**ПОЛИТИКА**

**информационной**

**безопасности**

**АО «Банк Акционерный Кредитный Стабильный»**

Москва, 2062 г.

**Содержание**

[1. ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc106384532)

[2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4](#_Toc106384533)

[3. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА 6](#_Toc106384534)

[4. СТРУКТУРА ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 8](#_Toc106384535)

[5. ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩАЕМЫХ АКТИВАХ БАНКА И ВОЗМОЖНЫХ УГРОЗАХ 9](#_Toc106384536)

[5.1. Защищаемые активы 9](#_Toc106384537)

[5.2. Источники угроз информационной безопасности Банка. 10](#_Toc106384538)

[5.3. Источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений 11](#_Toc106384539)

[5.4. Модель нарушителя информационной безопасности. 12](#_Toc106384540)

[6. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 13](#_Toc106384541)

[6.1. Основные принципы обеспечения информационной безопасности 13](#_Toc106384542)

[6.2. Требования к анализу информационной безопасности. 16](#_Toc106384543)

[7. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 16](#_Toc106384544)

[7.1. Общие требования в основе процессов обеспечения информационной безопасности Банка 16](#_Toc106384545)

[7.2. Обучение персонала 17](#_Toc106384546)

[7.3. Мониторинг событий информационной безопасности и контроль защитных мер 17](#_Toc106384547)

[7.4. Управление доступом к информационным активам и регистрация 18](#_Toc106384548)

[7.5. Антивирусная защита. 19](#_Toc106384549)

[7.6. Использование ресурсов Интернета. 20](#_Toc106384550)

[7.7. Использование средств криптографической защиты информации. 21](#_Toc106384551)

[7.8. Защита банковских платежных и информационных технологических процессов. 22](#_Toc106384552)

[7.9. Обеспечение восстановления после сбоев и непрерывности ведения деятельности Банка. 22](#_Toc106384553)

[7.10. Обеспечение физической безопасности. 23](#_Toc106384554)

[7.11. Управление рисками 23](#_Toc106384555)

[8. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 23](#_Toc106384556)

[9. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ 26](#_Toc106384557)

[10. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ПОЛИТИКУ 27](#_Toc106384558)

## ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Для достижения бизнес-целей, в условиях угроз в информационной сфере, кредитной организации необходимо обеспечивать достаточный уровень информационной безопасности своих активов (в т.ч. информационных), технологических процессов и автоматизированных систем. В этих целях АО «Банк Акционерный Кредитный Стабильный» выделяет на создание системы обеспечения информационной безопасности необходимые средства и ресурсы, в т.ч. обеспечивает разработку соответствующих нормативных документов, основным из которых является настоящая «Политика информационной безопасности АО «Банк Акционерный Кредитный Стабильный» (далее – Политика). АО «Банк Акционерный Кредитный Стабильный» ставит перед собой цель обеспечить соответствие системы обеспечения информационной безопасности (далее – ИБ) требованиям Стандарта Банка России (Обеспечение информационной безопасности организаций банковской системы Российской Федерации (далее – БС РФ), Общие положения СТО БР ИББС -1.0-2014, ГОСТ 57580.1- 2017, стандарта Банка России СТО БР ИББС-1.0-2014, ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.
  2. Настоящая Политика является внутренним нормативным документом АО «Банк Акционерный Кредитный Стабильный» (далее – Банк) и не подлежит представлению третьим лицам без согласования с Руководством Банка.
  3. Настоящая Политика определяет цели, задачи, основные принципы, общие требования и организацию системы обеспечения информационной безопасности в Банке и закрепляет риск-ориентированный и процессно-ориентированный подходы к ее функционированию и совершенствованию в соответствии с требованиями действующего законодательства РФ, документов Банка России, международных стандартов, внутренних нормативных документов Банка, рискам информационной безопасности, а также с учетом мировых и российских практик в сфере безопасности информационных технологий.
  4. Настоящая Политика определяет высокоуровневые цели и задачи, а также основные направления деятельности по обеспечению ИБ, предназначенные для Банка в целом, а также является ВНД верхнего уровня для документов:
* содержащих положения частных политик, детализирующих положения корпоративной политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка;
* содержащих положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) обеспечения ИБ, содержащих 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);
* содержащих свидетельства выполненной деятельности по обеспечению ИБ, отражающих достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению ИБ Банка.
  1. Настоящая Политика распространяется на все информационные системы Банка и их компоненты, включая банкоматы и беспроводные сети, и обязательна для выполнения всеми работниками Банка, включая обособленные структурные подразделения.
  2. Настоящая Политика должна учитываться при разработке всех внутренних нормативных документов Банка, т.е. положения настоящей Политики используются всеми структурными подразделениями Банка при разработке и внедрении процедур, инструкций, правил, стандартов или распорядительных документов Банка, которые не должны противоречить настоящей Политике.
  3. Контроль за выполнением требований настоящей Политики возложен на Отдел обеспечения информационной безопасности Банка (далее – ООИБ).

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированная банковская система (АБС)** – автоматизированная (информационная) система, реализующая технологию выполнения функций Банка.

**Администратор ИБ (АИБ)** – работник самостоятельного подразделения Банка, ответственный за взаимодействие со службой ИБ: оповещение об инцидентах и т.п.

**Актив[[1]](#footnote-1)** – Всё, что имеет ценность для Банка и находится в его распоряжении.

**Аудит информационной безопасности Банка** – периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в Банке установленных требований по обеспечению информационной безопасности.

**Банк** – АО «Банк Акционерный Кредитный Стабильный».

**Банковский технологический процесс** – технологический процесс, реализующий операции по изменению и (или) определению состояния активов Банка, используемых при функционировании или необходимых для реализации банковских услуг.

**Бизнес владелец информационной системы (ИС)** – подразделение/подразделения, являющееся основным владельцем бизнес-процесса, который автоматизирует информационная система, и, как правило, основным пользователем информационной системы;

**Владелец процесса** – самостоятельное подразделение Банка, несущее ответственность за качество и результативность процесса.

**ВНД** – внутренний нормативный документ.

**Внешние каналы связи** – каналы связи, территориально выходящие за пределы Банка.

**УИТ** –Управление информационных технологий.

**Доступность информационных активов** – свойство ИБ Банка, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

**Идентификация риска** – процесс выявления и классификации рисков.

**Информационная безопасность (ИБ) –** безопасность, связанная с угрозами в информационной сфере.

**Информационная сфера** – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

**Информационный актив** – информация с реквизитами, позволяющими ее иденти­фицировать; имеющая ценность для Банка; находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

**Инцидент информационной безопасности** – событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

**ИС ЭДО «БИС»** - Банковская информационная система, содержащая внутреннюю нормативную документацию и систему заявок и согласований.

**ИТ (IT)** – информационные технологии.

**ИТ-владелец информационной системы** – подразделение/подразделения, отвечающее за поддержание информационной системы в состоянии, отвечающем согласованному бизнес-владельцем информационной системы уровню ИТ-сервиса;

**Конфиденциальность информационных активов** – свойство ИБ, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

**Критичные банковские операции (критичные операции)** – операции, связанные с повышенными рисками информационной безопасности.

**Критичные процессы / системы** – технологические процессы / автоматизированные системы, связанные с использованием критичных информационных активов.

**Критичные уязвимости** – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных банковских систем, создающие повышенные риски информационной безопасности информационным активам.

**Критичный информационный актив (критичная информация)** – банковская информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

**ЛВС** – локальная вычислительная сеть

**Материальный носитель информации -** изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.

**НСД** – несанкционированный доступ.

**НРД** – нерегламентированные действия в рамках предоставленных полномочий.

**План ОНиВД** – План обеспечения непрерывности и восстановления деятельности Банка.

**ООИБ –** Отдел обеспечения информационной безопасности

**Оценка риска нарушения информационной безопасности** – систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации банковской системы Российской Федерации на всех стадиях их жизненного цикла.

**ПДн –** Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

**ПО** **–** программное обеспечение.

**Процесс** – совокупность взаимосвязанных активов и деятельности, преобразующая входы в выходы.

**Риск –** вероятность реализации угрозы и величина потерь (ущерба) от реализации этой угрозы.

**Риск ИБ[[2]](#footnote-2) –** риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности Банка.

**Роль** – заранее определенная совокупность функций, устанавливающих допустимое взаимодействие между субъектом и объектом в Банке.

Примечание: к субъектам относятся лица из числа руководителей и персонала Банка, клиентов или инициируемые от их имени процессы по выполнению действий над объектами. Объектами могут быть аппаратные, программные или программно-аппаратные средства, информационные активы, услуги, процессы, системы, над которыми выполняются действия.

**Система управления (менеджмента) информационной безопасностью (СУИБ)** – часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

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

**Система обеспечения информационной безопасности (СОИБ)** – совокупность системы информационной безопасности и системы управления (менеджмента) информационной безопасностью Банка.

**Событие ИБ** ‑ изменение состояния объекта или области мониторинга ИБ, действия работников организации БС РФ и (или) иных лиц, которые указывают на возможный инцидент ИБ.

**Средство вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**СУБД** – система управления базами данных.

**СУР** – Служба управления рисками

**Угроза** – внешний или внутренний фактор, создающий риск информационной безопасности.

**ЦБ РФ** – Центральный банк Российской Федерации.

**Целостность информационных активов** – свойство ИБ Банка сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

Дополнительный перечень терминов отражен в «Приложение 1».

## ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

* 1. Основными целями обеспечения информационной безопасности Банка являются:
* развитие и укрепление Банка, обеспечение его эффективного и бесперебойного функционирования в интересах собственников и клиентов Банка;
* повышение доверия к Банку;
* поддержание стабильности Банка;
* достижение адекватности мер защиты реальным угрозам информационной безопасности;
* предотвращение и (или) снижение ущерба от инцидентов информационной безопасности;
* установление единых требований по обеспечению информационной безопасности Банка;
* повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности Банка;
* защита интересов Банка в условиях угроз в информационной сфере, т.е. создание и постоянное соблюдение в Банке условий, при которых риски ИБ, постоянно контролируются и находятся на допустимом (приемлемом) уровне риска.
  1. Процессы управления рисками ИБ Банка являются составной и неотъемлемой частью процессов управления операционными рисками и осуществляются на основе циклической модели: «планирование-реализация-проверка-совершенствование-планирование-…». Процессы управления рисками ИБ включают в себя оценку необходимого уровня защиты информации; сбор и анализ данных о состоянии информационной безопасности в Банке; оценку рисков ИБ; планирование мер по снижению уровня выявленных рисков ИБ; реализацию и внедрение в рамках процедур информационной безопасности соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие действия.
  2. Информационные активы Банка оцениваются по следующим параметрам:
* доступность,
* целостность,
* конфиденциальность.

При этом основным критерием оценки является вероятность, размер и последствия нанесения Банку любого вида ущерба (невыполнение имеющихся перед государством, клиентами и партнерами обязательств, финансовые потери, потеря репутации и пр.). По результатам оценки разрабатываются и обеспечиваются соответствующие механизмы контроля и защитные мероприятия.

* 1. Состояние информационной безопасности Банка оказывает непосредственное влияние на операционные риски деятельности Банка, в связи с чем любой факт нарушения (инцидент) информационной безопасности Банка рассматривается как существенное событие.
  2. Задачами обеспечения информационной безопасности Банка являются:
* реализация требований законодательства и нормативных документов Российской Федерации по обеспечению информационной безопасности, в том числе по защите персональных данных, банковской тайны, а также норм финансовых регуляторов в части информационной безопасности кредитных организаций и мер контроля защищенности;
* формирование и реализация в соответствии с потребностями и возможностями Банка требований по режиму коммерческой тайны, защите внутрибанковской информации;
* обеспечение защищенности реализуемых Банком банковских технологических процессов и предоставляемых банковских продуктов и услуг;
* обеспечение защищенности операций клиентов Банка и информационной безопасности при взаимодействии с контрагентами, поставщиками продуктов и услуг;
* планирование, реализация и контроль использования защитных мер информационной безопасности, прогнозирование развития событий на основе мониторинга и менеджмента инцидентов информационной безопасности;
* координация всех видов деятельности Банка в целях обеспечения информационной безопасности, в том числе через инициирование / согласование / принятие соответствующих внутренних документов информационной безопасности Банка, реализацию программ по осведомленности и обучению персонала Банка, информированию своих клиентов о факторах рисков информационной безопасности банковских операций и возможным мерам противодействия;
* минимизация ущерба и обеспечение быстрейшего восстановления видов деятельности Банка, пострадавших в результате кризисных ситуаций, расследования причин возникновения таких ситуаций и принятия соответствующих мер по их предотвращению.
* снижение операционных рисков Банка в области информационной безопасности;
* предупреждение возможности реализации угроз информационным активам (минимизация рисков ИБ, устранение уязвимостей информационных активов);
* своевременное выявление новых угроз информационной безопасности;
* минимизация потерь Банка при реализации угроз информационной безопасности;
* контроль состояния информационной безопасности Банка на всех этапах жизненного цикла автоматизированных банковских систем;
* защита законных прав Банка и работников, в случаях неправомерного использования или злоупотребления информационными активами Банка.
  1. Основными принципами обеспечения информационной безопасности Банка являются:
* Своевременность обнаружения проблем (Банк своевременно обнаруживает проблемы, прямо или косвенно относящиеся к информационной безопасности, потенциально способные повлиять на его бизнес-цели);
* Прогнозируемость развития проблем (Банк выявляет причинно-следственную связь возможных проблем и строит на этой основе точный прогноз их развития);
* Оценка влияния проблем на бизнес-цели (Банк адекватно оценивает степень влияния выявленных проблем на его бизнес-цели);
* Адекватность защитных мер (Банк выбирает защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз);
* Эффективность защитных мер (Банк эффективно реализует принятые защитные меры);
* Использование опыта при принятии и реализации решений (Банк накапливает, обобщает и использует как свой опыт, так и опыт других организаций в обеспечении информационной безопасности на всех уровнях принятия решений и их исполнения);
* Непрерывность принципов безопасного функционирования (Банк обеспечивает непрерывность реализации принципов безопасного функционирования);
* Контролируемость защитных мер (Банк применяет только те защитные меры, правильность работы которых может быть проверена; при этом Банк регулярно оценивает адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на его бизнес-цели).
* Определенность целей (Функциональные цели и цели информационной безопасности Банка явно определяются во внутренних документах Банка);
* Знание своих клиентов и работников (Банк обладает информацией о своих клиентах, тщательно подбирает персонал (работников), вырабатывает и поддерживает корпоративную этику, что создает благоприятную доверительную среду для деятельности Банка по управлению активами);
* Персонификация и адекватное разделение ролей и ответственности (ответственность должностных лиц Банка за решения, связанные с его активами, персонифицируется и осуществляется преимущественно в форме поручительства; она должна быть адекватной степени влияния на цели Банка, фиксироваться в политиках, контролироваться и совершенствоваться);
* Адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки (роли адекватно отражают исполняемые функции и процедуры их реализации, принятые в Банке; при назначении взаимосвязанных ролей Банк учитывает необходимую последовательность их выполнения; роль согласовывается с критериями оценки эффективности ее выполнения; основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки);
* Доступность услуг и сервисов (Банк обеспечивает доступность для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и/или иными документами);
* Наблюдаемость и возможность оценки результата обеспечения информационной безопасности (любые предлагаемые защитные меры устраиваются так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен подразделением Банка, имеющим соответствующие полномочия).

## СТРУКТУРА ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* 1. Деятельность Банка по обеспечению информационной безопасности осуществляется на основании действующих законодательных и нормативно-правовых актов Российской Федерации по обеспечению безопасности информации, нормативно-правовых актов Банка России и внутренних документов Банка по обеспечению информационной безопасности.
  2. Внутренние документы Банка по обеспечению информационной безопасности являются едиными для Банка и:
* носят обязательный характер;
* выполнимы и контролируемы, т.е. не содержат положения, контроль реализации которых затруднен или невозможен;
* адекватны требованиям и условиям ведения деятельности, в том числе в условиях их изменчивости;
* не противоречат друг другу.

## ОБЩИЕ СВЕДЕНИЯ О ЗАЩИЩАЕМЫХ АКТИВАХ БАНКА И ВОЗМОЖНЫХ УГРОЗАХ

### Защищаемые активы

К активам Банка относятся:

* работники (персонал),
* финансовые (денежные) средства,
* средства вычислительной техники и телекоммуникационное оборудование,
* различные виды конфиденциальной информации (банковская тайна, коммерческая тайна, служебная информация, персональные данные и пр.), обрабатываемые в Банке.
  + 1. От угроз, связанных с риском ИБ, защищаются следующие активы Банка:
* платёжная информация;
* информация (данные) информационных и телекоммуникационных систем;
* управляющая информация платёжных, информационных и телекоммуникационных систем;
* документация внутреннего делопроизводства;
* платежные и информационные технологические процессы;
* банковские продукты и услуги, предоставляемые клиентам;
* аппаратно-программные, технические комплексы и программное обеспечение, обеспечивающие реализацию функций Банка;
* документация на программные, аппаратные средства и системы;
* персональные данные работников, клиентов;
* данные банковских карт.
  + 1. Информационный актив - информация с позволяющими ее идентифицировать реквизитами, имеющая ценность для Банка, находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Информационными активами Банка является следующая информация:

* информация об остатках денежных средств на банковских счетах;
* информация об остатках электронных денежных средств;
* информация о совершенных переводах денежных средств, в том числе информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений участников платежной системы, а также в извещениях (подтверждениях), касающихся исполнения распоряжений участников платежной системы;
* информация, содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств (далее - клиентов), распоряжениях участников платежной системы, распоряжениях платежного клирингового центра;
* информация о платежных клиринговых позициях;
* информация, необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе данные держателей платежных карт;
* ключевая информация средств криптографической защиты информации (далее - СКЗИ), используемая при осуществлении переводов денежных средств (далее - криптографические ключи);
* информация о конфигурации, определяющая параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается оператором по переводу денежных средств, оператором услуг платежной инфраструктуры, банковским платежным агентом (субагентом), и используемых для осуществления переводов денежных средств (далее - объекты информационной инфраструктуры), а также информация о конфигурации, определяющей параметры работы технических средств защиты информации;
* информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.
  + 1. Классификация информационных активов – это разделение существующих информационных активов Банка по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ (конфиденциальности, целостности или доступности).

По степени тяжести последствий информационные активы Банка классифицируются (относятся) к следующим типам:

* банковский платежный технологический процесс – относится к типу с высокой степенью тяжести последствий;
* платежная информация – относится к типу с высокой степенью тяжести последствий;
  + 1. Перечень информационных активов, структурированных по классам, разрабатывается УИТ в рамках «Политики информационных систем» и утверждается Правлением Банка и актуализируется не реже 1 (Одного) раза в год.
    2. В Банке должны быть определены бизнес-владельцы ИС по одному из следующих принципов:
* владельцем ИС является владелец основного процесса, автоматизируемого данной информационной системой;
* владельцем ИС является выделенное подразделение Банка;
* для инфраструктурных информационных систем владельцем ИС является Управление информационных технологий.
  + 1. В обязанности владельца ИС входит согласование критичных изменений в информационную систему, создание новых и изменение текущих доступов, а также согласование предоставления/изменения/удаления полномочий работников.
    2. В обязанности сотрудников УИТ входит поддержание информационных систем Банка в состоянии, отвечающем потребностям автоматизированных ею бизнес-процессов на основании требований владельцев ИС, а также соответствие информационной системы требованиям обеспечения ИБ.

### Источники угроз информационной безопасности Банка.

* + 1. В связи с тем, что Банк относится к организациям повышенного риска, в настоящей Политике ИБ определены источники угроз, модель нарушителя информационной безопасности и операционные риски информационной безопасности на стадии эксплуатации автоматизированной системы. Риски ИБ устанавливаются в соответствии с актуальной Методикой определения угроз безопасности информации в информационных системах (ФСТЭК).
    2. Любое лицо, имеющее физический и логический доступ к информационным активам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи), может являться потенциальным злоумышленником. При этом предполагается возможность сговора работника Банка с внешним злоумышленником, но не сговор 2 (Двух) и более работников Банка.
    3. Целью злоумышленника может являться получение контроля над информационным активом Банка, приводящего в результате к нарушению его свойств доступности, целостности или конфиденциальности.
    4. Для достижения целей злоумышленник может использовать все способы проведения атак на всех уровнях архитектуры автоматизированных систем.
    5. Угроза – это опасность, предполагающая возможность потерь (ущерба). Модель нарушителя информационной безопасности (модель нарушителя ИБ) – это описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.
    6. Модель угроз информационной безопасности (модель угроз ИБ) – это описание актуальных для Банка источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.
    7. Деятельность Банка поддерживается входящей в его состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде следующих основных уровней:
* физического (линии связи, аппаратные средства и пр.);
* сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
* сетевых приложений и сервисов;
* операционных систем (ОС);
* систем управления базами данных (СУБД);
* банковских технологических процессов и приложений;
* бизнес-процессов организации.
  + 1. На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы, средства защиты и подходы к оценке эффективности в Банке являются различными.

### Источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений

* + 1. Основными источниками угроз ИБ являются:
* 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 несанкционированного доступа или нерегламентированных действий в рамках предоставленных полномочий (внешние нарушители ИБ);
* сбои, отказы, разрушения/повреждения программных и технических средств;
* несоответствие требованиям надзорных и регулирующих органов, действующему законодательству;
* зависимость от поставщиков/провайдеров/партнеров/клиентов;
* неблагоприятные события природного, техногенного и социального характера;
* террористы и криминальные элементы.
  + 1. На физическом уровне, уровне сетевого оборудования и уровне сетевых приложений актуальными источниками угроз являются:
* внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки несанкционированного доступа или нерегламентированных действий;
* внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
* комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
* сбои, отказы, разрушения/повреждения программных и технических средств.
  + 1. На уровнях операционных систем, систем управления базами данных, банковских технологических процессов актуальными источниками угроз являются:
* внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;
* комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре (На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно без соучастия внутренних, практически невозможна).
  + 1. На уровне бизнес-процессов актуальными источниками угроз являются:
* внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;
* комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
* несоответствие требованиям надзорных и регулирующих органов действующему законодательству.
  + 1. Пересмотр моделей угроз и нарушителей ИБ осуществляется вместе с пересмотром Политики, а также в случае выявления инцидентов информационной безопасности, обнаружения новых угроз и уязвимостей, значительных изменениях в организационной или технической инфраструктуре Банка, а также в случае изменения требований законодательства или выявления нарушений.

### Модель нарушителя информационной безопасности.

* + 1. Модель нарушителя представляет собой описание источников угроз ИБ, актуальных для Банка:
* методов реализации угроз ИБ;
* объектов, пригодных для реализации угроз ИБ;
* уязвимостей, используемых источниками угроз ИБ;
* типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов);
* масштабов потенциального ущерба.
  + 1. Внутренние нарушители информационной безопасности:
* пользователи АБС;
* системные администраторы, работники, имеющие права администрирования систем управления базами данных и приложений;
* персонал, обслуживающий технические средства, работники службы безопасности и охраны;
* руководители всех уровней.
  + 1. Внешние нарушители информационной безопасности:
* технический персонал, обслуживающий здания Банка;
* клиенты Банка;
* посетители - лица, приглашенные по какому-либо поводу в Банк;
* представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности Банка (энерго-, тепло-, водоснабжения и т.д.);
* представители организаций-арендаторов помещений;
* лица, случайно или умышленно нарушившие пропускной режим.
  + 1. Мотивы нарушений информационной безопасности:
* безответственность;
* самоутверждение;
* месть;
* корыстный интерес.
  + 1. Уровень знаний нарушителей информационной безопасности, необходимый для реализации угрозы:
* нарушитель знает функциональные особенности автоматизированной системы, умеет пользоваться штатными средствами;
* нарушитель обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
* нарушитель обладает высоким уровнем знаний в области программирования и эксплуатации автоматизированных систем;
* нарушитель знает структуру, функции и механизм действия средств защиты, их слабые стороны.
  + 1. Уровень используемых методов и средств нарушения информационной безопасности:
* агентурные методы получения сведений;
* технические средства перехвата информации;
* использование недостатков системы защиты;
* использование магнитных носителей, мобильных средств перемещения/передачи значительных объемов информации (внешние жесткие диски, флэш накопители).
  + 1. Место действия нарушителей информационной безопасности:
* без доступа на территорию Банка;
* с рабочих мест пользователей;
* с доступом в серверную.

## ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### Основные принципы обеспечения информационной безопасности

* + 1. Законность – применение мер и средств обеспечения ИБ в строгом соответствии с положениями действующего законодательства РФ в области ИБ.
    2. Системность – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения ИБ
    3. Эшелонированность – применение нескольких защитных барьеров на пути реализации угроз ИБ.
    4. Непрерывность защиты – деятельность по обеспечению ИБ является составной частью повседневной деятельности и не должна прерываться, в том числе должна обеспечиваться постоянная поддержка физических, технических и программных средств защиты, а также непрерывный контроль выполнения требований ИБ.
    5. Гибкость – ООИБ Банка должен быть способен реагировать на изменения внешней среды и условий осуществления Банком своей деятельности.
    6. Исключение конфликта интересов – четкое разделение обязанностей и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. В частности, ни один работник Банка должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций.
    7. Своевременность обнаружения проблем, прогнозируемость их развития – все работники Банка должны своевременно обнаруживать проблемы, относящиеся к информационной безопасности и потенциально способные повлиять на бизнес – процессы Банка.
    8. Осведомленность о требованиях информационной безопасности – все работники Банка вне зависимости от своих должностных обязанностей и наличия у них компьютерной техники должны знать требования информационной безопасности и руководствоваться ими в своей работе. Все работники Банка проходят обучение по повышению осведомленности в области информационной безопасности.
    9. Персональная ответственность – ответственность за нарушения требований информационной безопасности возлагается непосредственно на работников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.
    10. Ограничение полномочий:
* Минимальность полномочий:

Любому работнику Банка доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными в Банке процедурами;

* Разделение полномочий:

Все критичные банковские операции выполняются 2 (Двумя) работниками. Возможность единоличного совершения критичной операции не допускается;

* Контроль лимитов и ограничений рисков информационной безопасности:

Возможность проведения банковских операций, подверженных рискам ИБ, должна ограничиваться по сумме операции, количеству операций, времени проведения операций, должности работника и другим показателям, исходя из уровня принятых рисков информационной безопасности. Автоматизированные банковские системы обеспечивают автоматический контроль соответствия параметров операций установленным лимитам и ограничениям.

* + 1. Комплексность защиты информационной безопасности – меры по обеспечению информационной безопасности принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков ИБ.
    2. Адекватность защиты информационной безопасности – принимаемые меры обеспечения информационной безопасности должны быть эффективны и соразмерны имеющим место рискам ИБ, модели угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз. Адекватность защитных мер и эффективность их реализации регулярно оцениваются с учетом влияния защитных мер на бизнес-цели Банка.
    3. Эргономичность защиты – средства защиты должны быть максимально «прозрачны» и удобны для пользователей и администраторов автоматизированных систем.
    4. Документированность[[3]](#footnote-3) - документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально.
    5. Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности:

В Банке осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых проводится анализ эффективности принятых мер с учетом изменений информационной сферы, появления новых угроз, инцидентов информационной безопасности и проблем; планирование и внедрение дополнительных мер защиты. С целью обеспечения непрерывности реализации принципов функционирования, системы обеспечения информационной безопасности:

* Пассивность контроля;
* Применяемые инструментальные средства контроля и обеспечения информационной безопасности не предоставляют доступ работникам, ответственным за их эксплуатацию, непосредственно к критичной банковской информации;
  + 1. Разделение полномочий по управлению ИТ – в Банке реализована структура управления информационными технологиями, направленная на исключение конфликта интересов и строгое разграничение ответственности при обеспечении функционирования и безопасности информационных активов. Обязанности подразделений и работников Банка, осуществляющих администрирование коммуникационного оборудования, операционных систем, СУБД, автоматизированных систем, средств защиты и осуществляющих функции мониторинга состояния информационной безопасности и контроля (аудита) выполнения требований информационной безопасности, разделены.
    2. Контроль со стороны Правления Банка – Банк использует только те защитные меры, правильность работы которых может быть проверена. Правление Банка на регулярной основе рассматривает отчеты о состоянии информационной безопасности в подразделениях Банка и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы и бизнес-цели Банка. При этом Банк накапливает и использует как свой опыт, так и опыт других организаций (лучшие практики) на всех уровнях принятия решений и их исполнения.
    3. Сочетание централизованного и децентрализованного подходов к управлению рисками ИБ – ООИБ проводит единую политику в области защиты информации, определяет требования к используемым в Банке средствам обеспечения информационной безопасности и к информационной безопасности в Банке, разрабатывает соответствующие проекты нормативных, методических и инструктивных документов.
    4. Целевое финансирование мероприятий по обеспечению информационной безопасности – ежегодный бюджет Банка предусматривает специальные статьи расходов на обеспечение информационной безопасности.
    5. Знание своих клиентов, работников и контрагентов – Банк обладает информацией о своих клиентах, тщательно подбирает персонал (служащих), вырабатывает и поддерживает корпоративную этику, создавая благоприятную доверительную среду для деятельности Банка по управлению информационными активами.
    6. Безопасность в соглашениях – для регулирования отношений со сторонними организациями (третьими лицами) с точки зрения информационной безопасности в соответствующие договоры (соглашения и т.д.) включается раздел, посвященный требованиям по информационной безопасности, либо разрабатывается отдельный документ (Соглашение о конфиденциальности), который подписывается обеими сторонами. Банк принимает меры по контролю деятельности третьих лиц, такие как:
* проверка результатов деятельности третьих лиц;
* осуществление деятельности третьих лиц только в присутствии работников Банка;
* ведение аудиторского следа за действиями третьих лиц;
* запись сессии доступа к информационным активам специальными программно-техническими комплексами.

### Требования к анализу информационной безопасности.

* + 1. Аудит информационной безопасности проводится как внешними аудиторами, так и внутренними аудиторами Банка в соответствии с Планом проверок Службы внутреннего аудита.
    2. Инструментальный анализ защищенности внешних и внутренних информационных активов Банка ежегодно осуществляется ООИБ при проведении самооценки в соответствии с Порядком организации и проведения аудитов и самооценок информационной безопасности, либо после значительных изменений в инфраструктуре Банка.
    3. Основные принципы реализации процедур оценки рисков ИБ.
* Учитывая, что наиболее трудоемким и субъективным процессом обеспечении информационной безопасности является оценка рисков, а также с учетом необходимости унификации и максимального удешевления технологий защиты, в Банке осуществляется классификация информационных активов по степени их критичности. Классификация осуществляется подразделением – владельцем информационного актива по каждому из аспектов информационной безопасности: конфиденциальности, доступности и целостности и направляется в виде служебной записки в ООИБ.
* Использование типовых требований безопасности, дифференцированных по классам информационных активов.
* Выполнение типовых требований обеспечивает соответствующий базовый уровень информационной безопасности для каждого класса информационных активов.
* Использование типовых средств и процедур обеспечения информационной безопасности для разных информационных активов одного класса.
* Использование единой модели злоумышленника, адекватной реальным угрозам.
* Оценка достаточности базового уровня безопасности с учетом конкретных особенностей применяемых информационных технологий и связанных с ними угроз осуществляется рабочей группой по оценке рисков, создаваемой приказом по Банку.

## ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### Общие требования в основе процессов обеспечения информационной безопасности Банка

* + 1. Назначение и распределение ролей и обеспечение доверия к персоналу;
    2. «Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.
    3. Роли формируются с учетом принципа минимальности полномочий.
    4. Ни одна роль не позволяет пользователю проводить единолично критичные операции.
    5. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированной банковской системы;
    6. Защита от несанкционированного доступа и нерегламентированных действий в рамках предоставленных полномочий, управление доступом и регистрацией всех действий в автоматизированной банковской системе, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;
    7. Организация и контроль антивирусной защиты;
    8. Контроль использования ресурсов сети Интернет;
    9. Контроль использования средств криптографической защиты информации;
    10. Защита банковских платежных и информационных технологических процессов, в рамках которых обрабатываются персональные данные.
    11. Критичные банковские технологические процессы защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления, при наличии технической возможности, выполняются через специальные роли в автоматизированных системах без непосредственного доступа к данным.
    12. В критичных системах при наличии технической возможности, по решению владельца информационного актива может вводиться роль администратора информационной безопасности системы, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.
    13. Обязанности по эксплуатации механизмов, средств и систем защиты информации возлагаются соответствующими приказами (распоряжениями) на Администратора (Администраторов) ИБ. Администраторы ИБ совместно с ИТ-владельцами ИС участвуют в управлении процессами эксплуатации и обеспечения ИБ автоматизированных систем. Допускается назначение одного Администратора ИБ на несколько автоматизированных систем, а также совмещение выполнения указанных функций с другими обязанностями. При этом совмещение в одном лице функций ИТ-владельца ИС и Администратора ИБ системы не допускается.
    14. Обеспечивается разделение контуров эксплуатации разработки и тестирования автоматизированных систем.
    15. Должностные обязанности работников и трудовые договоры предусматривают обязанности персонала по выполнению требований информационной безопасности, включая обязательства о соблюдении конфиденциальности. При этом условие о соблюдении конфиденциальности распространяется на всю защищаемую информацию, доверенную работнику или ставшую ему известной в процессе выполнения им своих служебных обязанностей.
    16. Порядок реализации вышеуказанных требований определяется в соответствующих частных политиках и порядках по информационной безопасности. Приказы и актуальная информация по вопросам обеспечения информационной безопасности доводится до всех работников Банка посредством ИС ЭДО «БИС».

### Обучение персонала

* + 1. В Банке, в соответствии с программой повышения осведомленности персонала в вопросах информационной безопасности, проводится ежегодное обучение работников Банка по вопросам обеспечения информационной безопасности. При периодической оценке проверяется и оценивается уровень компетентности работников Банка в вопросах информационной безопасности. Осуществляется контроль проведения мероприятий по повышению осведомленности в вопросах ИБ.
    2. При допуске к работе с критичными системами, а также периодически работники Банка могут подвергаться проверке методами, не запрещенными действующим законодательством Российской Федерации.

### Мониторинг событий информационной безопасности и контроль защитных мер

* + 1. В Банке обеспечивается мониторинг процессов с целью:
* обнаружения ошибок в результатах обработки информации;
* выявления удачных и неудавшихся попыток нарушений и инцидентов информационной безопасности;
* выявления отклонений от планового процесса обеспечения информационной безопасности Компании и определение причин отклонений;
* оценки эффективности мероприятий, предпринятых для совершенствования СУИБ (путем введения сигнальных значений и специальных показателей эффективности – метрик).
  + 1. По результатам анализа СУИБ, информации по произошедшим инцидентам ИБ, результатам оценки эффективности процессов ИБ, ООИБ определяются корректирующие и предупреждающие меры для совершенствования СУИБ.
    2. В Банке определена «Частная политика мониторинга событий и управления инцидентами информационной безопасности АО «Банк Акционерный Кредитный Стабильный» (АО)», регламентирующая процедуры мониторинга информационной безопасности и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты.

### Управление доступом к информационным активам и регистрация

* + 1. В Банке документально определены процедуры идентификации, аутентификации и авторизации; управления доступом; контроля целостности; регистрации событий и действий.
    2. В составе АБС применяются встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные ООИБ к применению средства защиты информации от НСД и НРД.
    3. Все информационные активы Банка идентифицируются, классифицируются и имеют своих владельцев.
    4. Каждый пользователь АБС в Банке наделяется индивидуальным, уникальным идентификатором, который используется только в рамках соответствующей подсистемы регистрации.
    5. Во всех защищаемых автоматизированных системах Банка обеспечиваются:
* идентификация, аутентификация, авторизация пользователей;
* управление доступом к информационным активам системы, исключающее возможность проведение критичных, в том числе финансовых операций без санкций предусмотренных ВНД банка;
* контроль целостности баз данных;
* функционирование системы парольной защиты ПК и ЛВС;
* регистрация событий и действий пользователей.
  + 1. В Банке осуществляются мониторинг и анализ данных регистрации событий, действий и операций, позволяющие по определенным критериям выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций в Банке могут использоваться специализи­рованные программные и (или) технические средства.
    2. Контроль доступа пользователей к информационным активам Банка осуществляется работниками ООИБ. Контроль предусматривает анализ заявок в системе ИС ЭДО «БИС», журналов регистрации событий Active Directory, АБС, контроль корректности назначения прав доступа пользователям автоматизированных систем. Факты выявления нарушений процедур предоставления доступа к информационным активам рассматриваются как инциденты ИБ.
    3. Доступ к информационным активам всем работникам Банка предоставляется на основании заявок, оформленных через систему ИС ЭДО «БИС», согласованных с ООИБ и, при необходимости, владельцами соответствующих информационных активов.
    4. Доступ к информационным активам прекращается в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения работника.
    5. При назначении или лишении полномочий доступа работников к информационным активам Банка применяются следующие принципы и подходы:
* каждый пользователь автоматизированных систем имеет свой индивидуальный, уникальный идентификатор;
* пользователь не имеет прав локального администратора;
* пользователь не имеет возможность осуществлять бесконтрольное копирование информации или ее передачу по сетям или системам электронной почты, или с использованием отчуждаемых носителей информации.
  + 1. Доступ работников Банка в помещения, в которых размещается оборудование, обрабатывающее защищаемые информационные активы, осуществляется только с использованием пропусков со специальным уровнем доступа.
    2. В Банке проводится периодический (для наиболее критичных систем – не реже одного раза в квартал) контроль соответствия согласованных и реальных прав доступа к информационным активам текущему статусу пользователя.
    3. Работа пользователей с базами данных осуществляется исключительно через экранные формы и отчеты автоматизированных банковских систем. Прямой доступ пользователей к базам данных не предоставляется.
    4. Доступ ко всем информационным активам Банка осуществляется только после авторизации пользователя. По возможности рекомендуется использование единых процедур сильной (не имеющей недостатков клавиатурных паролей) аутентификации при доступе к разным информационным активам.
    5. Журналы аудита действий пользователей и администраторов автоматизированных систем информативны, защищены от модификации и хранятся, по крайней мере, в течение 5 (пяти) лет, при этом в течение 3 (Трех) месяцев журналы доступны в режиме оперативного доступа для анализа. Банковские автоматизированные системы содержат штатные средства анализа журналов и формирования отчетов по заданным критериям.
    6. Санкционирование использования отчуждаемых носителей и устройств на объектах Банка осуществляется только после согласования с ООИБ и Кураторами подразделений/Руководителями внутренних структурных подразделений.
    7. В Банке применяются защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информационных активов, необходимых для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников Банка. Все попытки НСД и НРД к таким активам регистрируются с помощью встроенных механизмов регистрации событий.
    8. Доступ посторонних лиц к автоматизированным рабочим местам работников, выполняющих обработку защищаемых информационных активов, исключается.

### Антивирусная защита.

* + 1. Каждый работник Банка обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать ООИБ и УИТ при наличии подозрений или обнаружении факта вирусного заражения.
    2. Установка средств антивирусной защиты на автоматизированных рабочих местах и серверах АБС осуществляется специалистами УИТ, а регулярное обновление может проводиться как автоматически, так и администраторами АБС.
    3. Техническая возможность подключения пользователями к рабочим станциям ЛВС внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использования CD/DVD-дисководов, USB-накопителей ограничивается программными средствами и предоставляется только по согласованию с ООИБ.
    4. Антивирусная защита обеспечивается использованием в Банке специализированного программного обеспечения, по крайней мере, двух независимых производителей и их раздельной установкой на информационных активах сети Банка.
    5. Устанавливаемое или изменяемое программное обеспечение предварительно проверяется на отсутствие вирусов. После установки или изменения программного обеспечения выполняется антивирусная проверка.
    6. Для снижения влияния человеческого фактора, исключения возможности отключения или нерегулярного обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производятся централизованно в автоматизированном режиме.
    7. Отключение или не обновление сигнатурных баз не допускается. Установка и обновление антивирусных средств в Банке осуществляется УИТ. Контроль обновления антивирусных баз проводит ООИБ.
    8. При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных активов и техническими возможностями такого обновления.

### Использование ресурсов Интернета.

* + 1. Использование ресурсов Интернета в подразделениях Банка разрешается исключительно в целях выполнения служебных обязанностей.
    2. Иное использование ресурсов сети Интернет, решение о котором не принято Правлением Банка в установленном порядке, рассматривается как нарушение ИБ.
    3. По мере возможности следует ограничивать использование Интернета для информационного взаимодействия между подразделениями Банка.
    4. Предоставление услуг клиентам Банка и взаимодействие с партнерами по сети Интернет осуществляются с использованием специализированных систем и средств защиты.
    5. Подключение к рабочим станциям ЛВС Банка мобильных телефонов, беспроводных (радио) интерфейсов, модемов и прочего оборудования, позволяющего выходить в Интернет, запрещается.
    6. Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение работниками Банка на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний и разрешений руководства Банка.
    7. ООИБ осуществляет контроль за соблюдением работниками требований информационной безопасности при работе в сети Интернет, включая анализ содержания сообщений электронной почты и посещенных ресурсов.
    8. Почтовый обмен через сеть Интернет осуществляется с использованием защитных мер, реализованных посредством межсетевых экранов, подсистемы защиты от спама, антивирусных средств защиты на почтовом сервере и ПК работников. Все почтовые сообщения, полученные из сети Интернет/переданные в сеть Интернет, архивируются автоматизированной системой архивации, обеспечивающей контроль целостности указанной информации.
    9. Доступ к информации архива электронной почты предоставляется ООИБ для проведения расследований инцидентов ИБ.
    10. На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

### Использование средств криптографической защиты информации.

* + 1. Применение средств криптографической защиты информации для обеспечения безопасности информационных активов Банка и взаимодействия с клиентами производится в соответствии с порядком, установленным государственными уполномоченными органами.
    2. Применение средств криптографической защиты информации в Банке осуществляется в соответствии с моделью нарушителей и угроз информационной безопасности.
    3. При применении средств криптографической защиты информации поддерживается непрерывность процессов протоколирования их работы и обеспечения целостности программного обеспечения для среды функционирования средств криптографической защиты информации.
    4. Информационная безопасность процессов изготовления криптографических ключей средств криптографической защиты информации обеспечивается комплексом технологических, организационных, технических и программных мер и средств защиты.
    5. Использование электронно-цифровой подписи обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с клиентами.
    6. Использование иных аналогов собственноручной подписи (кодов аутентификации, PIN-кодов и пр.) при взаимодействии с клиентами допускается в технически и экономически обоснованных случаях по согласованию с ООИБ.
    7. Во внутренних системах Банка электронная цифровая подпись и/или другие механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков ИБ, а также в случаях, когда необходимо строго разделить ответственность между подразделениями или работниками Банка.
    8. Конфиденциальность банковской информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования. В обоснованных случаях информация, составляющая коммерческую тайну Банка, может также шифроваться при ее передаче в ЛВС и хранении на средствах вычислительной техники.
    9. Передаваемые клиентам Банка средства шифрования используются только для организации защищенного взаимодействия с Банком.
    10. Доступ к ключам шифрования разрешен только нескольким ответственным за их хранение и использование работникам. Процедуры управления ключами обеспечивают раздельное владение частями ключей при наличии технической возможности.
    11. Ключи шифрования хранятся только в строго определенных защищенных хранилищах и в строго определенном виде.
    12. В Банке документированы все процессы и процедуры управления ключами шифрования данных о держателях карт.
    13. Риски ИБ, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, минимизируются специальными техническими и организационными мерами, определяемыми ООИБ.
    14. Ключи усиленной квалифицированной электронной подписи (КЭП), предназначенные для защиты электронного документооборота Банка с клиентами и сторонними организациями, изготавливаются сторонами исключительно самостоятельно.

### Защита банковских платежных и информационных технологических процессов.

* + 1. Технологические процессы максимально автоматизированы и обеспечивают возможность выполнения массовых и потенциально опасных операций без участия работников за счет реализации эффективных процедур контроля и защиты.
    2. Электронные документы, не прошедшие процедуры контроля содержания и защиты, не передаются на ручную обработку. При этом в подразделения или клиентам, от которых они поступили, направляются извещения о необходимости повторного ввода.
    3. В Банке проводится политика максимального перевода клиентов на обслуживание в режиме полного защищенного электронного документооборота, что стимулируется тарифной политикой и бизнес-планами Банка.
    4. Выполнение критичных операций в ручном режиме осуществляется, с соблюдением принципа «двух рук», либо ограничивается системой лимитов и ограничений. Лучшей практикой является подтверждение операции самим клиентом при условии его надежной аутентификации.
    5. Для защиты технологических процессов по результатам анализа рисков ИБ могут применяться как штатные средства безопасности сетевых операционных систем, СУБД, так и дополнительные программные и программно-аппаратные комплексы и средства криптографической защиты, в совокупности обеспечивающие достаточный уровень безопасности на всех участках и этапах технологического процесса.

### Обеспечение восстановления после сбоев и непрерывности ведения деятельности Банка.

* + 1. В Банке определен «План действий, направленных на обеспечение непрерывности деятельности и/или восстановление деятельности АО «Банк Акционерный Кредитный Стабильный» в случае возникновения нестандартных и чрезвычайных ситуаций» (далее План ОНиВД), регламентирующий вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в том числе определяющий мероприятия по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи.
    2. В Банке разработан перечень критичных активов, бесперебойное функционирование которых необходимо для работы Банка, включающий как аппаратные, так и программные и информационные активы. Для каждого критичного актива предусмотрены меры по его резервированию или замене в случае выхода из строя.
    3. Непрерывность критичных процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах. Данные процедуры восстановления тестируются, как минимум, на полугодовой основе.
    4. Непрерывность работы Банка и безопасность его информационных активов в условиях неблагоприятных событий, техногенных и природных катастроф должна обеспечиваться созданием территориально удаленных Резервных комплексов и разработкой Планов перевода работы на резервные площадки.
    5. УИТ при участии ООИБ обеспечивает разработку и поддержание в актуальном состоянии Плана восстановления и непрерывности ведения деятельности. УИТ при участии ООИБ осуществляет тестирование плана и процедур восстановления.
    6. План восстановления и непрерывности ведения деятельности включает в себя:
* условия активизации Плана ОНиВД;
* процедуры восстановления деятельности;
* процедуры тестирования Плана ОНиВД;
* роли и обязанности лиц, ответственных за выполнение положений Плана ОНиВД.

### Обеспечение физической безопасности.

* + 1. Помещения Банка категорируются в зависимости от критичности размещаемых в них информационных активов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.
    2. Доступ в помещения регламентируется Положением о пропускном режиме.

### Управление рисками

* + 1. Сущность бизнеса заключается в вовлечении актива, принадлежащего Банку, в бизнес-процесс. Эта деятельность всегда подвержена рискам, так как и на сам актив, и на бизнес-процесс могут воздействовать различного рода угрозы. Угрозы реализуются через их источники и имеют соответствующую вероятность реализации. Выделяют источники угроз природного, техногенного и антропогенного характера. Источники угроз антропогенного характера могут быть как злоумышленные, так и незлоумышленные.
    2. В целях создания эффективной СУИБ, достижения адекватной защищенности информационных активов Банка в Банке реализуется деятельность по управлению рисками ИБ.
    3. Управление рисками ИБ представляет собой непрерывный процесс, в рамках которого проводится анализ того, что может произойти, а также возможных последствий, после чего принимаются решения о том, что и когда следует предпринять для уменьшения риска ИБ до приемлемого уровня путем предотвращения возникновения угроз ИБ и (или) минимизации последствий в случае их реализации.
    4. Подход к управлению рисками ИБ должен быть согласован с общим подходом к управлению рисками основной деятельности Банка. Процедура и методика оценки рисков ИБ должны быть определены и документированы. Пересмотр результатов оценки рисков ИБ должен проводиться через запланированные интервалы, включая пересмотр остаточных рисков и установленных уровней приемлемого риска ИБ.
    5. Анализ и оценка рисков нарушения информационной безопасности основываются на идентификации активов Банка, на их ценности для целей и задач Банка, на моделях угроз и нарушителей информационной безопасности Банка.
    6. Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) Банка в информационной сфере и возникновения ущерба бизнесу Банка или убытков.

## ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* 1. Общее руководство системой обеспечения информационной безопасности в Банке осуществляет Правление Банка, которое несет ответственность за общее состояние системы обеспечения информационной безопасности. Обеспечение ее функционирования возлагается на ООИБ. Ответственность за организацию и состояние обеспечения информационной безопасности в структурном подразделении Банка возлагается на соответствующего руководителя подразделения в рамках компетенции.
  2. Для координации деятельности по обеспечению информационной безопасности в Банке сформирован Отдел обеспечения информационной безопасности. ООИБ и УИТ не имеют общего куратора.
  3. Определение потребности ООИБ в кадровых ресурсах основано на анализе задач и функций, возложенных на Отдел, и заключается в установлении необходимого и достаточного количества, а также требуемой компетенции работников, выполняемой на основе:
* анализа задач и функций, возложенных на ООИБ организации банковской системы РФ;
* уровня автоматизации процессов СОИБ и централизации управления средствами автоматизации;
* прогноза возможного расширения состава задач и функций ООИБ в соответствии с планами совершенствования процессов СОИБ вследствие развития бизнес-процессов АО «Банк Акционерный Кредитный Стабильный» (АО), совершенствования процессов информатизации организации Банка, развития филиальной сети Банка.
  1. При планировании (совершенствовании) процессов СОИБ обеспечено выделение ресурсов ИБ для эффективной реализации требований законодательства РФ, нормативных актов Банка России, требований к обеспечению ИБ, установленных в Банке.
  2. ООИБ обеспечено кадровыми ресурсами, необходимыми и достаточными для реализации целевого уровня полноты для каждого управляемого процесса СОИБ.
  3. В Банке определена минимальная необходимая и достаточная численность работников ООИБ исходя из следующих показателей:
* трудозатраты на выполнение задачи и функций обеспечения ИБ;
* количество реализуемых процессов СОИБ;
* масштаб выполнения, управляемого процесса СОИБ, в том числе:
* количество подразделений (филиалов, отделений) организации Банка;
* количество АБС;
* количество работников организации банковской системы РФ;
* территориальное расположение подразделений организации БС РФ.
  1. Работники ООИБ 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 работников службы ИБ. К основным требованиям, определяющим необходимую компетенцию работников службы ИБ относится:
* наличие высшего профессионального образования в области ИБ;
* опыт работы в области ИБ не менее 1 (Одного) года;
* регулярное прохождение дополнительного (специализированного) обучения (повышения квалификации) в области ИБ;
* знание требований законодательства РФ, в том числе нормативных актов Банка России, необходимых для надлежащего выполнения функций, возложенных на работников службы ИБ;
* знание внутренних нормативно-методических и организационно-распорядительных документов организации БС РФ в области ИБ;
* осведомленность по вопросам, касающимся средств, систем и технологий обеспечения ИБ, а также способов и практик их применения.
  1. Руководители подразделений Банка, имеющих доступ к/обрабатывающих персональные данные, несут ответственность за то, что:
* применяемые меры обеспечения информационной безопасности соответствуют настоящей Политике;
* доступ к ПДн предоставлен только уполномоченным на то работникам в рамках их должностных обязанностей.
  1. Все подразделения Банка и их руководители отвечают за реализацию настоящей Политики и управление процессами ее обеспечения в рамках своей компетенции:
  2. Отдел обеспечения информационной безопасности:
* организует мероприятия по реализации настоящей Политики;
* организует процесс подготовки и актуализации настоящей Политики.
* разрабатывает нормативные, инструктивные и методические документы Банка по обеспечению информационной безопасности;
* разрабатывает планы повышения осведомленности работников Банка в вопросах ИБ;
* разрабатывает требования по защите информационных активов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;
* осуществляет оценку, выявление, контроль за рисками информационной безопасности;
* контролирует работников Банка в части соблюдения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ в рамках проверок;
* разрабатывает ежегодные планы по обеспечению ИБ;
* осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;
* эксплуатирует специализированные средства обеспечения безопасности информационных активов и обеспечивает соответствие характеристик данных средств необходимому подразделениям Банка уровню доступности;
* организует проведение единой антивирусной политики в Банке;
* организует работу и осуществляет взаимодействие с администраторами информационной безопасности подразделений Банка;
* проводит расследования фактов нарушений и инцидентов информационной безопасности[[4]](#footnote-4) и доводит результаты до сведения Председателя Правления Банка и своего куратора;
* организует обучение и тестирование персонала Банка по вопросам информационной безопасности;
* осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности;
* обеспечивает взаимодействие с уполномоченными государственными органами по вопросам лицензирования и сертификации средств криптографической защиты информации;
* проводит самооценку уровня информационной безопасности в соответствии со стандартами ЦБ РФ в области информационной безопасности;
* обеспечивает проведение оценки уровня информационной безопасности внешними организациями (аудиторами) в соответствии со стандартами ЦБ РФ в области информационной безопасности;
* разрабатывает требования в области банковских технологий, участвует в формировании решений, связанных с организацией технологических процессов, разрабатывает предложения по использованию современных банковских технологий с учетом требований по обеспечению информационной безопасности;
* обеспечивает реализацию требований информационной безопасности в разрабатываемых АБС.
  1. Управление информационных технологий:
* обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем и систем доставки;
* проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
* обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем и систем доставки.
* обеспечивает выполнение требований информационной безопасности при администрировании рабочих станций.
* разрабатывает требования в области банковских технологий, участвует в формировании решений, связанных с организацией технологических процессов, разрабатывает предложения по использованию современных банковских технологий с учетом требований по обеспечению информационной безопасности.
* обеспечивает реализацию требований информационной безопасности в разрабатываемых АБС.
* обеспечивает реализацию требований информационной безопасности в находящихся на сопровождении АБС;
* обеспечивает выполнение требований информационной безопасности в филиалах при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;
* проводит в филиалах обновление системного ПО, связанное с устранением критичных уязвимостей;
* обеспечивает доступность информационных активов филиалов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки, а также в части автоматизированных систем;
* обеспечивает в филиалах выполнение требований информационной безопасности при администрировании автоматизированных банковских систем.
  1. Служба внутреннего аудита:
* осуществляет общую проверку надежности функционирования системы внутреннего контроля за использованием автоматизированных систем, включая контроль целостности баз данных и их защиты от несанкционированного доступа и (или) использования, наличия планов действий на случай непредвиденных обстоятельств и планов непрерывности ведения деятельности в соответствии с Положением о Службе внутреннего аудита и Планом проверок, утвержденным Советом директоров.
  1. Подразделения Банка:
* совместно с ООИБ и УИТ проводят классифицирование информационных активов, владельцами которых они являются, и определяют степень их критичности;
* совместно с ООИБ, УИТ и СУР участвуют в оценке рисков реализации угроз их информационным активам;
* устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными активами, владельцами которых они являются;
* разрабатывают нормативные и инструктивные документы с учетом требований информационной безопасности;
* обеспечивают выполнение требований и процедур информационной безопасности при работе работников с информационными активами Банка.
  1. Руководитель отдела обеспечения информационной безопасности назначается Приказом Председателя Правления Банка во всех самостоятельных подразделениях Банка и обеспечивает:
* контроль соблюдения требований информационной безопасности;
* взаимодействие с ООИБ и УИТ при инцидентах информационной безопасности.

## ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ

* 1. Руководители структурных подразделений несут ответственность:
* за своевременное доведение требований внутренних нормативных документов Банка в области ИБ до работников их подразделений в части их касающейся;
* выделение информационных активов Банка, подлежащих защите, владельцем которых являются их подразделения, а также согласование заявок на доступ к данным активам;
* за выполнение работниками их подразделений требований внутренних нормативных документов Банка в области ИБ.
  1. Все работники Банка несут персональную ответственность за свои действия при работе в информационной инфраструктуре Банка и обращении с защищаемыми информационными активами Банка, а также за выполнение требований информационной безопасности, установленных настоящей Политикой и внутренними нормативными документами, разработанными на ее основе.
  2. Контроль выполнения требований настоящей Политики возлагается на ООИБ.
  3. Дополнительный контроль выполнения требований настоящей Политики могут осуществлять работники Службы внутреннего контроля путем проверки соответствия их действий требованиям законодательства РФ и внутренних документов, регулирующих деятельность по обеспечению ИБ в Банке.

## ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ПОЛИТИКУ

* 1. Настоящая Политика вступает в силу с момента утверждения Правлением Банка.
  2. Настоящая Политика должна пересматриваться не реже одного раза в год, а также в случае выявления инцидентов информационной безопасности, обнаружения новых угроз и уязвимостей, результатам аудитов информационной безопасности, значительных изменениях в организационной или технической инфраструктуре Банка, а также в случае изменения требований законодательства или выявления нарушений.

ЛИСТ СОГЛАСОВАНИЯ

«Политики информационной безопасности  
АО «Банк Акционерный Кредитный Стабильный»»

|  |  |  |  |
| --- | --- | --- | --- |
| № | Должность  согласующего лица | Фамилия,  инициалы | Отметка о согласовании,  Дата |
| 1 | Первый заместитель  Председателя Правления | Иванов И.И. |  |
| 2 | Руководитель Службы  экономической и информационной безопасности | Иванченко И.И. |  |
| 3 | Начальник отдела обеспечения информационной безопасности | Ивашенко И.И. |  |
| 4 | Руководитель Службы внутреннего контроля | Иващепкова И.И. |  |
| 5 | Начальник договорно-правового отдела | Ива И.И. |  |
| 6. | Начальник Управления  информационных технологий | Иванелов И.И |  |
| 7. | Заместитель руководителя Службы  управления рисками | Иванкевич И.И. |  |

1. К активам Банка относятся: работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.; различные виды банковской информации — платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.; банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы); банковские продукты и услуги, предоставляемые клиентам. [↑](#footnote-ref-1)
2. Вид операционного риска, процедуры управления по которому выполняются ООИБ при участии Службы управления рисками [↑](#footnote-ref-2)
3. Свидетельства выполнения деятельности по обеспечению информационной безопасности: Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ Банка [↑](#footnote-ref-3)
4. В соответствии с актуальной редакцией Частной политики мониторинга событий и управления инцидентами информационной безопасности АО «Банк Акционерный Кредитный Стабильный» [↑](#footnote-ref-4)