УТВЕРЖДЕНО
Председателем Правления ООО «Бланк банк»
Приказ от 20 июля 2022 г. №75/3

GBR.9

ПОЛИТИКА

информационной безопасности ООО «Бланк банк»

BLANC

СОДЕРЖАНИЕ

1. Общие положения

1.1. Политика информационной безопасности ООО «Бланк банк» (далее — Политика) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Банк в своей деятельности.

1.2. Основными целями Политики информационной безопасности Банка являются защита информации Банка и обеспечение эффективной работы всего информационно-вычислительного комплекса Банка при осуществлении деятельности, указанной в его Уставе.

1.3. Общее руководство обеспечением ИБ Банка осуществляет Председатель Правления Банка. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несут руководитель ОИБ и руководитель ЦСИС.

1.4. Руководители структурных подразделений Банка ответственны за обеспечение выполнения требований ИБ сотрудниками в своих подразделениях.

1.5. Сотрудники Банка обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией Банка, соблюдать требования настоящей Политики и других документов ИБ.

1.6. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна к исполнению всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Банка, а также в договорах.

2. Термины и сокращения

2.1. В настоящем документе использованы следующие термины с соответствующими определениями:

Автоматизированная банковская система — комплекс средств автоматизации Банка, используемый для реализации банковской информационной технологии.

Аудит информационной безопасности Банка — процесс проверки выполнения в Банке установленных требований по обеспечению информационной безопасности. Может проводиться как самим Банком (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит). Результаты проверки документально оформляются свидетельством аудита.

Аутентификация электронного сообщения — процесс проверки сообщения, позволяющий установить, что сообщение исходит из указанного источника, и не было изменено при передаче.

Банк — ООО «Бланк банк».

Банковская информационная технология — совокупность правил, приемов и методов применения средств вычислительной техники для выполнении функций хранения, обработки, передачи и использования финансовой, аналитической или другой связанной с функционированием Банка информации.

Банковский информационный технологический процесс — часть банковского технологического процесса, содержащая операции над неплатежной информацией, необходимой для функционирования Банка.

Банковский платежный технологический процесс — часть банковского технологического процесса, содержащая расчетные, учетные, кассовые и иные банковские операции над платежной информацией, связанные с перемещением денежных средств с одного счета на другой, открытием (закрытием) счетов или контролем за данными операциями.

База событий — постоянно обновляемая аналитическая база данных о событиях операционного риска и потерях, понесенных вследствие его реализации.

Интернет-банкинг — система дистанционного банковского обслуживания клиентов, осуществляемого Банком в сети Интернет.

Информационная безопасность Банка — состояние защищенности информационных активов Банка в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Банка. Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Банка.

Информационная система Банка — взаимосвязанная совокупность данных, программам и аппаратного обеспечения.

Информационные активы Банка — активы Банка, имеющие отношение к его информационной сфере и представляющие ценность для него с точки зрения достижения уставных целей.

Инцидент информационной безопасности — событие ИБ или комбинация таких событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:
- нарушение в СОИБ организации БС РФ, включая нарушение работы средств защиты информации;
- нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение в выполнении процессов СМИБ организации БС РФ;
- нарушение в выполнении Банковских технологических процессов организации БС РФ;
- нанесение ущерба организации БС РФ и (или) ее клиентам

Ключевые индикаторы риска — количественные контрольные показатели риска информационной безопасности, направленные на измерение и контроль уровня операционного риска в определенный момент времени.

Код аутентификации электронного сообщения — данные, используемые для установления подлинности и контроля целостности электронного сообщения.

Мобильный банкинг — доступ к услугам дистанционного банковского обслуживания с помощью специально разработанных приложений для мобильных телефонов и планшетов.

Мониторинг информационной безопасности Банка — постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности в Банке, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная банковская система или ее часть, банковские информационные технологические процессы, информационные банковские услуги и пр.

Операционный риск — риск возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов Банка, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий.

Политика информационной безопасности Банка — комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Банке для обеспечения его информационной безопасности.

Система обеспечения информационной безопасности — совокупность Системы информационной безопасности и Системы менеджмента информационной безопасности Банка.

Система информационной безопасности — совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента информационной безопасности — часть системы менеджмента Банка, предназначенного для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

Терминальное устройство дистанционного банковского обслуживания — устройство, используемое при осуществлении переводов денежных средств посредством дистанционного банковского обслуживания (банкоматы, платежные терминалы).

Управление информационной безопасностью Банка — совокупность целенаправленных действий, осуществляемых в рамках Политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

Уязвимость — недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Банка при реализации угроз в информационной сфере.

2.2. Принятые сокращения:

АБС — автоматизированная банковская система.

БЭСП — система банковских электронных срочных платежей.

ИБ — информационная безопасность.

НСД — несанкционированный доступ.

ОИБ — отдел информационной безопасности.

ОС — операционная система.

КИР — ключевые индикаторы риска.

РФ — Российская Федерация.

СКЗИ — средство криптографической защиты информации.

СУБД — система управления базами данных.

СВА — служба внутреннего аудита.

СВК — служба внутреннего контроля.

СКУД — система контроля и управления доступом.

ИСПДн — информационная система персональных данных.

ПД — персональные данные.

АРМ — автоматизированное рабочее место.

АС — автоматизированная система.

ТУ ДБО — терминальное устройство дистанционного банковского обслуживания.

ИС — информационная система.

ЦСИС — центр сопровождения информационных систем.

СОИБ — система обеспечения информационной безопасности.

СИБ — система информационной безопасности.

СМИБ — система менеджмента информационной безопасности.

3. Нормативная документация

— Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ
— Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2014 (далее — Стандарт БР СТО БР ИББС-1.0-2014)
— Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
— Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
— Положение Банка России от 23.12.2020 № 747-П «О требованиях к защите информации в платежной системе Банка России»
— Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»
— Национальный стандарт РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст) (далее — ГОСТ Р 57580.1-2017)
— Национальный стандарт РФ ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 г. № 156-ст) (далее — ГОСТ Р 57580.2-2018)
— Приказ ФАПСИ № 152 от 13.06.2001 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
— Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646)
— Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»
— Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
— Федеральный Закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
— GBR.45 Политика управления рисками
— GBR.716 Положение об управлении операционными рисками

4. Исходная концептуальная схема обеспечения информационной безопасности Банка

4.1. Концептуальная схема информационной безопасности Банка направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

4.2. Наибольшими возможностями для нанесения ущерба Банку обладает его собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом

злоумышленник может иметь сообщников как внутри, так и вне Банка), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

4.3. Для противодействия угрозам информационной безопасности в Банке на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ в Банке при минимальных ресурсных затратах.

4.4. Разработанная на основе прогноза Политика и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Банка. С течением времени меняется характер угроз, следовательно, необходимо своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

4.5. Стратегия обеспечения ИБ Банка заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала Банка и других пользователей ИС Банка.

5. Основные принципы обеспечения ИБ

5.1. Постоянный и всесторонний анализ ИС и банковской информационной технологии с целью выявления уязвимости информационных активов Банка.

5.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Банка, корректировка моделей угроз и нарушителя.

5.3. Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим банковским технологическим процессом. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Банка, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности для клиентов Банка.

5.4. Контроль эффективности принимаемых защитных мер.

5.5. Персонификация и адекватное разделение ролей и ответственности между сотрудниками Банка, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

6. Цели и задачи ИБ Банка

6.1. Основными целями ИБ Банка являются:
- повышение стабильности функционирования Банка в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение и (или) снижение ущерба от инцидентов ИБ.

6.2. Основными задачами деятельности по обеспечению ИБ Банка являются:
- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ
- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;

— организация антивирусной защиты информационных активов;
— защита информации от НСД и утечки по техническим каналам связи.
— своевременность обнаружения проблем, потенциально способных повлиять на бизнес-цели Банка;
— прогнозируемость развития проблем, что подразумевает выявление причинно-следственных связей возможных проблем и построение на этой основе точного прогноза их развития;
— адекватная оценка степени влияния выявленных проблем на бизнес-цели Банка;
— адекватность защитных мер, т.е. соответствующие защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз;
— эффективная реализация принятых защитных мер;
— использование опыта при принятии и реализации решений, т.е. накапливать, обобщать и использовать как свой опыт, так и опыт других банков на уровнях принятия решений и их исполнения;
— непрерывность принципов безопасного функционирования, т.е. обеспечение непрерывности реализации принципов безопасного функционирования;
— контролируемость защитных мер, т.е. применение только тех защитных мер, правильность работы которых может быть проверена, при этом регулярно оценивается адекватность защитных мер, и эффективность их реализации с учетом влияния защитных мер на бизнес-цели.

7. Объекты защиты

7.1. Объектами защиты, с точки зрения информационной безопасности в Банке, являются:
— АБС (ее ядро и подключаемые модули);
— Система обработки информации и транзакций по банковским картам;
— Система дистанционного банковского обслуживания;
— Система кадрового делопроизводства и бухгалтерской деятельности;
— Системы взаимодействия и предоставления отчетности в регулирующие и надзорные органы;
— Системы межбанковских и клиентских платежей (например, БЭСП и др.);
— Служебные системы, автоматизирующие второстепенные процессы внутреннего взаимодействия (например, корпоративная почта, СКУД и др.);
— различного рода носители защищаемой информации, в том числе информационные ресурсы, речевая информация, документы на бумажных и магнитных носителях, определенные как защищаемые нормативно-распорядительными документами Банка;
— защищаемые помещения (помещения серверной комнаты, хранения носителей резервных копий, иные, определённые внутренними документами Банка).
— другие системы, обрабатывающие защищаемую информацию.

Осуществление вышеперечисленных процессов и любых других, связанных с деятельностью Банка, характеризуется сбором, накоплением и обработкой информации, подлежащей защите. Защищаемая информация является таковой вне зависимости от способа обработки (ввод, хранение, накопление, распространение и т.д.) и ее вида (информация может быть представлена в электронном виде, на бумажном носителе, в виде аудио-видео сигналов).

7.2. Защищаемая информация делится на следующие виды:
— информация, составляющая коммерческую тайну, научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

— персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
— банковская тайна — информация об операциях, счетах и вкладах клиентов и корреспондентов Банка;
— другая информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая Приказами и распоряжениями руководства Банка.

Описание сведений, относящихся к видам защищаемой информации, утверждается отдельным перечнем, который определяет какая информация составляет банковскую, служебную, коммерческую тайну и обрабатываемые Банком персональные данные.

Информационные ресурсы относятся к защищаемой информации в соответствии с выше указанным перечнем и критичности для бизнеса, определяемой в рамках процесса управления рисками ИБ.

В связи с тем, что ИС Банка, как правило, обрабатывают совокупность сведений, содержащих различные виды защищаемой информации, требования по обеспечению ИБ внутренними документами по ИБ Банка едины для всех видов защищаемой информации и предъявляются ко всем ИС, представленным в Перечне информационных систем Банка, подлежащих защите, за исключением тех случаев, когда отдельные документы или разделы документов регламентируют особенности обеспечения ИБ для конкретного вида защищаемой информации или в конкретных ИС Банка.

8. Модели угроз и нарушителей

8.1. Угроза информационной безопасности компонентам ИС Банка, т. е. АС Банка — совокупность условий и факторов, создающих опасность несанкционированного доступа к информации, циркулирующей в автоматизированной системе, а также возможные последствия воздействий нарушителя на АС Банка, не предотвращение, не обнаружение и не ликвидация которого может привести к ухудшению заданных качественных характеристик функционирования АС Банка или нарушению ее работоспособности, а также искажению и утечке информации.

8.2. В соответствии со Стандартом БР СТО БР ИББС-1.0-2014 информационная инфраструктура АС Банка, обеспечивающая реализацию банковских технологий, может быть представлена в виде иерархии следующих основных уровней:
— физического (линии связи, аппаратные средства и пр.);
— сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
— сетевых приложений и сервисов;
— операционных систем;
— систем управления базами данных;
— банковских технологических процессов и приложений;
— бизнес-процессов организации.

Определение конкретных объектов защиты осуществляется на каждом из уровней информационной инфраструктуры.

8.3. Основными угрозами информационной безопасности автоматизированной системы, принятыми в Банке на основании Стандарта БР СТО БР ИББС-1.0-2014 являются:
— неблагоприятные события природного, техногенного и социального характера;
— террористы и криминальные элементы;
— зависимость от поставщиков / провайдеров / партнеров / клиентов;
— сбои, отказы, разрушения / повреждения программных и технических средств;
— работники Банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);

— работники Банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками Банка, но осуществляющие попытки НСД (внешние нарушители ИБ);
— несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Источники угроз на физическом, сетевом уровне и уровне сетевых приложений:
— внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры и иные лица, осуществляющие несанкционированный доступ (НСД);
— внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы сетевых приложений и т.п.);
— комбинированные источники угроз: внешние и внутренние, действующие совместно и (или) согласованно;
— сбои, отказы, разрушения / повреждения программных и технических средств.

8.4. Источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:
— внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.);
— комбинированные источники угроз: внешние и внутренние, действующие в сговоре.

8.5. Источники угроз на уровне бизнес-процессов:
— внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы ИС, представители менеджмента организации и пр.);
— комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

8.6. Угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью, определяются в Плане действий, направленных на обеспечение непрерывности деятельности и (или) восстановления деятельности Банка.

8.7. В соответствии с требованиями к обеспечению информационной безопасности автоматизированной системы Банка определены следующие модели угроз:
— преднамеренные программно-технические воздействия с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения в АС Банка;
— нарушения санкционированной доступности информации в АС Банка, за счет нарушения работоспособности программного обеспечения, коммуникационного оборудования и маршрутизаторов АС Банка или их перепрограммирования (дефекты, сбои, аварии и отказы аппаратно-программных комплексов);
— утечка и искажение конфиденциальной информации за счет несанкционированного доступа к ней через технические средства АС Банка, утечка конфиденциальной информации по техническим каналам;
— разглашение конфиденциальной информации и неправомерные действия со стороны лиц, имеющих право доступа к конфиденциальной информации и реализующих угрозы в рамках своих полномочий и за их пределами.

8.8. Основными критическими элементами средств автоматизации АС Банка (в порядке убывания их важности) являются:
— сервера баз данных и приложений;
— коммуникационное оборудование (компоненты) системы передачи данных (маршрутизаторы, концентраторы, модемы);
— специализированные АРМ с установленными СКЗИ;
— рабочие станции пользователей Банка.

8.9. Объектами защиты средств автоматизации являются:
- программно-технический комплекс АС Банка в целом как автоматизированная система, обрабатывающая конфиденциальную информацию;
- сервера баз данных и приложений;
- специализированные АРМ с установленными СКЗИ;
- рабочие станции конечных пользователей АС Банка;
- каналы связи, посредством которых осуществляется информационный обмен в АС Банка;
- помещения, в которых располагается серверная часть программно-технических комплексов и рабочие станции конечных пользователей (в зависимости от обрабатываемой информации).

8.10. Система информационной безопасности АС Банка строится в соответствии с определенным характером угроз и основных элементов системы, на которые эти угрозы распространяются, а также с учетом требований Стандарта БР СТО БР ИББС-1.0-2014 по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

9. Общие требования по СИБ Банка

9.1. Общие требования по системе информационной безопасности Банка формулируются для следующих областей:
- назначение и распределение ролей, доверия к персоналу;
- стадий жизненного цикла ИС;
- защиты от НСД, управления доступом и регистрацией в ИС;
- антивирусной защиты;
- использования ресурсов Интернет;
- использования средств криптографической защиты информации;
- защиты банковских платежных и информационных технологических процессов;
- защита от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи;
- обеспечение безопасности ПДн при обработке в ИСПДн;
- обеспечение работоспособности безопасного функционирования технических средств и информационных ресурсов Банка;
- обеспечение информационной безопасности ТУ ДБО;
- требования к повышению осведомленности Клиентов в области обеспечения защиты информации;
- обеспечение информационной безопасности Мобильного банкинга;
- обеспечение информационной безопасности среды виртуализации.

9.2. ОИБ определяет и контролирует достаточность предъявляемых в Банке требований к СИБ Банка.

9.3. На основании определенных настоящей Политикой принципов и с целью обеспечения требований к СИБ Банка в документах Банка по обеспечению ИБ второго уровня описана детализация применяемых подходов и методов реализации и эксплуатации СИБ.

10. Управление ИБ

10.1. С целью реализации, эксплуатации, контроля и поддержания на приемлемом уровне СОИБ в Банке создан ОИБ, а также реализован ряд управляющих процессов планирования, реализации, совершенствования и проверки.

Настоящая Политика сформирована с учетом необходимости цикличной реализации указанных процессов с целью планомерного совершенствования системы ИБ Банка.

10.2. Банк выбирает защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз.

Для успешного функционирования СМИБ в Банке необходимо выполнять следующие группы требований:
— требования к организации и функционированию ОИБ и обеспечения деятельности Банка;
— требования к определению / коррекции области действия СОИБ;
— требования к выбору / коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ;
— требования к разработке планов обработки рисков нарушения ИБ;
— требования проведению классификации информационных активов;
— требования к разработке / изменению внутренних документов Банка, регламентирующих деятельность в области обеспечения ИБ;
— требования к принятию решений о реализации и эксплуатации СОИБ;
— требования к организации реализации планов обработки рисков нарушения ИБ;
— требования к разработке и организации реализации программ по обучению и повышению осведомленности в области ИБ;
— требования к организации обнаружения и реагирования на инциденты ИБ;
— требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний;
— требования к мониторингу и контролю защитных мер в области ИБ;
— требования к проведению самооценки ИБ;
— требования к проведению аудита ИБ;
— требования к анализу СОИБ и функционирования СОИБ;
— требования к принятию решений по тактическим улучшениям СОИБ;
— требования к принятию решений по стратегическим улучшениям СОИБ.

Детализация применяемых подходов и методов для выполнения перечисленных требований отражена в настоящей Политике и иных документах Банка по информационной безопасности.

10.3. ОИБ имеет утвержденные руководством функции, полномочия и ресурсы, необходимые для выполнения установленных целей и задач и подчиняется непосредственно Председателю Правления Банка. Указанные функции, полномочия и ресурсы детализированы в иных документах Банка по ИБ.

10.4. В рамках обеспечения информационной безопасности ряд структурных подразделений и должностных лиц Банка выполняют иные функции, закрепленные во внутренних документах Банка.

В Банке установлены правила на случай возникновения нештатной ситуации (нарушения политики ИБ или возникновения инцидента ИБ). Реагирование на нештатные ситуации, решения, принятые на основании проведенных расследований, являются неотъемлемой частью СМИБ и регламентируются соответствующими внутренними нормативными документами.

10.5. Контроль за актуализацией внутренних документов, регламентирующих деятельность в области обеспечения ИБ, а также своевременную разработку / актуализацию внутренних документов, регламентирующих деятельность в области обеспечения ИБ реализуется на базе системы документационного обеспечения Банка, одновременно определяется иерархия внутренних документов:
— Политика ИБ Банка, утвержденная уполномоченным органом;
— в рамках Политики — частные Политики (положения);
— в рамках частных Политик — документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ в Банке.

10.6. Разработка / актуализация внутренних документов, регламентирующих деятельность в области обеспечения ИБ, проводится в Банке ОИБ на основе:
— ГОСТ Р 57580.1-2017;
— Стандарта БР СТО БР ИББС-1.0-2014;
— законодательства Российской Федерации в области обеспечения ИБ;
— нормативных актов Банка России;
— внутренних документов Банка.

Внутренние документы по обеспечению ИБ являются целой и неделимой системой документирования в Банке и охватывают все области обеспечения ИБ.

Для внутренних документов по обеспечению ИБ обеспечено их удовлетворение следующим требованиям:
— обязательность для выполнения;
— выполнимость и контролируемость;
— адекватность требованиям и условиям ведения деятельности и функционирования бизнес-процессов Банка;
— соответствие внутренним документам Банка.

В состав внутренней документации Банка по обеспечению ИБ включены следующие виды документов:
— документы первого уровня — Политика информационной безопасности, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ Банка;
— документы второго уровня — частные политики, детализирующие положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка;
— документы третьего уровня - содержат положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) обеспечения ИБ, содержат правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с ИБ, в рамках технологических процессов, используемых в Банке, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, регламенты, порядки, инструкции);
— документы четвертого уровня - содержат свидетельства выполненной деятельности по обеспечению ИБ, отражают достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ Банка

Документы всех четырех уровней являются целой и неделимой системой документирования в Банке и охватывают все области обеспечения ИБ. Документы нижнего уровня, регламентирующие ИБ в Банке, разрабатываются в рамках требований документов высшего уровня, стандартов Банка России.

11. Ресурсное обеспечение ИБ

11.1. Под ресурсным обеспечением ИБ понимается процесс управления, обеспечивающий определение потребностей в ресурсах ИБ и контроль эффективности использования ресурсов ИБ.

11.2. Основными целями реализации ресурсного обеспечения ИБ являются:
— обеспечение процессов системы ИБ финансовыми средствами;
— обеспечение Банка кадровыми ресурсами, необходимыми и достаточными для реализации процессов СОИБ;
— контроль эффективности использования ресурсов ИБ.

11.3. Потребности в обеспечении процессов системы ИБ ресурсами ИБ определяются на основе предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) в случае реализации актуальных рисков нарушения ИБ.

11.4. Банком обеспечивается надлежащий баланс между актуальными рисками ИБ, связанными с наличием уязвимостей в выполнении процессов СОИБ, и ресурсами ИБ, используемыми для обеспечения целевого уровня защиты информации и, соответственно, направленными на снижение указанных рисков.

11.5. Для реализации ресурсного обеспечения ИБ:
— устанавливается оценка уровня зрелости, выполнения процессов СОИБ;

— устанавливается оценка рисков ИБ с учетом данных о реализованном уровня зрелости, выполнения процессов СОИБ;
— обеспечивается целевой уровень защиты информации путем повышения уровня зрелости выполнения процессов СОИБ до значения, реализующего снижение рисков ИБ до допустимого уровня.
  Повышение уровня зрелости выполнения процессов СОИБ достигается путем:
  — инвестирования необходимых финансовых средств в обеспечение процессов СОИБ. При этом инвестирование не предполагает получение дохода от выполнения процессов СОИБ, а приводит к снижению предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) в случае реализации актуальных рисков ИБ;
  — обеспечения необходимых и достаточных кадровых ресурсов;
— проводится контроль эффективности инвестирования в обеспечение процессов СОИБ путем установления и мониторинга целевых (контрольных) показателей, выраженных в количественной (денежной) форме.

11.6. Определение потребности Банка в кадровых ресурсах заключается в установлении необходимого и достаточного количества, а также требуемой компетенции сотрудников, ответственных за обеспечение ИБ, выполняемой на основе:
— анализа задач и функций, возложенных на указанных сотрудников;
— уровня автоматизации процессов СОИБ и централизации управления средствами автоматизации;
— прогноза возможного расширения состава задач и функций указанных сотрудников в соответствии с планами совершенствования процессов СОИБ вследствие развития бизнес-процессов, совершенствования процессов информатизации, развития Банка.

11.6.1. При планировании (совершенствовании) процессов СОИБ необходимо обеспечить выделение ресурсов ИБ для эффективной реализации требований законодательства Российской Федерации, нормативных актов Банка России, требований к обеспечению ИБ, установленных Банком.

11.6.2. Банку необходимо установить состав задач и функций сотрудников, ответственных за обеспечение ИБ, для каждого уровня полноты и качества выполнения процессов СОИБ, оценив при этом трудозатраты на их выполнение.

11.6.3. Банком определяется минимальная необходимая и достаточная численность сотрудников, ответственных за обеспечение ИБ, исходя из следующих показателей:
— трудозатраты на выполнение задачи и функций обеспечения ИБ;
— количество реализуемых процессов СОИБ;
— масштаб выполнения управляемых процессов СОИБ, в том числе:
  — количество подразделений Банка;
  — количество автоматизированных банковских систем;
  — количество сотрудников Банка;
  — расположение подразделений Банка.

11.6.4. Сотрудники Банка, ответственные за обеспечение ИБ, должны обладать компетенцией, необходимой для выполнения их функциональных обязанностей. Определение компетенции сводится к установлению требований в отношении знаний, практических навыков и опыта работы в соответствующей области указанных сотрудников. К основным требованиям, определяющим необходимую компетенцию указанных сотрудников, следует среди прочего относить:
— наличие высшего профессионального образования в области ИБ и (или) информационных технологий;
— опыт работы в области ИБ не менее двух лет;
— регулярное прохождение дополнительного (специализированного) обучения (повышения квалификации) в области ИБ;

— знание требований законодательства Российской Федерации, в том числе нормативных актов Банка России, необходимых для надлежащего выполнения функций, возложенных на указанных сотрудников;
— знание внутренних нормативно-методических и организационно-распорядительных документов в области ИБ;
— осведомленность по вопросам, касающимся средств, систем и технологий обеспечения ИБ, а также способов и практик их применения.

11.7. Достижение надлежащего баланса между величинами рисков ИБ, связанных с наличием уязвимостей при выполнении процессов СОИБ и ресурсным обеспечением ИБ, направленным на снижение указанных рисков путем обеспечения необходимого и достаточного уровня зрелости выполнения процессов СОИБ, обеспечивается путем определения и анализа целевых (контрольных) показателей эффективности использования финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов СОИБ.

11.7.1. Показатели эффективности делятся на две группы:
— показатели, подлежащие анализу на этапе планирования инвестирования в повышение уровня зрелости выполнения процессов СОИБ;
— показатели, подлежащие анализу на этапе оценки результатов инвестирования в уровень зрелости выполнения процессов СОИБ.

11.7.2. В качестве основных показателей эффективности инвестирования в выполнение процессов СОИБ на этапе планирования рассматриваются:
— ожидаемые результаты от снижения уровня рисков ИБ, связанных с повышением уровня зрелости выполнения процессов СОИБ;
— срок получения ожидаемых результатов по повышению уровня зрелости выполнения процессов СОИБ;
— согласованность со стратегией информационного развития Банка.

11.7.3. Указанные показатели эффективности оцениваются экспертным путем с привлечением профильных подразделений Банка и включаются в оценку финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов СОИБ.

11.7.4. В качестве основного показателя эффективности инвестирования финансовых средств в повышение уровня зрелости выполнения процессов СОИБ на этапе оценки результатов инвестирования рассматривается соотношение фактического ущерба (финансового эквивалента понесенных потерь) от инцидентов ИБ, в том числе непосредственных финансовых потерь от инцидентов ИБ, финансовых потерь от нарушения непрерывности деятельности Банка, финансовых потерь от негативного влияния инцидентов ИБ на деловую репутацию, финансовые средства, затраченные для ликвидации последствий инцидентов ИБ, по отношению к предполагаемой на этапе планирования величине возможного ущерба (финансового эквивалента возможных потерь).

11.7.5. При превышении фактических финансовых потерь от инцидентов ИБ значений, предполагаемых на этапе планирования, определяются основные факторы возникновения рисковых событий, приводящих к ущербу (финансовым потерям) и вырабатываются планы, элементами которых могут являться:
— пересмотр модели угроз и нарушителя, применяемых требований к обеспечению ИБ;
— установление новых процессов СОИБ, в том числе связанных с изменениями состава актуальных угроз;
— повышение уровня зрелости выполнения установленных процессов СОИБ.

11.7.6. В качестве дополнительного показателя эффективности инвестирования в повышение уровня зрелости выполнения процессов СОИБ на этапе оценки результатов инвестирования рассматривается соответствие фактических сроков

реализации планов по повышению уровня зрелости выполнения процессов СОИБ планируемым срокам.

11.7.7. Банком выполняются с установленной периодичностью:
- анализ эффективности выполнения процессов СОИБ, в том числе выполняемый на основе показателей, установленных в пункте 11.7.1. настоящего раздела;
- анализ рисков ИБ с целью определения приоритетных направлений совершенствования процессов СОИБ.

12. Управление рисками ИБ

12.1. В целях управления риском ИБ на ОИБ возлагается выполнение следующих функций:
- идентификация риска ИБ;
- сбор и регистрация информации о событиях риска ИБ и потерях от его реализации;
- мониторинг риска ИБ;
- ведение Базы событий;
- повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ;
- оценка эффективности управления риском ИБ;
- осуществление мониторинга сигнальных и контрольных значений контрольных показателей уровня риска ИБ;
- составление отчетов по событиям риска ИБ и направление их в Службу управления рисками и Правлению Банка;
- участие в разработке внутренних документов в области управления риском ИБ;
- информирование работников Банка по вопросам, связанным с управлением риском ИБ;
- обмен информацией о событиях риска ИБ;
- осуществление других функций, связанных с управлением риском ИБ, предусмотренных внутренними документами Банка.

12.2. Идентификация риска ИБ, может осуществляться следующими способами:
- анализ Базы событий;
- проведение ОИБ ежегодной самооценки уровня риска ИБ и форм (способов) контроля, направленных на снижение его уровня;
- анализ динамики количественных показателей, направленных на измерение и контроль уровня риска ИБ в определенный момент времени;
- интервью с работниками Банка, в том числе с руководством Банка, в рамках которых работниками и руководством Банка обсуждаются риски ИБ;
- анализ актов проверок, судебных актов (решений, определений, постановлений) и (или) актов исполнительных органов государственной власти, Банка России в части фактов, относящихся к реализации риска ИБ;
- анализ информации внутреннего и внешнего аудита;
- анализ информации работников Банка, полученной в рамках инициативного информирования работниками Банка Службы управления рисками и (или) Службы внутреннего аудита;
- анализ других внешних и внутренних источников информации и способов выявления рисков ИБ.

12.3. Выявление событий риска ИБ заключается в обнаружении событий ИБ и инцидентов ИБ, в результате оценки последствий от которых было выявлено негативное влияние на Банк.

12.3.1. Основными источниками событий ИБ являются:
- технические и программные средства мониторинга ИБ и контроля эксплуатации применяемых защитных мер;
- работники Банка, выявляющие события ИБ;
- клиенты и партнеры Банка.

12.3.2. Для своевременного обнаружения событий риска ИБ, работники ОИБ проводят регулярный мониторинг следующего специального программного обеспечения:
— средств защиты от воздействия вредоносного кода;
— системы предотвращения утечек конфиденциальной информации;
— сетевого сканера безопасности; и т.д.

12.3.3. В качестве дополнительных источников информации о событиях ИБ, формируемых техническими и программными средствами, могут быть использованы:
— системные журналы операционных систем;
— системные журналы систем управления базами данных;
— регистрационные журналы прикладного программного обеспечения;
— регистрационные журналы активного сетевого оборудования;
— регистрационные журналы применяемых средств защиты информации, в том числе средств защиты информации от несанкционированного доступа, регистрационные журналы специализированных программно-технических средств обнаружения вторжений и сетевых атак, программного обеспечения проверки целостности файлов;
— информация специализированных устройств контроля физического доступа, в том числе телевизионных систем охранного наблюдения, систем контроля и управления доступом и охранной сигнализации.

12.3.4. Порядок обработки событий риска ИБ, выявленных в Банке определен в документе GBR.182 Регламент управления инцидентами информационной безопасности Общества с ограниченной ответственностью «Бланк банк».

12.4. Мониторинг риска ИБ.

12.4.1. Мониторинг риска ИБ может осуществляться следующими способами:
— установление и мониторинг КИР;
— анализ статистики событий риска ИБ, в том числе причин возникновения событий риска ИБ и потерь от их реализации;
— контроль выполнения мероприятий, направленных на повышение качества системы управления риском ИБ и уменьшение негативного влияния риска ИБ, включая мероприятия, направленные на предотвращение (снижение вероятности) событий риска ИБ, и мероприятия, направленные на ограничение размера потерь от реализации событий риска ИБ;
— контроль выполнения мер, направленных на уменьшение негативного влияния риска ИБ;
— контроль соблюдения выбранных способов реагирования на риски ИБ;
— мониторинг потоков информации в рамках реализации риска ИБ, поступающей от подразделений Банка и центров компетенций, Правления и Руководства Банка, из других источников информации.

12.4.2. Установление и мониторинг КИР.

В целях контроля за уровнем риска Банк определяет на плановый годовой период контрольные показатели КИР, а также устанавливает целевые значения этих показателей:

Сигнальное значение — значение показателя, при нарушении которого проводится ежедневный мониторинг значений показателя КИР и реализация мер, направленных на устранение превышения фактического значения данного показателя над предельно допустимым значением показателя;

Контрольное значение — предельно допустимое значение показателя КИР, при нарушении которого информация доводится до Руководства Банка и реализуется комплекс мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска на деятельность Банка.

Ключевые индикаторы риска	Периодичность	Сигнальное значение	Контрольное значение
Количество уведомлений от клиентов об использовании электронных средств платежа без их согласия (в том числе в результате побуждения клиентов к совершению операции путем обмана или злоупотребления доверием)	в постоянном режиме	1	3
Количество событий, связанных с осуществлением перевода денежных средств Банка или его клиентов без их согласия в результате несанкционированного доступа работников Банка или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к АБС Банка.	в постоянном режиме	1	2
Количество событий, связанных с осуществлением перевода денежных средств Банка или его клиентов без их согласия в результате реализации компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к АБС Банка.	в постоянном режиме	1	2
Количество событий, связанных с осуществлением перевода денежных средств Банка или его клиентов без их согласия в результате несанкционированного доступа Банка или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к программно-аппаратному обеспечению банкоматов, электронных терминалов.	в постоянном режиме	1	2
Количество событий, связанных с осуществлением перевода денежных средств Банка или его клиентов без их согласия в результате реализации компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к программно-аппаратному обеспечению банкоматов, электронных терминалов.	в постоянном режиме	1	2
Количество событий, связанных с осуществлением несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах в результате несанкционированного доступа работников Банка или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к программно-аппаратному обеспечению банкоматов	в постоянном режиме	1	2

Продолжение таблицы

Ключевые индикаторы риска	Периодичность	Сигнальное значение	Контрольное значение
Количество событий, связанных с осуществлением несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах в результате реализации компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры Банка, к программно-аппаратному обеспечению банкоматов	в постоянном режиме	1	2
Количество событий, связанных с неоказанием услуг по переводу денежных средств на период более двух часов в целом по всем субъектам Российской Федерации в результате реализации компьютерных атак работниками Банка или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество событий, связанных с неоказанием услуг по переводу денежных средств на период более двух часов в целом по всем субъектам Российской Федерации в результате реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество событий, связанных с неоказанием услуг по переводу денежных средств на период более двух часов в целом по отдельным субъектам Российской Федерации, в результате реализации компьютерных атак работниками Банка или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество событий, связанных с неоказанием услуг по переводу денежных средств на период более двух часов в целом по отдельным субъектам Российской Федерации в результате реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество случаев связанных с нарушениями правил предоставления отчетности в Банк России и/или Федеральные органы исполнительной власти в результате реализации компьютерных атак работниками Банка или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2

Продолжение таблицы

Ключевые индикаторы риска	Периодичность	Сигнальное значение	Контрольное значение
Количество случаев связанных с нарушениями правил предоставления отчетности в Банк России и/или Федеральные органы исполнительной власти в результате реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество случаев связанных с предоставлением недостоверной отчетности в Банк России и/или Федеральные органы исполнительной власти в результате реализации компьютерных атак работниками Банка или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество случаев связанных с предоставлением недостоверной отчетности в Банк России и/или Федеральные органы исполнительной власти в результате реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество случаев связанных с утечкой персональных данных клиентов Банка и работников Банка в результате реализации компьютерных атак работниками Банка или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2
Количество случаев связанных с утечкой персональных данных клиентов Банка и работников Банка в результате реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры Банка.	в постоянном режиме	1	2

Не реже одного раза в год работники ОИБ осуществляют оценку в целях пересмотра КИР для обеспечения поддержания КИР в актуальном состоянии. Результаты оценки согласуются с руководителем Службы управления рисками.

13. Планирование бесперебойной работы

13.1. Для бесперебойной работы АС Банка и возможности восстановления ее функционирования после аварийных ситуаций, обеспечивается:
— сохранность архивов базы данных и системных журналов;
— наличие актуальных планов обеспечения непрерывности бизнеса.

13.2. Комплекс программно-аппаратных средств системы АС Банка поддерживает функции ежедневного резервного копирования данных. Максимально допустимый объем потери данных при авариях и сбоях не должен превышать дневного объема изменений данных.

13.3. Для обеспечения бесперебойного функционирования АС Банка предусмотрено резервирование систем обработки и хранения данных, а также возможность сбора данных аудита о трафике в сети и его анализа.

13.4. Резервное копирование систем осуществляется ежедневно после рабочего дня.

13.5. Процедуры перехода на аварийный режим работы необходимо тестировать ежегодно.

13.6. Электронные носители информации с архивами баз данных хранятся в соответствии с внутренним порядком Банка. Хранение архивов баз данных осуществляется в защищаемых помещениях, удаленных от мест расположения серверов АС Банка.

14. Аудит и мониторинг ИБ

14.1. Порядок и периодичность проведения аудита ИБ Банка в целом (или отдельных структурных подразделений) может определяться Председателем Правления Банка либо иным органом управления Банка с учетом требований законодательства.

14.2. Внешний аудит ИБ проводится путем оценки соответствия защиты информации с ГОСТ Р 57580.2-2018 не реже одного раза в два года с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

14.3. ОИБ имеет право самостоятельно проводит самооценку соответствия ИБ Банка требованиям Стандарта БР СТО БР ИББС-1.0-2014. По результатам оценки принимаются меры по улучшению показателей ИБ Банка.

14.4. При проведении аудита ИБ Банк обеспечивается документальным и, если это необходимо, техническим подтверждением (отчетом) того, что:
— политика ИБ отражает требования бизнеса и цели Банка;
— организационная структура управления ИБ создана;
— процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям;
— защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
— остаточные риски оценены и остаются приемлемыми для Банка;
— система управления ИБ соответствует определенному уровню зрелости управления ИБ;
— рекомендации предшествующих аудитов ИБ реализованы.

14.5. Результаты проверок хранятся в Банке в соответствии с утвержденной Номенклатурой дел Банка. Доступ к результатам проверок разрешается только Председателю Правления Банка, руководителю ЦСИС, руководителю ОИБ, руководителю СВК, руководителю СВА, а также иным лицам, уполномоченным Председателем Правления Банка.

15. Порядок пересмотра Политики

15.1. Настоящая Политика вступает в силу с момента ее утверждения уполномоченным органом и действует бессрочно до замены ее новой Политикой информационной безопасности.

15.2. Требования настоящей Политики могут развиваться другими внутренними нормативными документами Банка, которые детализируют, дополняют и уточняют ее.

15.3. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Банка настоящая Политика применяется в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Банка. В этом случае Отдел информационной безопасности обязан инициировать внесение соответствующих изменений.

15.4. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:
- пересмотр настоящей Политики необходимо осуществлять не реже одного раза в 12 месяцев;
- внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения аудитов ИБ и других контрольных мероприятий.

15.5. Ответственным за внесение изменений в настоящую Политику является руководитель ОИБ Банка.

16. Ответственность за нарушение Политики информационной безопасности

16.1. Общее обеспечение ИБ Банка осуществляет Председатель Правления Банка.

16.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СМИБ Банка лежит на руководителе ОИБ.

16.3. Нарушение требований локальных нормативных актов Банка по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между Банком и сотрудниками и договорами, заключенными между Банком и контрагентами.

16.4. Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется, исходя из размера ущерба, причиненного Банку.

16.5. Руководители структурных подразделений Банка несут персональную ответственность за обеспечение соблюдений требований к ИБ в возглавляемых ими подразделениях.

16.6. Каждый сотрудник Банка несет персональную ответственность за обеспечение соблюдений требований к ИБ на своем рабочем месте.

16.7. Сторонние организации, нарушившие требования ИБ Банка, несут ответственность в соответствии с установленными гражданско-правовыми нормами Российской Федерации.

16.8. Виды ответственности, предусмотренные отдельными федеральными законами об обращении с информацией ограниченного доступа:
- Гражданско-правовая ответственность (1301 ГК РФ Ответственность за нарушение исключительного права на произведение).
- Уголовная ответственность: Статья 137. Нарушение неприкосновенности частной жизни; Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений; Статья 159.6. Мошенничество в сфере компьютерной информации; Статья 272. Неправомерный доступ к компьютерной информации; Статья 273. Создание, использование и распространение вредоносных компьютерных программ; Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
- Административная ответственность: Статья 13.11. Нарушение установленного законом «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных); Статья 13.13 Незаконная деятельность в области защиты информации; Статья 13.12. Нарушение правил защиты информации; Статья 13.14. Разглашение информации с ограниченным доступом; Статья 5.39. Отказ в предоставлении гражданину информации.