



УТВЕРЖДЕНА
Правлением АО «РЕАЛИСТ БАНК»
Протокол № 5066 от 21.09.2020 г.

**ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «РЕАЛИСТ БАНК»**

**МОСКВА
2020**

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	3
3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ	4
4. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	4
5. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	5
6. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	5
7. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	6
8. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ	8

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности АО «РЕАЛИСТ БАНК» (далее – Политика) разработана в соответствии с требованиями законодательства Российской Федерации и нормативных документов Банка России.

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

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

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

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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 РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних 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 – Председатель Правления, курирующий вопросы информационной безопасности Банка.

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

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

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

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 09.06.2012 № 382-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 09.01.2019 № 672-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 И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью деятельности по обеспечению информационной безопасности Банка является снижение уровня угроз информационной безопасности до приемлемого для Банка значения.

Основные задачи деятельности по обеспечению информационной безопасности Банка:

- 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.

5. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источники угроз, уязвимости, используемые угрозами, методы и объекты атак, пригодные для реализации угрозы, а также описание потенциальных нарушителей определяются утвержденным в Банке Положением об организации и функционировании системы информационной безопасности, Приложением 16 Построение модели угроз и потенциального нарушителя для информационных ресурсов.

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.

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.

6. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. 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.

6.2. 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.

6.3. 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 сотрудников 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.

6.4. 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 сотрудниками Банка действующих внутренних нормативных документов по обеспечению информационной безопасности Банка;
- расследование и анализ инцидентов информационной безопасности.

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

6.6. 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.

7. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

- Куратор;
- ответственное подразделение (отдел информационной безопасности);
- сотрудник Банка.

7.2. Общее руководство обеспечением информационной безопасности Банка осуществляет Куратор.

7.3. Основными функциями Куратора в вопросах информационной безопасности являются:

- назначение ответственных лиц в области информационной безопасности;
- координация деятельности Отдела информационной безопасности Департамента экономической безопасности в Банке.

7.4. Текущая деятельность и планирование деятельности по обеспечению информационной безопасности Банка осуществляются и координируются отделом информационной безопасности.

7.5. Основными задачами сотрудников Банка в рамках их участия в деятельности по обеспечению информационной безопасности Банка являются:

- соблюдение требований информационной безопасности, устанавливаемых нормативными документами Банка;
- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
- выявление и реагирование на инциденты информационной безопасности;
- информирование своего руководства и отдела информационной безопасности о выявленной угрозе в информационной среде Банка.

7.6. Основные нормативные документы Банка в области информационной безопасности.

7.6.1. Положение об организации и функционировании системы информационной безопасности в Банке содержит требования к системе информационной безопасности в Банке и включает в себя:

• **Приложение 1. «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем».**

Определяет требования по обеспечению защиты информации, применяемой на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры.

• **Приложение 2. «Предоставление прав доступа к ресурсам автоматизированных систем».**

Определяет требования по обеспечению защиты информации, применяемой при осуществлении доступа к объектам информационной инфраструктуры.

• **Приложение 3. «Парольная защита».**

Определяет требования к парольной защите.

• **Приложение 4. «Защита от воздействия вредоносных кодов».**

Определяет требования по обеспечению защиты информации, применяемой от воздействия вредоносного кода, приводящих к нарушению штатного функционирования средства вычислительной техники.

• **Приложение 5. «Порядок использования сети интернет».**

Определяет требования по обеспечению защиты информации, применяемой при использовании информационно-телекоммуникационной сети Интернет.

• **Приложение 6. «Порядок безопасного использования корпоративной электронной почты».**

Определяет требования по обеспечению защиты информации, применяемой при использовании корпоративной электронной почты.

• **Приложение 7. «Программа обучения сотрудников Банка».**

Определяет требования к повышению осведомленности работников Банка в области обеспечения защиты информации.

• **Приложение 8. «Правила информационной безопасности для сотрудников Банка».**

Определяет требования информационной безопасности для сотрудников Банка.

• **Приложение 9. «Обработка инцидентов информационной безопасности».**

Определяет требования по реагированию на инциденты информационной безопасности и их обработку.

• **Приложение 10. «Инвентаризация и классификация активов».**

Определяет требования по инвентаризации и классификации активов в Банке.

- **Приложение 11. «Защита информации при использовании средств криптографической защиты информации».**

Определяет требования к обеспечению защиты информации, применяемые для защиты информации при использовании средств криптографической защиты информации.

- **Приложение 12. «Инструкция по обращению и хранению носителей ключевой информации».**

Определяет требования по обращению и хранению носителей ключевой информации.

- **Приложение 13. «Обеспечение защиты информации на участке платежной системы Банка России».**

Определяет требования к обеспечению защиты информации на участке платежной системы Банка России.

- **Приложение 14. «Обеспечение безопасности банкоматов».**

Определяет требования к обеспечению безопасности банкоматов при их эксплуатации.

- **Приложение 15. «Фродмониторинг платежной информации».**

Определяет требования к обеспечению безопасности при переводе денежных средств.

- **Приложение 16. «Построение модели угроз и потенциального нарушителя для информационных ресурсов».**

Определяет требования к разработке модели угроз и модели нарушителя информационной безопасности, а также разработке методики оценки рисков нарушения информационной безопасности.

- **Приложение 17. «Защита при использовании технологии виртуализации».**

Определяет требования по защите при использовании технологии виртуализации.

- **Приложение 18. «Порядок проверки усиленной квалифицированной электронной подписи».**

Определяет требования к порядку проверки усиленной квалифицированной электронной подписи и хранению электронных документов, подписанных усиленной квалифицированной электронной подписью.

- **Приложение 19. «Порядок взаимодействия Департамента информационных технологий и Отдела информационной безопасности».**

Определяет требования к порядку взаимодействия Департамента информационных технологий и Отдела информационной безопасности.

7.6.2. Политика обработки персональных данных в АО «РЕАЛИСТ БАНК» и Положение об обработке и защите персональных данных в АО «РЕАЛИСТ БАНК».

Данные документы определяют перечень персональных данных, обрабатываемых Банком, цели, принципы, сроки и способы такой обработки, порядок передачи и хранения 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».

8. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ

8.1. Ответственность за поддержание положений настоящей Политики и основных нормативных документов Банка в области ИБ, приведенных в п. 7.6 настоящей Политики, в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы обеспечения информационной безопасности лежит на Отделе информационной безопасности.

8.2. Ответственность сотрудников Банка за неисполнение настоящей Политики и основных нормативных документов Банка в области ИБ, приведенных в п. 7.6 настоящей Политики, определяется соответствующими положениями, включаемыми в договоры с работниками Банка, а также положениями внутренних нормативных документов Банка.

8.3. Общий контроль состояния информационной безопасности Банка осуществляет Куратор.

8.4. Текущий контроль соблюдения настоящей Политики осуществляет Отдел информационной безопасности Департамента экономической безопасности. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Банка, по результатам оценки информационной безопасности Банка, а также в рамках иных контрольных мероприятий.

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