УТВЕРЖДЕН
Правлением АО «РЕАЛИСТ БАНК»
Протокол № 6076 от 20.12.2024 г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «РЕАЛИСТ БАНК»

МОСКВА
2024

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности АО «РЕАЛИСТ БАНК» (далее – Политика) определяет высокоуровневые цели и задачи обеспечения информационной безопасности Банка, включая способы контроля реализации требований политики информационной безопасности, а также определяет содержание, назначение и требования к деятельности Банка по обеспечению информационной безопасности.

1.2. Настоящая Политика устанавливает принципы построения системы управления информационной безопасностью АО «РЕАЛИСТ БАНК» (далее – Банк) на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.

1.3. Требования информационной безопасности предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.4. Настоящая Политика разработана в соответствии с:

– Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», введенным в действие Распоряжением Банка России от 17.05.2014 № Р-399;

– Стандартом 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», введенным в действие Распоряжением Банка России от 28.04.2007 № Р-348;

– Национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», введенным в действие Приказом Росстандарта от 08.08.2017 № 822-ст;

– Национальным стандартом Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения», введенным в действие Приказом Росстандарта от 22.12.2022 № 1548-ст;

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности»;

– Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Положением Банка России от 17.08.2023 № 821-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»;

– Положением Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России»;

– Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»;

– Положением Банка России от 17.04.2019 г. № 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»;

– другими нормативными и правовыми актами.

1.5. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна для применения всеми работниками и руководством Банка, а также пользователями его информационных ресурсов.

1.6. Требования настоящей Политики могут развиваться другими внутренними нормативными документами Банка, которые дополняют и уточняют её.

1.7. В случае изменения действующего законодательства и иных нормативны актов Российской Федерации настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Служба информационной безопасности инициирует внесение соответствующих изменений.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационный актив (ИА) – информация (в электронном виде на материальных носителях) с реквизитами, позволяющими ее идентифицировать и имеющая ценность для достижения поставленных перед Банком или его подразделениями целей. Основными характеристиками информационных активов, рассматриваемых в рамках обеспечения информационной безопасности, являются конфиденциальность, целостность и доступность.

Информационная безопасность (ИБ) – состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.
Безопасность информации определяется отсутствием недопустимого риска, связанного с несанкционированными и непреднамеренными воздействиями на информацию и (или) на другие ресурсы информационной системы, используемые в Банке.

Информационная система – совокупность программно-аппаратных комплексов Банка, применяемых для обеспечения бизнес-процессов Банка.

Инцидент информационной безопасности – событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности, результатом которой являются:

– нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности Банка;

– нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних нормативных документов Банка в области обеспечения информационной безопасности, нарушение или возможное нарушение в выполнении процессов системы обеспечения информационной безопасности Банка;

– нарушение или возможное нарушение в выполнении банковских технологических процессов Банка.

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

Куратор ИБ – заместитель Председателя Правления Банка, курирующий вопросы информационной безопасности Банка. Приказом Председателя Правления Банка наделяется полномочиями по координации и контролю работы Службы информационной безопасности.

Модель угроз – описание актуальных для Банка источников угроз информационной безопасности; методов реализации угроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

Модель нарушителя – описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз информационной безопасности со стороны указанных нарушителей.

Пользователь информационной системы – физическое лицо, обладающее возможностью доступа к информационной системе Банка.

Угроза информационной безопасности – угроза нарушения свойств информационной безопасности: доступности, целостности или конфиденциальности информационных активов Банка.

3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

3.1. Основными объектами защиты системы информационной безопасности в Банке являются информационные ресурсы, содержащие:

- коммерческую тайну;
- банковскую тайну;
- персональные данные физических лиц (работников и клиентов);
- сведения ограниченного доступа;
- открыто распространяемую информацию, необходимую для работы Банка, независимо от формы и вида ее представления.

3.2. Особые объекты защиты, имеющие высокую важность для Банка:

- банковский платежный технологический процесс;
- банковский информационный технологический процесс;
- платежная информация;
- информация, отнесенная к защищаемой в соответствии с Положением Банка России от 17.08.2023 № 821-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»;
- информация в платежной системе Банка России, отнесенная к защищаемой в соответствии с Положением Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России»;
- иная значимая для Банка информация, разглашение или модификация которой может привести к негативным последствиям для Банка;
- носители защищаемой информации, в т. ч. информационные ресурсы, речевая информация, документы на физических носителях информации, определенные как защищаемые нормативно-распорядительными документами Банка.

4. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Целью деятельности по обеспечению информационной безопасности Банка является защита информационных активов Банка, снижение уровня угроз информационной безопасности до приемлемого для Банка значения.

4.2. Основные задачи деятельности по обеспечению информационной безопасности Банка:

- организация выполнения требований законодательства Российской Федерации, нормативных актов Банка России и иных государственных органов в области информационной безопасности, внутренних нормативных документов Банка по обеспечению информационной безопасности, в том числе по защите персональных данных, включая контроль реализации данных требований;
- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- исключение либо минимизация выявленных угроз;
- повышение уровня информационной безопасности Банка;
- разработка и поддержание в актуальном состоянии нормативных документов Банка в области информационной безопасности;

- предотвращение инцидентов информационной безопасности и минимизация возможного ущерба от инцидентов;
- внедрение, поддержка и при необходимости восстановление систем защиты информации;
- участие в расследованиях инцидентов информационной безопасности;
- участие и осуществление контроля выполнения требований информационной безопасности в ИТ-проектах Банка;
- согласование и контроль предоставления доступа к информационным активам Банка.

4.3. При обеспечении информационной безопасности Банк руководствуется следующими принципами:

- **системность** – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности;
- **комплексность** – согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;
- **непрерывность защиты** – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем;
- **своевременность** – упреждающий характер мер обеспечения безопасности информации;
- **преемственность и непрерывность совершенствования** - постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и их систем защиты;
- **разумная достаточность** – соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения;
- **персональная ответственность** – возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий;
- **разделение функций** – отсутствие полномочий, позволяющих работнику Банка единолично осуществлять выполнение критичных банковских операций;
- **минимизация полномочий** – предоставление пользователям минимально возможных прав доступа в соответствии с должностными обязанностями, либо в соответствии с условиями договора, соглашения;
- **гибкость системы защиты** – возможность варьирования уровнем защищенности. Это свойство является важным для случаев, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования;
- **эффективность применения средств защиты** – затраты на внедрение и эксплуатацию механизмов защиты соизмеримы с возможным ущербом;
- **специализация и профессионализм** – привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области;
- **контроль** – обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе проверок и экспертиз используемых систем и средств защиты информации, бизнес-процессов и деятельности работников Банка.

5. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Источники угроз, уязвимости, используемые угрозами, методы и объекты атак, пригодные для реализации угрозы, а также описание потенциальных нарушителей определяются внутренним нормативным документом Банка, регламентирующим построение моделей угроз и потенциального нарушителя информационных ресурсов.

5.2. Модель угроз содержит систематизированный перечень категорий защищаемой информации, источников актуальных угроз ИБ, уровней реализации угроз и объектов среды ИА, а также свойств ИБ, на которые направлена угроза.

5.3. Модель нарушителя содержит типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации, цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации, и возможные способы реализации угроз безопасности информации.

6. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Уязвимость ИБ создает предпосылки к реализации угрозы через нее (инцидентам ИБ). Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) Банка в информационной сфере, в результате чего Банку может быть нанесен ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

6.2. Риски нарушения информационной безопасности являются неотъемлемой частью операционных рисков и определяются на основании качественных оценок:

− степени возможности реализации угроз безопасности информации выявленными и (или) предполагаемыми источниками угроз безопасности информации в результате их воздействия на информационные активы Банка;

− степени тяжести последствий от потери свойств информационной безопасности для рассматриваемых типов информационных активов.

6.3. Оценка рисков ИБ на уровне бизнес-процессов Банка осуществляется с соблюдением общего подхода к оценке операционных рисков, определенного «Политикой управления операционным риском в АО «РЕАЛИСТ БАНК», с учетом особенностей риска ИБ.

6.4. Анализ и оценка рисков ИБ основывается на:

− идентификации автоматизированных систем Банка;

− идентификации информационных активов Банка;

− ценности информационных активов для целей и задач Банка;

− моделях угроз и нарушителей ИБ Банка.

6.5. Цели обработки рисков ИБ:

− добиться значительного уменьшения рисков ИБ при относительно низких затратах;

− поддерживать принятые риски ИБ на допустимом, низком уровне.

6.6. Управление рисками ИБ предполагает решение следующих задач:

− построение модели взаимодействия бизнес-процессов Банка и информационных систем с целью выделения наиболее критичных ИА Банка;

− построение модели нарушителя ИБ и модели угроз ИБ;

− оценка рисков реализации угроз ИБ, направленных на критичные ИА Банка;

− выявление мер по снижению рисков угроз ИБ;

− разработка плана по снижению рисков ИБ;

− оценка остаточного уровня риска ИБ после внедрения мер по его снижению.

6.7. В целях эффективности управления риском ИБ в Банке осуществляются следующие мероприятия:

– обеспечение выполнения порядка функционирования системы информационной безопасности, определенного внутренними нормативными документами Банка, с учетом требований Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее

– Положение № 716-П) (идентификации, сбора и регистрации информации о событиях риска ИБ и потерях, мониторинга риска ИБ);

– распределение функций и ответственности Правления Банка (коллегиального исполнительного органа) и работников Банка в части решения вопросов, связанных с управлением риском реализации информационных угроз, обеспечением операционной надежности и защиты информации, в том числе исключающее конфликт интересов;

– определение основных принципов функционирования системы обеспечения информационной безопасности и задачи управления риском ИБ;

– определение и поддержание допустимого уровня риска ИБ, разработка мероприятий, направленных на уменьшение негативного влияния риска ИБ.

6.8. К компетенции Правления Банка относятся следующие вопросы:

– обеспечение принятия внутренних нормативных документов, определяющих правила и процедуры управления риском ИБ;

– распределение полномочий и ответственности по управлению риском ИБ между руководителями подразделений, установление порядка взаимодействия и представления отчетности;

– определение потребности Банка в ресурсах для обеспечения информационной безопасности Банка и организация ресурсного (кадрового и финансового) обеспечения процессов системы управления риском ИБ;

– определение комплекса мероприятий, направленных на повышение качества системы управления риском ИБ и уменьшение негативного влияния риска ИБ;

– осуществление контроля за реализацией политики управления риском ИБ и соблюдения установленных значений сигнальных и контрольных значений контрольных показателей уровня риска ИБ.

6.9. В Банке в целях управления риском ИБ определено специализированное подразделение – Служба информационной безопасности с прямым подчинением Заместителю Председателя Правления Банка (Куратора ИБ), ответственному за обеспечение информационной безопасности и не участвующего в обеспечении функционирования информационных систем Банка.

6.10. На Службу информационной безопасности с учетом требований Положения № 716-П возложено выполнение следующих функций:

− соблюдение процедур управления риском ИБ в части идентификации, сбора и регистрации информации о событиях риска ИБ и потерях, мониторинга риска ИБ;

− ведение базы событий риска ИБ;

− участие в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ;

− составление на регулярной основе специализированных отчетов по событиям риска ИБ и направление их Заместителю Председателя Правления Банка, ответственному за обеспечение информационной безопасности, и в Департамент риск-менеджмента для формирования сводных отчетов для Совета директоров и Правления Банка;

− осуществление мониторинга сигнальных и контрольных значений контрольных показателей уровня риска ИБ;

− участие в разработке внутренних нормативных документов в области управления риском ИБ;

− информирование работников Банка по вопросам, связанным с управлением риском ИБ.

6.11. Сигнальные и контрольные значения контрольных показателей уровня риска ИБ устанавливаются в порядке, определенном «Политикой управления операционным риском в АО «РЕАЛИСТ БАНК».

6.12. По результатам оценки рисков ИБ определяется способ обработки для каждого из рисков ИБ, который является недопустимым.

6.13. Цели обработки рисков ИБ:

− добиться значительного уменьшения рисков ИБ при относительно низких затратах;

− поддерживать принятые риски ИБ на допустимом, низком уровне.

6.14. Возможными вариантами обработки рисков ИБ, с учетом требований «Политики управления операционным риском в АО «РЕАЛИСТ БАНК», являются:

− применение защитных мер, позволяющих снизить величину риска ИБ до допустимого уровня;

− уход от риска ИБ (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);

− перенос риска ИБ на другие организации (например, путем страхования или передачи деятельности на аутсорсинг);

− осознанное принятие риска ИБ.

7. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Система менеджмента информационной безопасности Банка основывается на осуществлении следующих основных процессов: планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование, соответствующих требованиям положениям международных стандартов по обеспечению информационной безопасности. 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.

7.2. При планировании мероприятий по обеспечению информационной безопасности в Банке осуществляется:

- определение и распределение ролей персонала Банка, связанного с обеспечением информационной безопасности;
- оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности;
- выявление потенциальных угроз информационной безопасности, анализ причин их возникновения и прогнозирования их развития;
- построение моделей угроз и нарушителей информационной безопасности;
- оценка рисков информационной безопасности;
- рассмотрение и оценка различных вариантов решения задач по обеспечению информационной безопасности;
- поддержка в актуальном состоянии нормативно-методического обеспечения деятельности в сфере информационной безопасности.

7.3. В рамках реализации деятельности по обеспечению информационной безопасности в Банке осуществляется:

- сбор информации о событиях информационной безопасности;
- выявление инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Банка информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним;
- повышение уровня знаний работников Банка в вопросах обеспечения информационной безопасности;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;

- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения Банка.

7.4. В целях проверки деятельности по обеспечению информационной безопасности в Банке осуществляются;

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигураций систем и подсистем Банка;
- контроль реализации и исполнения требований работниками Банка действующих внутренних нормативных документов по обеспечению информационной безопасности Банка;
- расследование и анализ инцидентов информационной безопасности.

7.5. В целях совершенствования деятельности по обеспечению информационной безопасности в Банке осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности.

7.6. Политика информационной безопасности должна быть пересмотрена в следующих случаях:

- внесения изменений в законодательные акты РФ и нормативные акты Банка России в области обеспечения информационной безопасности;
- изменения ключевых требований к защите информации;
- выявления недостатков настоящей Политики;
- принятия решения об улучшении системы ИБ.

8. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. В целях выполнения задач по обеспечению информационной безопасности Банка, в Банке определены следующие роли:

- Куратор ИБ;
- ответственное подразделение (Служба информационной безопасности);
- работник Банка.

8.2. Общее руководство обеспечением информационной безопасности Банка осуществляет Куратор ИБ.

8.3. Основными функциями Куратора ИБ в вопросах информационной безопасности являются:

- согласование назначения ответственных лиц в области информационной безопасности;
- организация и контроль деятельности Службы информационной безопасности в Банке.

8.4. Текущая деятельность и планирование деятельности по обеспечению информационной безопасности Банка осуществляются и координируются Службой информационной безопасности.

8.5. Банком при организации ресурсного (кадрового и финансового) обеспечения Службы информационной безопасности определяется минимально необходимая и достаточная численность работников Службы информационной безопасности, исходя из следующих показателей:

− уровень автоматизации процессов обеспечения операционной надежности и защиты информации;

− трудозатраты на выполнение задачи и функций обеспечения информационной безопасности;

− количество реализуемых процессов системы обеспечения информационной безопасности;

− масштаб выполнения управляемых процессов системы обеспечения информационной безопасности;

− прогноз возможного расширения состава задач и функций, возложенных на работников Службы информационной безопасности, в результате развития бизнес- и технологических процессов Банка.

8.6. Работники Службы информационной безопасности должны обладать компетенцией, необходимой для выполнения их функциональных обязанностей. Определение компетенции сводится к установлению требований в отношении знаний, практических навыков и опыта работы в области ИБ.

8.7. Состав задач, функции и требования, предъявляемые Банком к работникам Службы информационной безопасности, определены в Положении о Службе информационной безопасности АО «РЕАЛИСТ БАНК» и в должностных инструкциях указанных работников.

8.8. Основными задачами работников Банка в рамках их участия в деятельности по обеспечению информационной безопасности Банка являются:

- соблюдение требований информационной безопасности, установленных действующим законодательством, нормативными актами Российской Федерации и внутренними нормативными документами Банка;
- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
- выявление и реагирование на инциденты информационной безопасности;
- информирование своего руководителя и Службы информационной безопасности о выявленной угрозе в информационной среде Банка.

8.9. Основные внутренние нормативные документы Банка в области информационной безопасности регламентируют:

- требования по обеспечению защиты информации, применяемой на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- требования по обеспечению защиты информации, применяемой при осуществлении доступа к объектам информационной инфраструктуры;
- требования к парольной защите;
- требования по обеспечению защиты информации, применяемой от воздействия вредоносного кода, приводящих к нарушению штатного функционирования средств вычислительной техники;
- требования по обеспечению защиты информации, применяемой при использовании информационно-телекоммуникационной сети Интернет;
- требования по обеспечению защиты информации, применяемой при использовании корпоративной электронной почты;
- требования к повышению осведомленности работников Банка в области обеспечения защиты информации;
- требования информационной безопасности для сотрудников Банка;
- требования по реагированию на инциденты информационной безопасности и их обработку;
- требования по инвентаризации и классификации активов в Банке;
- требования к обеспечению защиты информации, применяемые для защиты информации при использовании средств криптографической защиты информации;
- требования по обращению и хранению носителей ключевой информации;
- требования к обеспечению защиты информации на участке платежной системы Банка России;
- требования к обеспечению безопасности банкоматов при их эксплуатации;
- требования к разработке модели угроз и модели нарушителя информационной безопасности, а также разработке методики оценки рисков нарушения информационной безопасности;
- требования по защите при использовании технологии виртуализации;

- требования к порядку проверки усиленной квалифицированной электронной подписи и хранению электронных документов, подписанных усиленной квалифицированной электронной подписью;
- требования к порядку взаимодействия Департамента информационных технологий и Службы информационной безопасности;
- порядок проведения мониторинга операций, совершаемых физическими лицами с использованием банковских карт, операций физических лиц с использованием Системы быстрых платежей;
- порядок проведения мониторинга операций, совершаемых юридическими лицами и индивидуальными предпринимателями с использованием системы ДБО;
- порядок предоставления удаленного доступа к персональным рабочим станциям АО «РЕАЛИСТ БАНК»;
- порядок предоставления доступа к системе электронного документооборота Банка;
- правила пользования услугами Удостоверяющего центра АО «РЕАЛИСТ БАНК» и основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра;
- условия осуществления обмена электронными сообщениями (далее – ЭС) и (или) пакетами ЭС при взаимодействии между Банком и Центральным Банком Российской Федерации;
- перечень персональных данных, обрабатываемых Банком, цели, принципы, сроки и способы такой обработки, порядок передачи, хранения и удаления персональных данных, ответственность на нарушение норм, регулирующих обработку персональных данных, а также другие требования, определенные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

9. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ

9.1. Ответственность за поддержание положений настоящей Политики и внутренних нормативных документов Банка в области ИБ в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы обеспечения информационной безопасности лежит на Службе информационной безопасности.

9.2. Ответственность работников Банка за неисполнение настоящей Политики и внутренних нормативных документов Банка в области ИБ определяется соответствующими положениями, включаемыми в договоры с работниками Банка, а также положениями внутренних нормативных документов Банка.

9.3. Общий контроль состояния информационной безопасности Банка осуществляет Куратор ИБ.

9.4. Текущий контроль соблюдения требований настоящей Политики осуществляет Служба информационной безопасности. Контроль осуществляется посредством проведения мониторинга и менеджмента инцидентов информационной безопасности Банка, по результатам оценки информационной безопасности Банка, а также в рамках иных контрольных мероприятий.

9.5. Служба внутреннего аудита осуществляет контроль соблюдения настоящей Политики на основе проведения внутренних проверок информационной безопасности.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Настоящая Политика вступает в силу с момента ее утверждения Правлением Банка и действует до момента отмены или принятия нового документа.

10.2. Если при изменении законодательства Российской Федерации отдельные пункты Политики вступают в противоречие с ним, то эти пункты утрачивают силу, и до момента внесения изменений в документ работники Банка руководствуются действующим

законодательством Российской Федерации, при этом факт прекращения действия одного или нескольких пунктов не влияет на действие Политику в целом.

10.3. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте Банка в информационно-телекоммуникационной сети «Интернет» по адресу: https://www.realistbank.ru.