КОММЕРЧЕСКИЙ БАНК
«РЕСПУБЛИКАНСКИЙ КРЕДИТНЫЙ АЛЬЯНС»
(общество с ограниченной ответственностью)

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Коммерческого Банка «Республиканский Кредитный Альянс»
(общество с ограниченной ответственностью)

Новая редакция

Москва 2020 г.

ОГЛАВЛЕНИЕ

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АБС – автоматизированная банковская система
ИС – информационная система
ИБ – информационная безопасность
АРМ – автоматизированное рабочее место
ЛВС – локальная вычислительная сеть
МЦОИ – Межрегиональный центр обработки информации Банка России
НСД – несанкционированный доступ
РКЦ – расчетно-кассовый центр
РФ – Российская Федерация
СКЗИ – средство криптографической защиты информации
СОИБ – система обеспечения информационной безопасности
ЭВМ – электронная вычислительная машина.

Комплекс БР ИББС – взаимоувязанная совокупность документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации".

2. ОБЩИЕ ПОЛОЖЕНИЯ

Политика информационной безопасности (далее - Политика ИБ) Коммерческого Банка «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью) (далее – «Банк») определяет цели и задачи обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Банк в своей деятельности.

2.1. Обеспечение соответствия законодательным актам, нормативным документам Российской федерации в области обеспечения ИБ и нормативным актам Банка России. Политика ИБ разработана с учетом следующих документов:
1. Федерального закона «О банках и банковской деятельности» от 02.12.1990 №395-1;
2. Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ;
3. Федерального закона «О коммерческой тайне» от 29.07.2004 г. №98-ФЗ;
4. Федерального закона «О персональных данных» от 27.07.2006 г. №152-ФЗ;
5. Федерального закона «О национальной платежной системе» от 27.06.2011г. №161-ФЗ;
6. Постановления Правительства РФ от 01.11.2012 г. №1119 об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных;
7. Постановления Правительства РФ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г. №687;
8. Положения Банка России от 09.06.2012 г. №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»;
9. Положения 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»;
10. Положения Банка России от 09.01.2019 г. №672-П «О требованиях к защите информации в платежной системе Банка России»;

11. Национальные стандарты РФ ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018;
12. Стандарты Банка России.

2.2. Цели и задачи.

Основными целями Политики ИБ являются защита информации Банка и обеспечение стабильной и эффективной работы всего информационно-вычислительного комплекса Банка при осуществлении деятельности, указанной в Уставе, достижение адекватных мер при защите от реальных угроз ИБ, предотвращение и/или снижение ущерба от инцидентов ИБ.

Основными задачами обеспечения 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 ИБ;
- выявление, оценка и прогнозирование угроз ИБ;
- организация антивирусной защиты информационных активов;
- защита информации от НСД и утечки по техническим каналам
- бесконтрольного выхода конфиденциальной информации за пределы Банка или круга лиц, которым она была доверена.

2.3. Определение общих ролей и обязанностей, связанных с обеспечением ИБ.

Общее руководство обеспечением ИБ Банка осуществляет Председатель Правления Банка. Ответственность за организацию мероприятий по обеспечению ИБ и контроль соблюдения требований в области ИБ несет Служба информационной безопасности, курируемый Заместителем Председателя Правления Банка, в зону ответственности которого не входит Департамент автоматизации банковских операций. Руководители структурных подразделений Банка ответственны за обеспечение выполнения требований в области ИБ в своих подразделениях. Сотрудники Банка обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией Банка, соблюдать требования настоящей Политики ИБ и других документов СОИБ.

2.4. Область действия.

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

2.5. Объекты защиты.

Объектами защиты с точки зрения информационной безопасности в Банке являются:

- банковский платежный технологический процесс;
- платежная информация;
- банковский информационный технологический процесс;
- носители защищаемой информации, в т.ч. информационные ресурсы, речевая информация, документы на бумажных и магнитных носителях, определенные как защищаемые в организационно-распорядительных документах Банка.

2.5.1. Защищаемая информация делится на следующие виды:

− информация ограниченного доступа: информация, содержащая сведения составляющие банковскую тайну и коммерческую тайну, платежную информацию и содержащую персональные данные; управляющая информация платежных, информационных и телекоммуникационных систем;
− другая информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая распорядительными актами Банка;
− открытая (общедоступная) информация.

3. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ

3.1. Общие положения:

Модели угроз и нарушителей ИБ являются определяющими при развертывании, поддержании и совершенствовании СОИБ Банка. Описание моделей угроз и блок-схема источников угроз раскрываются во внутренних нормативных документах Банка, в частности в Положение о системе информационной безопасности в Банке.

3.2. Классификация угроз ИБ:

3.2.1. Основными источниками угроз ИБ 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.

3.2.2. Угрозы ИБ могут быть реализованы нарушителем ИБ на каждом из основных уровней среды обработки информационных активов, включая:

— 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.

3.2.3. На каждом из перечисленных уровней, угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты, подходы к оценке эффективности являются различными.

3.3. Классификация нарушителя ИБ:

3.3.1. Все нарушители ИБ разделяются на следующие категории:

— внешние нарушители ИБ, не имеющие санкционированного доступа к активам Банка;
— внутренние нарушители ИБ, имеющие права доступа к АБС Банка и реализующие угрозы ИБ как в рамках своих полномочий, так и за их пределами;
— комбинированные, внешние и внутренние нарушители ИБ, действующие в сговоре.

4. ПРАВИЛА И ТРЕБОВАНИЯ ПО ИБ

4.1. Требования Политики ИБ формулируются для следующих направлений, представляющих особую важность для Банка:

4.1.1. Обеспечение соответствия СОИБ Банка законодательным актам, нормативным документам Российской Федерации в области обеспечения ИБ и нормативным актам Банка России. В Банке осуществляются доступные и разумные мероприятия, позволяющие соответствовать требованиям Комплекса БР ИББС Банка России.

4.1.2. Управление ИБ Банка включает в себя:

- разработку политики информационной безопасности;
- разработку нормативно-методических документов обеспечения ИБ;
- обеспечение штатного функционирования комплекса средств ИБ Банка;
- осуществление контроля (мониторинга) функционирования системы ИБ Банка;
- обучение с целью поддержки (повышения) квалификации персонала Банка;
- управление рисками, связанными с нарушениями ИБ.

4.2. Четкое распределение ролей.

4.2.1. Для выполнения целей по эффективному управлению активами Банка и достижение поставленных бизнес-целей, должны быть четко определены соответствующие роли персонала Банка. Роли необходимо персонифицировать с установлением ответственности за их исполнение. Формирование ролей должно осуществляться на основании бизнес-процессов. Ответственность должна быть четко прописана во всех должностных инструкциях.

4.1.2. Одна персональная роль не должна полностью охватывать цель, требуемую для реализации бизнес-процесса целиком. Совокупность правил, составляющих роли, не должна быть критичной для Банка с точки зрения последствий успешного нападения на ее исполнителя. Запрещается совмещать в одном лице роли разработки, сопровождения, исполнения, администрирования и контроля в любой комбинации.

4.2. Управление непрерывностью деятельности Банка.

4.2.1. В Банке должен быть разработан и в дальнейшем поддерживаться управляемый и документированный процесс обеспечения непрерывности деятельности Банка, учитывающий требования ИБ и служащий для того, чтобы препятствовать прерываниям хозяйственной деятельности и защищать критические важные бизнес-процессы от влияния крупных сбоев или аварий и обеспечивать их своевременное восстановление.

4.2.2. Для этого должен использоваться план обеспечения непрерывности деятельности Банка (далее – План). План определяет основные меры, методы и средства сохранения (поддержания) работоспособности АБС при возникновении различных аварийных ситуаций, а также порядок работ по восстановлению процессов обработки информации в случае

нарушения работоспособности АБС и/или основных компонентов АБС.

4.2.3. План также должны определять последовательность действий и способы взаимодействия персонала в критических ситуациях, связанных с нарушением ИБ Банка.

4.3. Управление доступом и регистрация.

4.3.1. При распределении прав доступа персонала и клиентов к активам Банка необходимо руководствоваться принципами:

- “знай своего клиента” – принцип, используемый для выражения осведомленности Банка о деятельности его клиентов;
- “знай своего служащего” – принцип, демонстрирующий озабоченность Банка по вопросам отношения к своим обязанностям и возможных проблем, которые могут приводить к проблемам с ИБ;
- “необходимо знать” – принцип, ограничивающий доступ к информации и ресурсам по обработке информации для всех, кроме лиц, функционал которых требует выполнять определенные обязанности.
- “двойное управление” – принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий того, чтобы два лица независимо предпринимали некое действие до завершения определенных транзакций.

4.4. Обеспечение антивирусной безопасности.

4.4.1. В Банке должны применяться средства антивирусной защиты. Установка и регулярное обновление средств антивирусной защиты на серверах и рабочих местах пользователей должны осуществляться уполномоченными администраторами АБС.

4.4.2. Запрещается отключение и отсутствие процедур обновления антивирусных средств.

4.5. Контролируемое использование ресурсов сети Интернет.

4.5.1. Нецелевое использование ресурсов Интернет (не связанное со служебной деятельностью) должно рассматриваться как нарушение ИБ.

4.5.2. При взаимодействии с сетью Интернет должно обеспечиваться противодействие атакам злоумышленников (хакеров) и распространение компьютерных вирусов, спама и вредоносного кода.

4.5.3. Порядок подключения и использования ресурсов сети Интернет должен контролироваться Службой внутреннего аудита и Службой информационной безопасности. Любое подключение к сети Интернет должно быть санкционировано руководителем функционального подразделения, Службой безопасности и Службой информационной безопасности Банка.

4.6. Использование средств криптографической защиты информации.

4.6.1. Банк самостоятельно определяет необходимость применения СКЗИ для защиты информации, кроме случаев, предусмотренных действующим законодательством.

4.6.2. При применении СКЗИ в АБС должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечение целостности ПО для всех звеньев АБС.

4.6.3. Процессы изготовления ключевых документов СКЗИ должны обеспечиваться комплексом технологических, организационных, технических и программных мер защиты.

4.6.4. Использование СКЗИ в Банке должно осуществляться строго в соответствии с внутренними нормативными документами и эксплуатационной документацией, поставляемыми вместе со СКЗИ.

4.7. Защита банковских технологических процессов.

4.7.1. Банковский платежный и информационный технологические процессы должны быть явно определены в нормативно-методических документах Банка.

4.7.2. Порядок обмена платежной информацией должен быть документально зафиксирован.

4.7.3. Комплекс мер по обеспечению ИБ банковских технологических процессов должен включать в себя:

— процедуры контроля за результатами технологических операций;
— защиту обрабатываемой информации от угроз, направленных на нарушение целостности, конфиденциальности и доступности.

4.8. Оповещения о нарушениях ИБ.

4.8.1. Работники Банка обязаны информировать о ставших им известными фактах нарушения положений настоящей Политики и инцидентах ИБ своего непосредственного руководителя, руководителя Службы информационной безопасности Банка в соответствии с Положением о системе информационной безопасности в Банке.

4.8.2. Руководитель Службы информационной безопасности обязан инициировать и проводить служебные расследования по фактам нарушений и инцидентов ИБ в соответствии с установленной в Банке процедурой, и докладывать о результатах расследований руководству Банка.

4.9. Осведомленность.

4.9.1. Все работники Банка должны пройти соответствующие процедуры, направленные на повышение осведомленности в вопросах ИБ.

4.9.2. Руководство Банка, все постоянные и временные работники, подрядчики, консультанты и любые внешние стороны должны быть осведомлены о своей ответственности за обеспечение ИБ, сообщении о нарушениях безопасности в соответствии с установленной в Банке процедурой оповещения.

5. САНКЦИИ И ПОСЛЕДСТВИЯ НАРУШЕНИЯ ПОЛИТИКИ ИБ

Все сотрудники Банка дают письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования о недопустимости возникновения конфликта интересов. При заключении договоров с внешними

организациями и клиентами требования по обеспечению ИБ регламентируются положениями, включаемыми в договоры (соглашения) с ними.

Обязанности персонала по выполнению требований по обеспечению ИБ включаются в трудовые контракты (соглашения, договоры) и (или) должностные инструкции.

Невыполнение сотрудниками Банка требований по обеспечению ИБ приравнивается к невыполнению должностных обязанностей и приводит, как минимум, к дисциплинарной ответственности.

6. ПОЛОЖЕНИЯ, РАЗВИВАЮЩИЕ И ДЕТАЛИЗИРУЮЩИЕ ЧАСТНЫЕ НАПРАВЛЕНИЯ ПОЛИТИКИ ИБ

В дополнение к Политике ИБ с целью обеспечения ИБ на конкретном направлении деятельности Банка, разрабатываются внутренние документы, развивающие и детализирующие отдельные направления Политики ИБ. В частности, могут разрабатываться частные политики ИБ, Положения, содержащие основные требования к обеспечению ИБ по отдельным направлениям деятельности Банка и порядки их реализации. А также инструкции и регламенты, содержащие последовательность действий при реализации требований к ИБ Банка, а также способы их контроля и зоны ответственности исполнителей, по отдельным направлениям деятельности Банка.

7. РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ ПО ОБЕСПЕЧЕНИЮ ИБ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ И ДОЛЖНОСТНЫМИ ЛИЦАМИ

7.1. Служба информационной безопасности.

В обязанности Службы информационной безопасности входит:

- организация составления и контроль выполнения всех планов по обеспечению ИБ Банка;
- определение требований к мерам обеспечения ИБ Банка;
- определение характера угроз и разработка предложений по изменению Политики ИБ Банка;
- разработка предложений по изменению существующих и принятию новых нормативно-методических документов по обеспечению ИБ Банка;
- определение минимально необходимого набора технических средств, критически важных для функционирования Банка в условиях технических сбоев, аварий, перебоев в электропитании, и разработка мер по обеспечению их безотказной работы;
- осуществление методического руководства структурными подразделениями Банка по вопросам информационной безопасности;
- контроль сотрудников Банка в части выполнения требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь сотрудников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- согласование заявок руководителей подразделений на доступ пользователей к АБС Банка, информационным активам ограниченного доступа, внешней почте и сети Интернет;
- контроль функционирования средств антивирусной и антиспамовой защиты, а также применения других средств обеспечения ИБ;
- расследование событий, связанных с нарушениями ИБ, и разработка мер, исключающих подобные события в будущем.
- участие в восстановлении работоспособности АБС, анализ причин технических сбоев и аварий и разработка мер по их предотвращению;
- участие в создании, поддержании, эксплуатации и совершенствовании СОИБ Банка.

7.2. Департамент автоматизации банковских операций.

Основными функциями по обеспечению ИБ, выполняемыми Департаментом автоматизации банковских операций, являются:

- администрирование информационных ресурсов Банка;
- обеспечение бесперебойной работы имеющихся в банке информационно-технических средств и программного обеспечения;
- обеспечение бесперебойной работы ИС Банка и оперативное восстановление их работоспособности после сбоев;
- подготовка предложений по закупке требуемых средств защиты ИС Банка;
- установка и сопровождение средств защиты ИС Банка;
- осуществление централизованного учета и хранения носителей ключевой информации;
- создание и сопровождение фонда алгоритмов и программ;
- обучение пользователей АБС безопасной работе с информационными активами;
- участие в обеспечении бесперебойной работы средств защиты внутренней информационной инфраструктуры Банка, при работе в сетях Интернет и с электронной почтой;
- администрирование и обеспечение ИБ Интернет сайта Банка;
- обеспечение связи банка с РКЦ, МЦОИ, с клиентами банка, в том числе обеспечение работы всего используемого для этой цели оборудования, средств защиты и ИБ при его использовании;
- мониторинг работы АБС Банка, Интернет-сайта Банка, каналов связи Банка с РКЦ, МЦОИ, с клиентами Банка;
- участие в работе специальной группы реагирования на инциденты ИБ;
- участие в проведении внутреннего и внешнего аудита ИБ АБС Банка;
- разработка технических заданий, проектирование, создание, тестирование и приемки средств и систем защиты ИБ Банка;
- установка и обновление антивирусных средств, проверка программных средств, используемых в Банке на отсутствие вирусов реагирование в случае обнаружения вирусов согласно нормативным документам Банка;
- подключение в установленном порядке и обеспечение использования ресурсов сети Интернет, контроль трафика;
- мониторинг работы электронной почты;
- обеспечение бесперебойного и качественного электропитания технических средств и ИС Банка;
- выполнение прочих функций в соответствии с регламентирующими документами по ИБ Банка.

7.3. Служба безопасности:

- осуществляет организацию доступа к объектам (помещениям), предназначенным для обработки конфиденциальной информации, а также помещениям, в которых находятся технические средства, предназначенные для обработки защищаемой информации;
- принимает участие в разработке технических и организационных требований к объектам (помещениям), предназначенным для обработки конфиденциальной информации;
- участвует в проведении внутреннего и внешнего аудита ИБ АБС Банка;
- согласует заявки руководителей подразделений на доступ пользователей к АБС Банка, информационным активам ограниченного доступа, внешней почте и сети Интернет;
- осуществляет обращение с персональными данными в соответствии с Политикой Банка в отношении обработки персональных данных;
- участвует в расследовании случаев несанкционированного доступа к АБС или попыток такого доступа;

− выполняет прочие функции в соответствии с регламентирующими документами по ИБ Банка.

7.4. Служба внутреннего аудита:

− проводит периодические проверки соблюдения требований ИБ;
− участвует в работе специальной группы реагирования на инциденты ИБ;
− участвует в проведении внутреннего и внешнего аудита ИБ Банка;
− выполняет прочие функции в соответствии с регламентирующими документами по ИБ Банка.

7.5. Служба управления рисками:

− осуществляет деятельность с учетом рисков ИБ Банка;
− участвует в работе специальной группы реагирования на инциденты ИБ;
− выполняет другие функции в соответствии с регламентирующими документами по ИБ Банка.

7.6. Руководители структурных подразделений:

− контролируют безопасность работы с информацией подчиненными сотрудниками;
− осуществляют обращение с персональными данными в соответствии с Политикой Банка в отношении обработки персональных данных;
− обеспечивают соблюдение сотрудниками положений Политики информационной безопасности, других внутренних документов по ИБ, разработанных в Банке требований по безопасности проводимых работ.
− выполняют прочие функции в соответствии с регламентирующими документами по ИБ Банка.

8. ПОЛОЖЕНИЯ ПО КОНТРОЛЮ РЕАЛИЗАЦИИ ПОЛИТИКИ ИБ

Председателю Правления Банка представляются следующие документы, необходимые для принятия решений в области обеспечения ИБ:

− отчеты с результатами анализа функционирования СОИБ;
− отчеты с результатами аудитов СОИБ;
− отчеты с результатами самооценок ИБ;
− документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
− документы, содержащие информацию о новых выявленных недостатках в защите информации и угрозах ИБ;
− документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
− документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве РФ и (или) в положениях стандартов Банка России;
− документы, содержащие информацию по выявленным инцидентам ИБ;
− отчетные документы о результатах выполнения требуемой деятельности по обеспечению ИБ;
− отчетные документы о результатах выполнения требований непрерывности бизнеса и его восстановления после прерывания.

Проверка и оценка ИБ.

Проверка и оценка ИБ Банка проводится путем выполнения следующих мероприятий:

- мониторинг и контроль защитных мер;
- самооценка ИБ;
- аудит ИБ;
- анализ функционирования СОИБ.

Аудит ИБ.

Порядок и периодичность проведения аудита ИБ Банка в целом (или отдельных структурных подразделений) определяется Председателем Правления Банка на основании потребности в такой деятельности и требований внешних и внутренних документов.

Внешний аудит ИБ проводится независимыми аудиторами. По результатам проведения аудита подготавливаются отчеты и доводятся до руководства. Срок хранения материалов, получаемых в процессе проведения аудита ИБ, - 5 лет. Ответственным за хранение и предоставление материалов является Служба внутреннего аудита.

9. ПЕРЕСМОТР ПОЛИТИКИ ИБ

Пересмотр Политики ИБ проводится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой ИБ защитных мер реальным условиям и текущим требованиям законодательства РФ в области защиты информации.
Пересмотр Политики ИБ осуществляется специально назначаемой для этой цели руководством Банка комиссией или рабочей группой.