав доступа в соответствии с должностными обязанностями.

4.2.11 Тщательный подбор персонала, соответствие профессиональных, образовательных, организационных и личных качеств каждого кандидата предполагаемой работе.

4.2.12 Предварительное планирование мероприятий по изменению существующей структуры информационных ресурсов Банка, предварительные испытания систем.

4.2.13 Недопущение несанкционированных модификаций используемых систем, процессов, способов организации работ.

4.2.14 Мониторинг используемых систем обработки информации, телекоммуникационных каналов, информационных ресурсов, ведение протоколов работы, их периодический анализ.

4.2.15 Оперативное реагирование на инциденты и нарушения политики ИБ, информирование руководства.

4.2.16 Постоянный контроль за уровнем ИБ сотрудниками Банка, информирование руководства службы безопасности обо всех замеченных или предполагаемых недостатках или угрозах ИБ

4.2.17 Персональная ответственность за обеспечение безопасности информации и банковских систем каждого сотрудника в пределах его полномочий.

4.2.18 Экономическая целесообразность уровня затрат на обеспечение ИБ ценности информационных ресурсов и величине возможного ущерба. Постоянное совершенствование мер и средств защиты информации

4.2.19 Обязательность контроля, своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

5. Методы и средства защиты

5.1 Обеспечение ИБ реализуются комплексом организационных, технологических мер, разработкой нормативной документации.

5.2 Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Банка обеспечивает эффективное решение следующих задач:

5.2.1 своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Банка;

5.2.2 создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

5.2.3 создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидации последствий нарушения безопасности информации;

5.2.4 защиту от вмешательства в процесс функционирования информационной системы Банка посторонних лиц;

5.2.5 разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Банка;

5.2.6 защиту от несанкционированной модификации используемых в корпоративной информационной системе Банка программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

5.2.7 обеспечение безотказной работы криптографических средств защиты информации.

5.3 Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

5.3.1 строгим учетом всех подлежащих защите ресурсов информационной системы Банка (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

5.3.2 регистрацией в Журналах действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;

5.3.3 полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Банка по вопросам обеспечения безопасности информации;

5.3.4 подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

5.3.5 наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Банка;

5.3.6 четким знанием и строгим соблюдением всеми пользователями информационной системы Банка требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

5.3.7 персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Банка;

5.3.8 непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Банка;

5.3.9 применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

5.3.10 эффективным контролем над соблюдением пользователями информационных ресурсов Банка требований по обеспечению безопасности информации;

5.3.11 юридической защитой интересов Банка при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

6. Система обеспечения ИБ (СОИБ)

СОИБ Банка строится на основе следующих принципов:

6.1 Законность. Любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства Российской Федерации с применением всех разрешенных законом методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты Банка.

6.2 Взаимная ответственность. У станавливаются требования к владению, классификации и индивидуальной ответственности пользователей, так или иначе имеющих отношение к информационным активам. Определяется персональная ответственность руководителей и исполнителей всех уровней за выполнение требований и соблюдение установленных мер ИБ.

6.3 Взаимодействие и координация. Меры СОИБ осуществляются на основе четкой взаимосвязи соответствующих структурных единиц Банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями (органами государственного управления, другими организациями и предприятиями).

6.4 Осведомленность. Работники Банка, а также представители внешних организаций - клиентов и контрагентов Банка, осведомляются о требованиях по обеспечению ИБ в объёме, требуемом для выполнения их служебных обязанностей. Нормативные документы по ИБ содержат предмет, обязательства и меры ответственности, как со стороны Банка, так и со стороны осведомляемого лица или организации. Уровень осведомленности в области ИБ подлежит регулярному контролю со стороны уполномоченных лиц.

6.5 Знание своих клиентов и служащих. Банк принимает необходимые меры для получения информации о своих клиентах в рамках федерального законодательства. В Банке существуют процедуры идентификации работников перед приемом на работу.

6.6 Компетентность и специализация. Решения, влияющие на уровень обеспечения ИБ, включая выбор средств информатизации и защиты информации, распределение обязанностей работников, информационного взаимодействия с бизнес-партнёрами и др. обязательно согласуются с Управлением экономической безопасности.

6.7 Комплексность. Для обеспечения ИБ Банка необходимо согласованное применение всех доступных правовых, организационных и технических мер, перекрывающих в совокупности все существенные каналы реализации угроз ИБ. СОИБ строится не только с учетом известных атак и каналов утечки информации, но и с учетом возможности появления принципиально новых атак и путей реализации угроз ИБ.

6.8 Непрерывность процесса защиты информации. Обеспечение ИБ представляет собой непрерывный процесс, осуществляемый на всех этапах жизненного цикла информации и банковских систем.

6.9 Эшелонирование защиты. В целях усиления защищённости и повышения вероятности обнаружения атак, защита строится эшелонировано. Наряду с защитой периметра Банка от внешних угроз, обеспечивается организация и защита внутренних периметров.

6.10 Простота реализации и применения средств защиты информации. Выбираемые механизмы защиты как правило максимально просты и понятны в реализации и использовании. Простота и общепримснимость механизмов защиты является дополнительным фактором защищенности Банка.

6.11 Приоритет мер предупреждения. СОИБ Банка ориентирована на профилактику и своевременное выявление предпосылок возникновения и реализации угроз ИБ.

6.12 Минимизация привилегий, разделение полномочий. Каждому пользователю предоставляются минимально необходимые для выполнения его должностных обязанностей права. Эти права изменяются в соответствии с изменением должностных обязанностей работников. Выполняется периодический мониторинг соответствия прав доступа пользователей их должностным обязанностям.

6.13 Доступность услуг и сервисов. Активы доступны легальным пользователям, внутренним и внешним, в течение определённого нормативными документами времени. Для критически важных активов разработаны планы обеспечения непрерывности деятельности и восстановления работоспособности после прерываний.

6.14 Централизация управления. Организационные и технические меры СОИБ строятся максимально централизованными, обеспечивая функционирование системы по единым правовым, организационным, функциональным и методологическим принципам. Централизация управления обеспечивает максимальную информированность работников, обеспечивающих управление средствами ИБ, обоснованность, оперативность и минимальные затраты на координацию решений.

6.15 Гибкость управления и применения. При построении/модернизации СОИБ процессы организуются таким образом, чтобы состав средств защиты и техническая политика, реализуемая средствами защиты, могли с минимальными затратами времени и

ресурсов перенастраиваться в зависимости от изменений бизнес-процессов, появления новых (реальных или потенциальных) угроз.

6.16 Адекватность и экономическая обоснованность защитных мер. Применяемые защитные меры соответствуют адекватным моделям угроз и нарушителей, а также учитывают соотношение между величиной затрат на их реализацию и возможными потерями от реализации угроз. Объем финансовых затрат на СОИБ определяется на основе оценок ущерба от ликвидируемых угроз.

7. *Система менеджмента информационной безопасности (СМИБ)*

7.1 СМИБ является частью общей системы менеджмента Банка, которая ориентирована на содействие достижению бизнес-целей через обеспечение защищенности информационной сферы.

7.2 Общее руководство обеспечением информационной безопасности Банка осуществляют Совет Директоров, Правление и Председатель Правления Банка.

7.3 Координация ИБ на корпоративном уровне осуществляется Председателем Правления Банка. Для выполнения этой задачи Председатель Правления Банка:

- определяет задачи и распределяет обязанности для обеспечения ИБ Банка;
- оценивает возможности практического применения специальных методологий и процессов, принимает решение об их использовании;
- исследует инициативы, связанные с ИБ, и принимает решение по их одобрению;
- знакомится с основными событиями ИБ;

7.4 Правление Банка назначает Куратора СМИБ из числа заместителей Председателя Правления Банка или директоров Департаментов. Куратор СМИБ не должен быть одновременно куратором информационных технологий.

7.5 Ответственность за реализацию мероприятий системы информационной безопасности и общий контроль за соблюдением требований информационной безопасности в Банке несет начальник Управления экономической безопасности.

7.6 Руководители структурных подразделений Банка несут ответственность за обеспечение выполнения требований политик ИБ в своих подразделениях.

7.7 В случае изменения действующего законодательства и иных нормативных актов, а также Устава Банка настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Банка.

7.8 С целью поддержки заданного уровня защищенности Банк придерживается процессного подхода в построении системы менеджмента информационной безопасности. Система менеджмента информационной безопасности Банка основывается на осуществлении основных процессов - планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование, соответствующих требованиям стандарта Банка России СТО БР ИББС–1.0. Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности Банка и повышение ее эффективности.

7.9 Нормативно-методическое обеспечение предполагает создание сбалансированной базы внутренних нормативных документов в области ИБ. Для этого разрабатывается и поддерживается в актуальном состоянии комплекс внутренних нормативных документов, обеспечивающих процесс эксплуатации СОИБ с учетом рекомендаций по стандартизации

Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».

7.10 Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, в Банке должен быть реализован ряд процессов, сгруппированных в виде циклической модели Деминга: «...- планирование – реализация и эксплуатация – мониторинг и анализ - совершенствование - планирование -...».

8. Планирование системы обеспечения информационной безопасности

8.1 Целью Банка в рамках группы процессов «планирование» является запуск «цикла» СМИБ путем определения первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе «совершенствование».

8.2 Выполнение деятельности на стадии «планирование» заключается в определении, документировании и реализации в Банке следующих процессов:

- определение/коррекция области действия СОИБ и подхода к оценке рисков нарушения ИБ;
- проведение оценки и разработка планов обработки рисков нарушения ИБ;
- принятие руководством Банка решений о реализации и эксплуатации СОИБ.

9. Реализация и эксплуатация системы обеспечения информационной безопасности

9.1 Этап «реализация» выполняется по результатам выполнения этапов «планирование» и (или) «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование», и (или) реализации решений, определенных на этапе «совершенствование».

9.2 Выполнение деятельности на стадии «реализация» заключается в определении, документировании и реализации в Банке следующих процессов:

- реализация планов внедрения СОИБ;
- реализация программ по обучению и повышению осведомленности в области ИБ;
- обнаружение и реагирование на инциденты ИБ;
- обеспечение непрерывности бизнеса и его восстановления после прерываний.

10. Мониторинг и анализ системы обеспечения информационной безопасности

10.1 Целью Банка на этапе процесса «мониторинг и анализ» является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и (или) внешним условиям функционирования Банка, связанным с ИБ. Результат выполнения деятельности на данном этапе является основой для выполнения деятельности по совершенствованию СОИБ.

10.2 Процессы мониторинга и анализа СОИБ Банка должны быть интегрированы в систему внутреннего контроля. Для этого в Банке должны быть определены, документированы и реализованы следующие процессы:

- мониторинг и контроль защитных мер;
- проведение периодического аудита и самооценки ИБ;
- анализ функционирования СОИБ;
- анализ СОИБ со стороны руководства Банка.

11. Совершенствование системы обеспечения информационной безопасности

11.1 Группа процессов «совершенствование» включает в себя деятельность по принятию решений о реализации тактических и (или) стратегических улучшений СОИБ.

11.2 Выполнение деятельности на стадии «совершенствование» заключается в определении, документировании и реализации в Банке следующих процессов:

- принятие решений по тактическим и стратегическим улучшениям СОИБ;
- информирование об изменениях и их согласование с заинтересованными сторонами.

12. Заключительные положения

12.1 Настоящая Политика должна пересматриваться и совершенствоваться на регулярной основе, не реже, чем один раз в три года, а также в случаях изменения законодательной базы или нормативных документов Банка России.

12.2 Предпосылками для пересмотра и совершенствования настоящей Политики могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния ИБ требованиям нормативных и регламентирующих документов).

12.3 Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.

12.4 Плановая проверка актуальности Политики проводится ежегодно с целью определения необходимости ее пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обеспечению информационной безопасности. Плановая проверка актуальности Политики проводится Координатором СМИБ или начальником Управления банковских информационных технологий Департамента банковских технологий не позднее двадцатого числа месяца ввода в действие последней редакции документа по состоянию на первый день этого месяца. В результате проверки устанавливается возможность продления или необходимость пересмотра действующей редакции Политики. Информация о проведенной проверке заносится в прилагаемый Лист записей о проверках актуальности документа.

12.5 Пересмотр Политики производится по решению Правления Банка по результатам плановой проверки актуальности, в случае выявления несоответствия определенного Политикой комплекса защитных мер фактам зафиксированных инцидентов информационной безопасности, при существенных изменениях в бизнес-процессах или при изменениях нормативной базы в области обеспечения информационной безопасности.