Утверждено
Решением Общего собрания участников
КБ «Максима» (ООО)
№ 204 от 10.01.2023г

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КБ «Максима» (ООО)

Москва
2023

Оглавление

1. Общие положения.

Настоящая Политика информационной безопасности КБ «Максима» (ООО) (далее – Политика) является основополагающим документом в области информационной безопасности и определяет систему приоритетов, направленных на достижение целей обеспечения защищённости информационных активов КБ «Максима» (ООО) (далее – Банк) в условиях наличия угроз, характерных и существенных для организаций банковской системы Российской Федерации.

Целью документа является защита интересов Банка, его клиентов и партнёров, а также обеспечение стабильной работы Банка путём определения процесса обеспечения информационной безопасности, соответствующего потребностям бизнеса и обязательствам Банка и минимизации воздействия на бизнес Банка со стороны инцидентов информационной безопасности.

Политика Банка определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, как свод инструкций, регламентов, правил, процедур, практических приёмов и руководящих принципов в области информационной безопасности, которыми руководствуется Банк в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Банке.

Основные положения и требования Политики распространяются на процессы Банка, в которых осуществляется обработка информации, содержащей сведения, составляющие банковскую и коммерческую тайну, персональные данные, иную информацию конфиденциального характера, информацию необходимую для обеспечения деятельности Банка, а также на подразделения, принимающие участие в вышеуказанных процессах.

Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в Банке, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений Банка.

Под Политикой понимается совокупность документированных управленческих решений, направленных на обеспечение безопасности во всех информационных системах Банка, включая бумажный, электронный документооборот, а также обмен речевой информацией конфиденциального характера.

Требования информационной безопасности, которые предъявляются Банком, соответствуют интересам (целям) деятельности Банка и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Банка имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере Банка составляют значимую часть операционных рисков Банка, а также имеют отношение и к иным рискам основной и управленческой деятельности Банка.

Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в Банке;
- принятия управленческих решений и разработке практических мер по обеспечению информационной безопасности и выработки комплекса, согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз информационной безопасности;
- координации деятельности структурных подразделений Банка при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению информационной безопасности;
- основополагающим документом для разработки положений, регламентов, инструкций и других внутренних документов Банка, касающихся вопросов обеспечения информационной безопасности Банка;

- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в Банке.

Необходимые требования обеспечения информационной безопасности Банка должны неукоснительно соблюдаться сотрудниками Банка и другими сторонами как это определяется положениями внутренних нормативных документов Банка, а также требованиями договоров и соглашений, стороной которых является Банк.

Политика распространяется на бизнес – процессы Банка и обязательна для применения всеми сотрудниками и руководством Банка, а также пользователями его информационных ресурсов.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Центрального банка Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается, в том числе на:

- Федеральном законе №149-ФЗ от 27.06.2006 «Об информации, информационных технологиях и о защите информации»;
- Федеральном законе №161-ФЗ от 27.06.2011 «О национальной платёжной системе»;
- Федеральном законе №152-ФЗ от 27.06.2006 «О персональных данных»;
- Федеральном законе №162-ФЗ от 27.06.2011 «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О национальной платёжной системы»;
- Федеральном законе №167-ФЗ от 27.06.2018 «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств»;
- Постановлении Правительства РФ №584 от 13.06.2012 «Об утверждении положения о защите информации в платёжной системе»;
- Положении Банка России №719-П от 23.09.2020 «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» (далее – Положение №719-П);
- Положении Банка России №747-П от 23.12.2020 «О требованиях к защите информации в платёжной системе Банка России» (далее – Положение №747-П);
- Положение Банка России №242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»;
- Указании Банка России №2831-У от 09.06.2012 «Об отчётности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платёжных систем, операторов услуг платёжной инфраструктуры, операторов по переводу денежных средств» (далее – Указание №2831-У);
- Стандартах Банка России (СТО БР ИББС);
- Рекомендациях в области стандартизации Банка России (РС БР ИББС);
- Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских_ операций защиты информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1);
- Национальный стандарт Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских_ операций защиты информации финансовых организаций. Методика оценки соответствия»;

Также Политика разработана на основе: накопленного в Банке опыта в области обеспечения информационной безопасности; результатов идентификации активов, подлежащих защите; результатов оценки рисков, с учётом особенностей бизнеса и технологий.

Политика в соответствии с рекомендациями в области стандартизации Банка России, является корпоративным документом по ИБ первого уровня, т.е. определяет высокоуровневые цели и задачи обеспечения информационной безопасности Банка.

Документами, детализирующими положения Политики применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности Банка, являются частные политики по обеспечению информационной безопасности (далее – Политики), которые являются документами по информационной безопасности второго уровня, оформляются как отдельные внутренние документы Банка, разрабатываются, согласовываются и утверждаются в соответствии с установленным в Банке порядком.

Документы, содержащие положения информационной безопасности, применяемые к процедурам (порядку выполнения действий или операций) обеспечения информационной безопасности (документы третьего уровня), содержат правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с информационной безопасностью, в рамках технологических процессов, используемых в Банке, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах (технические задания, регламенты, порядки, инструкции).

Документы, содержащие свидетельства выполненной деятельности по обеспечению информационной безопасности (документы четвёртого уровня), отражают достигнутые результаты (промежуточные и окончательные), относящиеся к обеспечению информационной безопасности Банка.

Список сокращений

№	Термин	Сокращение
1.	Автоматизированная банковская система	АБС
2.	Банковская система Российской Федерации	БС РФ
3.	Жизненный цикл	ЖЦ
4.	Информационная банковская система	ИБС
5.	Информационная безопасность	ИБ
6.	Информационная система персональных данных	ИСПДн
7.	Информационные технологии	ИТ
8.	Локальная вычислительная сеть	ЛВС
9.	Несанкционированный доступ	НСД
10.	Нерегламентированные действия в рамках предоставленных полномочий	НРД
11.	Операционная система	ОС
12.	Персональные данные	ПДн
13.	Программное обеспечение	ПО
14.	Система информационной безопасности	СИБ
15.	Система менеджмента информационной безопасности	СМИБ
16.	Система обеспечения информационной безопасности	СОИБ
17.	Система управления информационной безопасности	СУИБ
18.	Средство защиты информации	СЗИ
19.	Средство криптографической защиты информации	СКЗИ
20.	Отдел информационной безопасности	Служба ИБ
21.	Отдел автоматизации и банковских технологий	Служба ИТ

2. Термины и определения.

Автоматизированная система обработки информации – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего ПО;

- массивов (наборов, баз) данных на различных носителях;
- персонала и пользователей, объединённых по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации.

Автоматизированная банковская система – автоматизированная система, реализующая банковский технологический процесс.

Авторизация - предоставление прав доступа.

Авторизованный субъект доступа – субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Администратор информационной безопасности – лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

Актив - все, что имеет ценность для Банка, находится в его распоряжении. К активам Банка могут относиться:

- работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды банковской информации – платёжная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;
- банковские процессы (банковские платёжные технологические процессы, банковские информационные технологические процессы);
- банковские продукты и услуги, предоставляемые клиентам.

Атака на информационную систему – любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путём использования уязвимостей системы.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Аутсорсинг – передача Банком на основании договора на длительный срок сторонней (внешней) организации – поставщику услуг выполнения бизнес-функций Банка, которые являются необходимыми для её деятельности и которые в обычных условиях (без привлечения поставщика услуг) осуществлялось бы Банком самостоятельно.

Банк – Акционерное Общество КБ«Максима»(ООО).

Банковская система Российской Федерации (далее БС РФ) - Банк России, кредитные организации, а также представительства иностранных банков.

Банковский информационный технологический процесс - часть банковского технологического процесса, реализующая действия с информацией, необходимые для выполнения Банком своих функций, и не являющаяся банковским платёжным технологическим процессом.

Банковский платёжный технологический процесс - часть банковского технологического процесса, реализующая действия с информацией, связанные с осуществлением переводов денежных средств, платёжного клиринга и расчёта, и действия с архивами указанной информации.

Банковский технологический процесс - технологический процесс, реализующий операции по изменению и (или) определению состояния активов Банка, используемых при функционировании или необходимых для реализации банковских услуг. В зависимости от вида деятельности выделяют: банковский платёжный технологический процесс, банковский информационный технологический процесс и др.

Безопасность – состояние защищённости интересов (целей) Банка в условиях угроз.

Безопасность информации – защищённость информации от нежелательного (для соответствующих субъектов информационных отношений) её разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного её тиражирования.

Безопасность информационной технологии – защищённость технологического процесса обработки информации.

Безопасность любого ресурса информационной системы – складывается из обеспечения

трёх его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Безопасность субъектов информационных отношений – защищённость жизненно важных интересов субъектов информационных отношений от нанесения им материального, морального или иного вреда путём воздействия на информацию и/или средства её обработки и передачи. Безопасность достигается проведением единой концепции в области охраны и защиты важных ресурсов, системой мер экономического, организационного и иного характера, адекватных угрозам жизненно важным интересам.

Внешний воздействующий фактор – воздействующий фактор, внешний по отношению к объекту информатизации.

Внутренний воздействующий фактор – воздействующий фактор, внутренний по отношению к объекту информатизации.

Вредоносные программы – программы или изменённые программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

Выделенное помещение – помещение для размещения технических средств защищённого объекта информатизации, а также помещение, предназначенное для проведения семинаров, совещаний, бесед и других мероприятий, в котором циркулирует конфиденциальная речевая информация.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать. [ГОСТ Р 52069.0-2013] – под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие её копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотоплёнка.

Документация - совокупность взаимосвязанных документов, объединённых общей целевой направленностью**.**

Допустимый риск нарушения ИБ - риск нарушения ИБ, предполагаемый ущерб, который Банк в данное время и в данной ситуации готов принять.

Доступ к информации – ознакомление с информацией или получение возможности её обработки. Доступ к информации регламентируется её правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществлённый с нарушениями требований её правового режима, рассматривается как несанкционированный доступ.

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Доступность информации – важнейшее свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

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

Естественные угрозы – это угрозы, вызванные воздействиями на информационную

систему и её компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

Жизненно важные интересы **–** совокупность потребностей, удовлетворение которых необходимо для надёжного обеспечения существования и возможности прогрессивного развития субъекта.

Замысел защиты **–** основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации и объекта.

Защита информации **–** деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

Защита информации от несанкционированного доступа **–** деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Защищаемая информация **–** информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями документов или требованиями, устанавливаемыми собственником информации.

Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ Банка.

Злоумышленник **–** нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Идентификация - процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал **–** электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта информация ограниченного распространения, передаваемая, хранимая, обрабатываемая или обсуждаемая в выделенных помещениях.

Информация **–** сведения о предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность **–** безопасность, связанная с угрозами в информационной сфере. Защищённость достигается обеспечением совокупности свойств ИБ – доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) Банка.

Информационная инфраструктура - система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам.

Информационные ресурсы **–** отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

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

Информационная система Банка **–** организационно упорядоченная совокупность документов (массивов документов), независимо от формы их представления, и информационных технологий, в том числе с использованием вычислительной техники и связи. Информационная система Банка включает в себя множество всех документов, существующих в Банке.

Информационные способы нарушения безопасности информации **–** включают:

- противозаконный сбор, распространение и использование информации;
- манипулирование информацией (дезинформация, сокрытие или искажение информации);
- незаконное копирование информации (данных и программ);
- незаконное уничтожение информации;

- хищение информации из баз и банков данных;
- нарушение адресности и оперативности информационного обмена;
- нарушение технологии обработки данных и информационного обмена.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

- нарушение или возможное нарушение работы средств защиты информации в составе СОИБ Банка;
- нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний, регулирующих и надзорных органов, внутренних документов Банка в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ Банка;
- нарушение или возможное нарушение в выполнении банковских технологических процессов Банка;
- нанесение или возможное нанесение ущерба Банку и (или) её клиентам.

Инцидент ИБ при осуществлении переводов денежных средств *– событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:*

- несанкционированные переводы денежных средств, которые привели или могут привести к:
  - осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
  - несвоевременности осуществления переводов денежных средств;
  - осуществлению переводов денежных средств с использованием искажённой информации, содержащейся в распоряжениях на осуществление переводов денежных средств (реквизитов платежей);
- деструктивные воздействия на информационную инфраструктуру, используемую для осуществления переводов денежных средств, которые привели или могут привести к нарушению непрерывности оказания платёжных услуг.

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

Искусственные угрозы – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и её элементов, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Классификация информационных активов - разделение существующих информационных активов Банка по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

Комплекс средств автоматизации автоматизированной банковской системы – совокупность всех компонентов автоматизированной банковской системы организации БС РФ за исключением людей.

Компьютерная информация – информация в виде:

- записей в памяти компьютеров, электронных устройствах, на машинных носителях (элементы, файлы, блоки, базы данных, микропрограммы, прикладные и системные программы, пакеты и библиотеки программ, микросхемы, программно-информационные комплексы и др.), обеспечивающих функционирование объекта информатизации (сети);
- сообщений, передаваемых по сетям передачи данных;
- программно-информационного продукта, являющегося результатом генерации новой или обработки исходной документированной информации, представляемого непосредственно на экранах дисплеев, на внешних носителях данных (магнитные диски, магнитные ленты, оптические диски, дискеты, бумага для распечатки и т.п.) или через сети передачи данных;
- электронных записей о субъектах прав.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Границей контролируемой зоны могут являться:

- периметр охраняемой территории Банка;
- ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

В отдельных случаях на период обработки техническими средствами секретной информации (проведения закрытого мероприятия) контролируемая зона временно может устанавливаться большей, чем охраняемая территория Банка. При этом должны приниматься организационно-режимные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

Конфиденциальность информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

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

Корпоративная информационная система – автоматизированная система обработки информации Банка.

Лицензия в области защиты информации – разрешение на право проведения тех или иных работ в области защиты информации.

Менеджмент - скоординированная деятельность по руководству и управлению.

Модель нарушителя информационной безопасности (модель нарушителя ИБ) – 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. Расчёт данной модели отражён в РС БР ИББС-2.2-2009.

Модель угроз информационной безопасности (модель угроз ИБ) – описание актуальных 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.

Морально-этические меры защиты информации – традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, однако, их несоблюдение ведёт обычно к падению авторитета, престижа человека, группы лиц или Банка. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и написанные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Мониторинг ИБ - постоянное наблюдение за объектами и субъектами, влияющими на ИБ

Банка, а также сбор, анализ и обобщение результатов наблюдений.

Нарушитель – это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещённых ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

Национальная платёжная система – совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платёжных агентов (субагентов), платёжных агентов, организаций федеральной почтовой связи при оказании ими платёжных услуг в соответствии с законодательством Российской Федерации, операторов платёжных систем, операторов услуг платёжной инфраструктуры (субъекты национальной платёжной системы).

Неплатёжная информация – информация, необходимая для функционирования Банка, не являющаяся платёжной информацией, которая может включать в себя, например, данные статистической отчётности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ – доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Несанкционированный перевод денежных средств – перевод денежных средств лицами, не обладающими правом распоряжения денежными средствами.

Область действия СОИБ - совокупность информационных активов и элементов информационной инфраструктуры Банка.

Обработка риска нарушения ИБ - процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

Объект – пассивный компонент системы, единица ресурса информационной системы, доступ к которому регламентируется правилами разграничения доступа.

Объект защиты – информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Объект среды информационного актива - материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения.

Оператор по переводу денежных средств – организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Оператор платёжной системы – организация, определяющая правила платёжной системы, а также выполняющая иные обязанности, предусмотренные Федеральным законом №161-ФЗ.

Организационно-правовые способы нарушения безопасности информации – включают:

- закупку несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
- невыполнение требований законодательства или нормативных актов и задержки в разработке и принятии необходимых нормативных правовых и технических документов в области безопасности информации.

Организационные меры защиты – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности, циркулирующей в ней информации.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Осознание необходимости обеспечения ИБ - понимание руководством Банка необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению ИБ, а также поддерживать эту деятельность адекватно прогнозу.

Остаточный риск нарушения ИБ - риск, остающийся после обработки риска нарушения ИБ.

Оценка риска нарушения ИБ - систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов Банка на всех стадиях их жизненного цикла.

Оценка соответствия информационной безопасности (оценка соответствия ИБ) – систематический и документируемый процесс получения свидетельств деятельности Банка по реализации требований ИБ и установлению степени выполнения в Банке критериев оценки (аудита) ИБ. Оценка соответствия должна осуществляться Банком с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации N 79.

Пароль – служебное слово, которое считается известным узкому кругу лиц (одному лицу) и используется для ограничения доступа к информации, в помещение, на территорию.

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

План работ по обеспечению ИБ - документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению ИБ Банка, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей.

Платёжная информация – информация, на основании которой совершаются операции, связанные с осуществлением переводов денежных средств.

Пользователь – субъект, пользующийся информацией, полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Правила платёжной системы – документ (документы), содержащий (содержащие) условия участия в платёжной системе, осуществления перевода денежных средств, оказания услуг платёжной инфраструктуры и иные условия, определяемые оператором платёжной системы в соответствии с Федеральным законом №161-ФЗ.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Правовые меры защиты информации – действующие в государстве законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному её использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Программно-математические способы нарушения безопасности информации – включают:

- внедрение программ-вирусов;
- внедрение программных закладок как на стадии проектирования системы (в том числе путём заимствования «заражённого» закладками программного продукта), так и на стадии её эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам её защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

Радиоэлектронные способы нарушения безопасности информации – включают:

- перехват информации в технических каналах её утечки (побочных электромагнитных излучений, создаваемых техническими средствами обработки и передачи информации, наводок в коммуникациях (сети электропитания, заземления, радиотрансляции, пожарной и

охранной сигнализации и т.д.) и линиях связи, путём прослушивания конфиденциальных разговоров с помощью акустических, виброакустических и лазерных технических средств разведки, прослушивания конфиденциальных телефонных разговоров, визуального наблюдения за работой средств отображения информации);

- перехват и дешифрование информации в сетях передачи данных и линиях связи;
- внедрение электронных устройств перехвата информации в технические средства и помещения;
- навязывание ложной информации по сетям передачи данных и линиям связи, радиоэлектронное подавление линий связи и систем управления.

Разграничение доступа к ресурсам – это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Регистрация - фиксация данных о совершенных действиях (событиях).

Ресурс - актив Банка, который используется или потребляется в процессе выполнения некоторой деятельности.

Ресурс ИБ – кадровые ресурсы (персонал) службы ИБ и финансовые средства, необходимые для планирования, реализации, выполнения, проверки и совершенствования процессов СОИБ с целью обеспечения целевого уровня обеспечения ИБ.

Ресурсное обеспечение ИБ – процесс управления, обеспечивающий определение потребностей в ресурсах ИБ и контроль эффективности использования ресурсов ИБ.

Ресурс ПДн - совокупность ПДн, обрабатываемых в Банке с использованием или без использования средств автоматизации и АБС, в том числе ИСПДн, объединённых общими целями обработки.

Риск - мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Риск нарушения ИБ - риск, связанный с угрозой ИБ.

Роль - заранее определённая совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

- к субъектам относятся лица из числа руководителей Банка, её персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.
- объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

Свидетельства выполнения деятельности по обеспечению ИБ - документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ Банка.

Система информационной безопасности – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности Банка.

Система менеджмента информационной безопасности – часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

Система обеспечения информационной безопасности – совокупность СИБ и СМИБ организации банковской системы Российской Федерации.

Спам – общее наименование не запрошенных пользователями электронных посланий и рекламных писем, рассылаемых в информационно-телекоммуникационной сети «Интернет» по ставшим известными рассылающей стороне адресам пользователей.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Субъект – активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Субъекты информационных отношений – государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

Технические (аппаратно-программные) средства защиты – различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Технологический процесс - процесс, реализующий некоторую технологию.

Технология - совокупность взаимосвязанных методов, способов, приёмов предметной деятельности

Технология обеспечения информационной безопасности – определённое распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников Банка по обеспечению комплексной защиты информационных ресурсов Банка.

Угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования объекта и нарушения свойств защищаемой информации или других ресурсов объекта.

Угроза безопасности информации – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации.

Угроза интересам субъектов информационных отношений – потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие информационной системы может привести к нанесению ущерба интересам данных субъектов.

Уровень защиты (класс и категория защищённости) – характеристика, описываемая в нормативных документах определённой группой требований к данному классу и категории защищённости.

Уровень зрелости выполнения процесса СОИБ – мера оценки полноты, адекватности и эффективности выполнения процесса СОИБ.

Участники платёжной системы – организации, присоединившиеся к правилам платёжной системы в целях оказания услуг по переводу денежных средств.

Ущерб - утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Банка или другой вред активам и (или) инфраструктуре Банка, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Уязвимость автоматизированной системы – любая характеристика автоматизированной системы, использование которой может привести к реализации угрозы.

Уязвимость информации – подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

Уязвимость субъекта информационных отношений – потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки.

Физические меры защиты – это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации и другим ресурсам информационной системы, а также технические средства визуального наблюдения, связи и охранной сигнализации.

Физические способы нарушения безопасности информации – включают:

- уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, целенаправленное внесение в них неисправностей;

- уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;
- хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа;
- воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз безопасности информации;
- диверсионные действия по отношению к объектам безопасности информации (взрывы, поджоги, технические аварии и т.д.).

Физический канал утечки информации – неконтролируемый физический путь от источника информации за пределы Банка или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное (несанкционированное) овладение нарушителем защищаемой информацией.

Целостность информации – свойство информации, заключающееся в её существовании в неискажённом виде (неизменном по отношению к некоторому фиксированному её состоянию).

Цель защиты информации – предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты информационной системы, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

3. Объекты защиты.

Основными объектами системы ИБ в Банке являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую, банковскую тайну, персональные данные или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Банка, независимо от формы и вида её представления. Информация, находящаяся на файл-серверах, базы данных, носители информации и прочая информация, включая пароли пользователей;
- процессы обработки информации в информационной системе Банка, информационные технологии, регламенты и процедуры сбора, систематизация, накопление, уточнение, использование, хранение, блокирование, уничтожение и передача информации, пользователи и администраторы АБС;
- сотрудники Банка, являющиеся разработчиками и пользователями информационных систем Банка;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты АБС.

3.1 Структура, состав и размещение основных объектов защиты, информационные связи.

Информационная среда Банка является распределённой структурой, объединяющей информационные подсистемы Банка в единую информационную систему Банка.

К основным особенностям информационной среды Банка, относятся:

- объединение в единую систему технических средств обработки;
- значительное расширение сферы использования автоматизированных систем обработки информации;
- разнообразие решаемых задач (от подготовки и отправки платежей до внедрения ДБО (дистанционное банковское обслуживание)) режимы автоматизированной обработки

информации с широким совмещением выполнения информационных запросов различных пользователей АБС;

- значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных (подготовка отчётности, подготовка рейсов, отправка денежных переводов и др.);
- объединение в единую базу данных информации различного назначения, принадлежности и уровней конфиденциальности;
- абстрагирование владельцев данных от физических структур и места размещения данных (информации);
- наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации) (информационно-телекоммуникационная сеть «Интернет», система «Банк-Клиент»);
- необходимость обеспечения функционирования Банка (в соответствии с внутренними документами Банка);
- интенсивность информационных потоков между подразделениями Банка;
- разнообразие категорий доступа персонала к системам.

В этих условиях резко возрастает уязвимость информации и одним из важнейших элементов информационной среды Банка становится корпоративная информационная система, в которой обрабатываются и накапливаются значительные объёмы информации, совместно используемой различными пользователями, различной организационной принадлежности.

3.2 Категории информационных ресурсов, подлежащих защите.

В АБС Банка циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного доступа (служебная, коммерческая, банковская информация, персональные данные) и открытые сведения.

Защите подлежит вся информация и информационные ресурсы Банка, независимо от ее представления и местонахождения в информационной среде Банка:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с Федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
- сведения, составляющие банковскую тайну, доступ к которым ограничен в соответствии с Федеральным законом от 02.12.1990 №395-1 «О банках и банковской деятельности»;
- сведения о частной жизни граждан (персональные данные), доступ к которым ограничен в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- открытая информация, необходимая для обеспечения нормального функционирования Банка.

4 Цели и задачи информационной безопасности.

4.1 Интересы затрагиваемых субъектов информационных отношений.

Субъектами информационных отношений при обеспечении ИБ Банка являются:

- Банк, как собственник информационных ресурсов; подразделения Банка, участвующие в информационном обмене;
- руководство и сотрудники структурных подразделений Банка, в соответствии с возложенными на них функциями;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе Банка;

- другие юридические и физические лица, задействованные в обеспечении выполнения Банком своих функций (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (её доступности);
- достоверности (полноты, точности, адекватности, целостности) информации;
- конфиденциальности (сохранения в тайне) определённой части информации; защиты от навязывания им ложной (недостоверной, искажённой) информации;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты части информации от незаконного её тиражирования (защиты авторских прав, прав собственника информации и т.п.).

4.2 Цели защиты.

Основной целью обеспечения ИБ в Банке является защита субъектов информационных отношений, интересы которых затрагиваются при создании и функционировании АБС, от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации Банка, правовой риск, операционный риск и т.д.).

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и самой ИБС, её обрабатывающей:

- доступности информации и операций с ней для зарегистрированных пользователей, устойчивого функционирования АБС Банка, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;
- обеспечения информации конфиденциального характера, хранимой, обрабатываемой в АБС и передаваемой по каналам связи;
- целостности и аутентичности информации, хранимой и обрабатываемой в АБС и передаваемой по каналам связи;
- ответственности субъектов информационных отношений за допущенные нарушения порядков и инструкций безопасности, повлёкшие за собой ущерб для одного или нескольких субъектов информационных отношений;
- предотвращение и (или) снижение ущерба от инцидентов ИБ.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству значимых угроз методами и средствами.

4.3 Основные задачи системы обеспечения безопасности информации Банка.

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения ИБ Банка должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Банка;

- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования АБС Банка посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Банка (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих должностных обязанностей), то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- защиту от несанкционированной модификации используемых в корпоративной информационной системе Банка программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- обеспечение живучести шифровальных (криптографических) средств защиты информации;
- установление единых требований по обеспечению ИБ Банка;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ Банка.

4.4 Основные пути решения задач системы защиты.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учётом всех подлежащих защите ресурсов системы (информации, задач, каналов связи, серверов, автоматизированных рабочих мест);
- регламентацией процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений Банка, использующих АБС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АБС, на основе утверждённых внутренних документов по вопросам обеспечения ИБ;
- полнотой, реальной выполнимостью и непротиворечивостью требований регламентирующих документов Банка по вопросам обеспечения ИБ;
- назначением и подготовкой должностных лиц (сотрудников Банка), ответственных за организацию и осуществление практических мероприятий по обеспечению ИБ и процессов её обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих должностных обязанностей полномочиями по доступу к ресурсам Банка;
- чётким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АБС, требований регламентирующих внутренних документов по вопросам обеспечения ИБ;
- персональной ответственностью за свои действия каждого сотрудника, участвующего в рамках своих должностных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам Банка;
- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;
- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищённости компонентов АБС;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- разграничением потоков информации, предусматривающим предупреждение попадания информации более высокого уровня конфиденциальности на носители и в файлы с более низким уровнем конфиденциальности, а также запрещением передачи информации ограниченного распространения по незащищённым каналам связи;
- эффективным контролем со стороны Службы ИБ за соблюдением сотрудниками подразделений Банка требований по обеспечению ИБ;
- юридической защитой интересов Банка при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;
- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информации.

4.5 Требования к защите информации в платёжной системе Банка.

Правила платёжной системы должны предусматривать, в том числе следующие требования к защите информации:

а) создание и организация функционирования структурного подразделения по защите информации или назначение должностных лиц (сотрудников Банка), ответственных за организацию защиты информации;

б) включение в должностные обязанности сотрудников Банка, участвующих в обработке информации, обязанности по выполнению требований к защите информации;

в) осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем;

г) проведение анализа рисков нарушения требований к защите информации и управление такими рисками;

д) разработка и реализация систем защиты информации в информационных системах;

е) применение средств защиты информации (шифровальные (криптографические) средства, средства защиты информации от несанкционированного доступа, средства антивирусной защиты, средства межсетевого экранирования, системы обнаружения вторжений, средства контроля (анализа) защищённости);

ж) выявление инцидентов, связанных с нарушением требований к защите информации, реагирование на них;

з) обеспечение защиты информации при использовании информационно-телекоммуникационных сетей общего пользования;

и) определение порядка доступа к объектам инфраструктуры платёжной системы, обрабатывающим информацию;

к) организация, проведение оценки соответствия требований к защите информации на собственных объектах инфраструктуры не реже 1 раза в 2 года, согласно Положению №719-П.

л) организация ежегодного тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры

м) Организация проведения оценки соответствия в пределах выделенных сегментов (группы сегментов) вычислительных сетей требований к защите информации в платёжной системе Банка России не реже 1 раза в 2 года, согласно Положению №747-П по ГОСТ Р 57580.

Банк к инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, относят события, которые возникли вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и (или) условий осуществления (требований к

осуществлению) перевода денежных средств, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, которые установлены оператором по переводу денежных средств и доведены им до клиента, и которые:

- приводят к несвоевременности (к нарушению сроков, установленных законодательством Российской Федерации, правилами платёжных систем и (или) договорами, заключаемыми клиентами, операторами по переводу денежных средств, операторами услуг платёжной инфраструктуры, операторами платёжных систем, банковскими платёжными агентами (субагентами), участниками платёжных систем) осуществления переводов денежных средств;
- приводят или могут привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
- приводят к осуществлению переводов денежных средств с использованием искажённой информации, содержащейся в распоряжениях клиентов, распоряжениях участников платёжной системы, распоряжениях клирингового центра.

5 Основные угрозы безопасности информации Банка.

Модели ИБ (угроз и нарушителей) предназначены отражать будущее, вследствие чего они носят прогнозный характер. Модели ИБ разрабатываются на основе фактов прошлого и опыта, но ориентированы на будущее. При разработке модели используется имеющий опыт и знания.

В связи с тем, что со временем угрозы, их источники и риски могут изменяться, то следует периодически пересматривать модели.

Модель угроз и нарушителя должна учитывать требования законодательства Российской Федерации в области ИБ, разработки ведущих специалистов банковской системы, Базы данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru/threat), а также международный опыт в этой сфере.

В области обеспечения безопасности персональных данных Банк учитывает в своей работе Указание Банка России №3889-У от 10.12.2015 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

5.1 Угрозы безопасности информации и их источники.

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и её компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

Искусственные угрозы – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и её элементов, ошибками в действиях персонала и т.п.;
- *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

Основными источниками угроз безопасности информации Банка являются:

- непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также

процедур, правил и требований ИБ и другие действия сотрудников подразделений Банка при эксплуатации АБС, приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

- преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия сотрудников подразделений Банка, допущенных к работе с АБС Банка, а также сотрудников подразделений Банка, отвечающих за обслуживание и администрирование программного и аппаратного обеспечения, средств защиты и обеспечения ИБ;
- деятельность преступных групп, экономических структур, а также отдельных лиц по добыванию и/или искажению информации, нарушению работоспособности системы в целом или её отдельных компонентов;
- воздействия из внутренней сети Банка со стороны сотрудников подразделений Банка, а также удалённое несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (информационно-телекоммуникационная сеть «Интернет»), используя недостатки протоколов обмена, средств защиты и разграничения удалённого доступа к ресурсам Банка;
- ошибки, допущенные при проектировании АБС и её системы защиты, ошибки в ПО, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) АБС;
- аварии, стихийные бедствия и прочие форс-мажорные обстоятельства.

Наиболее значимыми угрозами безопасности информации Банка (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационной системы Банка, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов Банка, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих банковскую или коммерческую тайну, а также персональные данные.

Пользователи, операторы и другие сотрудники Банка, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих внутренних документов Банка.

5.2 Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации.

Сотрудники Банка, зарегистрированные как легальные пользователи информационной системы Банка или обслуживающие её компоненты, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих внутренних документов Банка.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации Банка (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов АБС Банка или разрушению информационных, или программно-технических ресурсов;
- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие её общедоступной;

- разглашение, передача или утрата атрибутов разграничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);
- игнорирование организационных ограничений (установленных правил) при работе с информационными ресурсами;
- проектирование архитектуры систем, технологий обработки данных, представляющими опасность для функционирования информационной системы Банка и безопасности информации;
- пересылка данных и документов по ошибочному адресу (устройства);
- ввод ошибочных данных;
- неумышленная порча носителей информации;
- неумышленное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы устройств или программ;
- заражение компьютеров вирусами;
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности компонентов информационной системы Банка или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты.

5.3 Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации.

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы Банка из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

- умышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы Банка или разрушению информационных, или программно-технических ресурсов;
- действия по дезорганизации функционирования информационной системы Банка, хищение документов и носителей информации;
- несанкционированное копирование документов и носителей информации, умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- перехват данных, передаваемых по каналам связи и их анализ;
- хищение производственных отходов (распечаток документов, записей, носителей информации и т.п.);
- незаконное получение атрибутов разграничения доступа (агентурным путём, используя халатность пользователей, путём подделки, подбора и т.п.);
- несанкционированный доступ к ресурсам АБС Банка с рабочих станций сотрудников;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов корпоративной информационной системы Банка;
- незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
- применение подслушивающих устройств, дистанционная фото- и видео съёмка для несанкционированного съёма информации;

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические средства, непосредственно не участвующие в информационном обмене (сети питания).

5.4 Неформальная модель возможных нарушителей.

Нарушитель – это лицо, которое предприняло попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник – нарушитель, действующий намеренно из корыстных, идейных или иных побуждений.

Система обеспечения ИБ Банка строится исходя из предположений о следующих возможных типах нарушителей в системе (с учётом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

- *некомпетентный* (невнимательный) пользователь – сотрудник Банка (или подразделения другой организации, являющийся сотрудником информационной системы Банка), который может предпринимать попытки выполнения запрещённых действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства;
- *любитель* – сотрудник Банка (или подразделения другого организации, являющийся зарегистрированным пользователем информационной системы Банка), пытающийся нарушить систему защиты без корыстных целей или злого умысла, или для самоутверждения. Для преодоления системы защиты и совершения запрещённых действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешённых средств). Кроме этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;
- *внутренний злоумышленник* – сотрудник Банка (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесённую обиду, возможно в сговоре с лицами, не являющимися сотрудниками Банка. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Банка;
- *внешний злоумышленник* – постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Банка.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников Банка:

- зарегистрированные пользователи информационной системы Банка;
- сотрудники Банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы Банка, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы Банка;
- сотрудники подразделений Банка, задействованные в разработке и сопровождении программного обеспечения;
- сотрудники Службы безопасности Банка и Службы ИБ;
- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники Банка;
- представители организаций, взаимодействующих по вопросам технического обеспечения Банка;
- клиенты Банка;
- посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
- представители конкурирующих организаций;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в корпоративную информационную систему Банка из внешних телекоммуникационных сетей (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников Банка имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определённых полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих внутренних документов.

Особую категорию составляют администраторы различных автоматизированных систем, имеющих практически неограниченный доступ к информационным ресурсам компонентов АБС Банка. Численность данной категории пользователей должна быть минимальной, а их действия должны находиться под обязательным контролем со стороны Службы ИБ.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные во время работы в Банке знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры являются наиболее агрессивным источником внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников Банка всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в автоматизированных системах обработки информации. Они представляют наибольшую угрозу при взаимодействии с работающими или уволенными сотрудниками Банка и криминальными структурами.

Организации, занимающиеся разработкой, поставкой, ремонтом и обслуживанием оборудования или информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам.

Конкурирующие организации, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к ресурсам информационной системы Банка.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

- нарушитель скрывает свои несанкционированные действия от других сотрудников Банка;
- несанкционированные действия могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж и другие средства, и методы для достижения стоящих перед ним целей.

5.5 Менеджмент инцидентов ИБ.

Менеджмент инцидентов ИБ, включают в себя:

- сбор информации о событиях ИБ;
- выявление и анализ инцидентов ИБ;
- расследование инцидентов ИБ;
- оперативное реагирование на инцидент ИБ;
- минимизация негативных последствий инцидентов ИБ;
- оперативное доведение до руководства Банка информации по наиболее значимым инцидентам ИБ и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты ИБ;
- выполнение принятых решений по всем инцидентам ИБ в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению ИБ по результатам рассмотрения инцидентов ИБ;
- повышение уровня знаний персонала Банка в вопросах обеспечения ИБ;
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Банка и информации, обрабатываемой в них;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение ИБ на стадиях жизненного цикла автоматизированных систем Банка, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
- обеспечение ИБ при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения Банка.

5.6 Утечка информации по техническим каналам.

При проведении мероприятий и эксплуатации технических средств возможны следующие каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

- побочные электромагнитные излучения информативного сигнала от технических средств Банка и линий передачи информации;
- наводки информативного сигнала, обрабатываемого техническими средствами корпоративной информационной системы Банка, на провода и линии, выходящие за пределы контролируемой зоны Банка, в т.ч. на цепи заземления и электропитания;
- электрические сигналы или радиоизлучения, обусловленные воздействием на средства передачи информации высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, по эфиру и проводам, либо сигналов промышленных радиотехнических устройств (радиовещательные, радиолокационные станции, средства радиосвязи и т.п.), и модуляцией их информативным сигналом;

- радиоизлучения или электрические сигналы от внедрённых в помещения Банка специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключённых к каналам связи или техническим средствам обработки информации;
- акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счёт микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации;
- вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений;
- просмотр информации с экранов дисплеев и других средств её отображения с помощью оптических средств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена, в том числе электромагнитное, через специально внедрённые электронные и программные средства («закладки»).

Перехват информации ограниченного распространения или воздействие на неё с использованием технических средств может вестись непосредственно из зданий, расположенных в непосредственной близости от объектов Банка, мест временного пребывания, заинтересованных в перехвате информации или воздействии на неё лиц при посещении ими подразделений Банка, а также с помощью скрытно устанавливаемой в районах важнейших объектов и на их территориях автономной автоматической аппаратуры.

В качестве аппаратуры разведок или воздействия на информацию и технические средства могут использоваться:

- средства разведки для перехвата радиоизлучений от средств радиосвязи, радиорелейных станций, и приёма сигнала от автономных автоматических средств разведки и электронных устройств перехвата информации («закладок»);
- стационарные средства, размещаемые в зданиях;
- портативные возимые и носимые средства, размещаемые в зданиях, в транспортных средствах, а также носимые лицами, ведущими разведку;
- автономные автоматические средства, скрытно устанавливаемые на объектах защиты или поблизости от них.

Стационарные средства обладают наибольшими энергетическими, техническими и функциональными возможностями. В то же время они, как правило, удалены от объектов защиты и не имеют возможности подключения к линиям, коммуникациям и сооружениям. Портативные средства могут использоваться непосредственно на объектах защиты или поблизости от них и могут подключаться к линиям и коммуникациям, выходящим за пределы контролируемой территории.

Кроме перехвата информации техническими средствами разведки возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны.

Такого рода утечка информации возможна в следствии:

- непреднамеренного прослушивания без использования технических средств разговоров, ведущихся в выделенном помещении, из-за недостаточной звукоизоляции его ограждающих конструкций, систем вентиляции и кондиционирования воздуха;

- случайного прослушивания телефонных переговоров при проведении профилактических работ на АТС, кроссах, кабельных коммуникациях с помощью контрольной аппаратуры;
- просмотра информации с экранов дисплеев и других средств ее отображения.

6 Общие принципы оценки рисков нарушения информационной безопасности.

Информационные активы Банка рассматриваются в совокупности с соответствующими им объектами среды. При этом обеспечение свойств ИБ для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды.

Угрозы ИБ реализуются их источниками (источниками угроз ИБ), которые могут воздействовать на объекты среды информационных активов Банка. В случае успешной реализации угрозы ИБ информационные активы теряют часть или все свойства ИБ.

Оценка рисков нарушения ИБ проводится для типов информационных активов (типов информации), входящих в предварительно определённую область оценки. Для оценки рисков нарушения ИБ предварительно определяются и документально оформляются:

- полный перечень типов информационных активов, входящих в область оценки;
- полный перечень типов объектов среды, соответствующих каждому из типов информационных активов области оценки;
- модель угроз ИБ, описывающую угрозы ИБ для всех выделенных типов объектов среды на всех уровнях иерархии информационной инфраструктуры Банка.

Формирование перечня источников угроз и моделей угроз проводится с учётом положений комплекса стандартов Банка России - СТО БР ИББС.

Перечень типов информационных активов формируется на основе результатов выполнения классификации информационных активов. Состав перечня типов информационных активов (классификация информации) соответствует нормам законодательства РФ, в том числе нормативным актам Банка России. В Банке используется следующий перечень типов информационных активов:

- информация ограниченного доступа;
- информация, содержащая сведения, составляющие банковскую тайну;
- платёжная информация (информация, предназначенная для проведения расчётных, кассовых и других банковских операций, и учётных операций);
- информация, содержащая сведения, составляющие коммерческую тайну;
- персональные данные;
- управляющая информация платёжных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации);
- открытая (общедоступная) информация.

Формирование перечней типов объектов среды выполняется в соответствии с иерархией уровней информационной инфраструктуры Банка, определённой в комплексе стандартов Банка России - СТО БР ИББС.

Указанные перечни содержат следующие типы объектов среды:

- линии связи и сети передачи данных;
- сетевые программные и аппаратные средства, в том числе сетевые серверы;
- файлы данных, базы данных, хранилища данных;
- носители информации, в том числе бумажные носители;
- прикладные и общесистемные программные средства;
- программно-технические компоненты автоматизированных систем;
- помещения, здания, сооружения;
- платёжные и информационные технологические процессы.

Риск нарушения ИБ определяется на основании качественных оценок:

- степени возможности реализации угроз ИБ (далее - СВР угроз ИБ) выявленными и (или) предполагаемыми источниками угроз ИБ в результате их воздействия на объекты среды рассматриваемых типов информационных активов;
- степени тяжести последствий от потери свойств ИБ для рассматриваемых типов информационных активов (далее - СТП нарушения ИБ).

Оценка СВР угроз ИБ и СТП нарушения ИБ базируется на экспертной оценке. Для оценки СТП нарушения ИБ дополнительно привлекаются сотрудники профильных подразделений, использующих рассматриваемые типы информационных активов. Взаимодействие сотрудников указанных подразделений осуществляется в рамках постоянно действующей или создаваемой на время проведения оценки рисков нарушения ИБ рабочей группы.

Для проведения оценки рисков нарушения ИБ Банком выполняются процедуры, предусмотренные Методикой оценки рисков нарушения ИБ, которая изложена в Рекомендациях в области стандартизации Банка России (РС БР ИББС-2.2-2009).

7 Общие принципы обеспечения информационной безопасности Банка.

7.1 Общие принципы обеспечения информационной безопасности Банка.

При построении АБС Банк руководствуется рядом основополагающих принципов:

- **Своевременность обнаружения проблем.**

Банк должен своевременно обнаруживать проблемы, потенциально способные повлиять на его бизнес-цели.

- **Прогнозируемость развития проблем.**

Банк должен выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

- **Оценка влияния проблем на бизнес-цели.**

Банк должен адекватно оценивать степень влияния выявленных проблем на его бизнес-цели.

- **Адекватность защитных мер.**

Банк должен выбирать защитные меры, адекватные моделям угроз и нарушителей, с учётом затрат на реализацию таких мер и объёма возможных потерь от выполнения угроз.

- **Эффективность защитных мер.**

Банк должен эффективно реализовывать принятые защитные меры.

- **Использование опыта при принятии и реализации решений.**

Банк должен накапливать, обобщать и использовать как свой опыт, так и опыт других кредитных организаций на всех уровнях принятия решений и их исполнения.

- **Непрерывность принципов безопасного функционирования.**

Банк должен обеспечивать непрерывность реализации принципов безопасного функционирования.

- **Контролируемость защитных мер.**

Банк должен применять только те защитные меры, правильность работы которых может быть проверена, при этом Банк должен регулярно оценивать адекватность защитных мер и эффективность их реализации с учётом влияния защитных мер на бизнес-цели Банка.

7.2 Специальные принципы обеспечения информационной безопасности Банка.

Реализация специальных принципов обеспечения ИБ направлена на повышение уровня зрелости процессов управления ИБ в Банке.

- **Определённость целей.**

Функциональные цели и цели ИБ Банка определены Политикой.

- **Знание своих клиентов и служащих.**

Банк должен обладать информацией о своих клиентах, тщательно подбирать персонал (сотрудников), вырабатывать и поддерживать корпоративную этику, что создаёт благоприятную доверительную среду для деятельности Банка по управлению активами.

Банк в своей деятельности руководствуется принципом «Знай своего служащего», который обеспечивает определённые проверочные процедуры при приёме сотрудников на работу, а также контроль за подбором и расстановкой кадров, чёткие критерии квалификационных и личностных характеристик сотрудников применительно к содержанию и объёму выполняемой работы и мере ответственности.

Политика работы с клиентом «Знай своего клиента» включает в себя порядок, согласно которому оценивается каждый клиент в тот момент, когда он устанавливает свои отношения с Банком, в целях предотвращения любой возможности неправомерных действий в рамках деятельности Банка.

- **Персонификация и адекватное разделение ролей и ответственности.**

Ответственность должностных лиц Банка за решения, связанные с его активами, должна персонифицироваться и осуществляться преимущественно в форме поручительства. Она должна быть адекватной степени влияния на цели Банка, фиксироваться в политиках, контролироваться и совершенствоваться.

- **Адекватность ролей функциям, процедурам и их сопоставимость с критериями и системой оценки.**

Роли должны адекватно отражать исполняемые функции и процедуры их реализации, принятые в Банке. При назначении взаимосвязанных ролей должна учитываться необходимая последовательность их выполнения. Роль должна быть согласована с критериями оценки эффективности её выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки.

- **Доступность услуг и сервисов.**

Банк должен обеспечить доступность для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определённые соответствующими договорами (соглашениями) и (или) иными документами.

- **Наблюдаемость и оцениваемость обеспечения ИБ.**

Любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно виден (прозрачен) и мог быть оценён подразделением Банка, имеющим соответствующие полномочия.

7.3 Обеспечение формирования Службы информационной безопасности Банка.

В состав требований к организации и функционированию Службы ИБ Банка включаются следующие требования:

- обеспечивают формирование Службы ИБ, а также определяют во внутренних документах цели и задачи деятельности этого подразделения;
- предоставляют полномочия и выделяют ресурсы, необходимые для выполнения Службой ИБ установленных целей и задач.

В Банке назначается куратор Службы ИБ из состава своего органа управления, и определяют его полномочия. При этом Служба ИБ и Отдел информационных технологий не должны иметь общего куратора.

Служба ИБ осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется следующими полномочиями:

- осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
- контролировать выполнение сотрудниками требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;
- участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платёжной системы после сбоев и отказов в работе объектов информационной инфраструктуры.

7.4 *«Осведомлённость в области обеспечения защиты информации».*

Банк обеспечивает повышение осведомлённости сотрудников в области обеспечения защиты информации:

- по порядку применения организационных мер защиты информации;
- по порядку использования технических средств защиты информации.

Банк обеспечивает:

- повышение осведомлённости сотрудников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации;
- доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению;
- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- информирование Службы ИБ о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты.

8 *Основные требования по обеспечения информационной безопасности Банка.*

Требования ИБ формулируются для следующих областей:

- назначении и распределении функциональных прав и обязанностей (ролей) и обеспечении доверия к персоналу Банка;
- стадий жизненного цикла АБС;
- защиты от НСД, управления доступом и регистрацией в АБС;
- защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.
- использования ресурсов информационно-телекоммуникационной сети «Интернет»;
- использования средств криптографической защиты информации;
- защиты банковских платёжных и информационных технологических процессов.
- защита от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи;
- обеспечение защиты информации при переводе денежных средств;
- обработка персональных данных;

- разработка и организация реализации программ по обучению и повышению осведомлённости.

8.1 *Требования по обеспечению защиты информации при назначении и распределении функциональных прав и обязанностей (ролей) и обеспечении доверия к персоналу Банка.*

Наибольшую угрозу безопасности информации в Банке представляет его персонал. Недостаток квалификации, избыточные полномочия, неисполнение или ненадлежащее исполнение своих должностных обязанностей и требований безопасности могут привести к нарушению режима ИБ Банка и, как следствие, привести к различным потерям.

В связи с этим, при приёме нового сотрудника на работу, влияющую на обеспечение ИБ, должны выполняться и регистрироваться следующие условия:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности.

При приёме на работу, связанную с защищаемой информацией, сотрудник даёт письменное Обязательство о неразглашении банковской и коммерческой тайн, а также персональных данных.

При необходимости Банк может официально потребовать от учебных заведений, военкомата и т.д. подлинность предоставляемого диплома, военного билета и т.д. Результаты проверки, документ (ы) подшивают(ся) в личное дело сотрудника.

На основании бизнес-процессов Правлением Банка определяются и персонифицируются роли персонала с учётом целей Банка, имеющихся ресурсов, функциональных требований, а также критериев оценки эффективности выполнения правил для данных ролей. Для эффективного выполнения целей и задач по управлению информационными активами определяются соответствующие роли сотрудников. Роли определяются исходя из задач, функциональных и процедурных требований, и обеспечиваются соответствующими ресурсами и достаточными профессиональными знаниями сотрудников. Роли персонифицируются с установлением ответственности за их исполнение. Совмещение в одном лице роли следующих функций: разработка и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения. Банк обеспечивает контроль и регистрацию действий лиц, которым назначены данные роли.

При определении ролей не допускается создание критичных ролей, концентрирующие в себе все или большинство наиболее важных функций, необходимых для реализации одной из целей Банка. Совокупность правил, составляющих роли, не должна быть критичной для Банка с точки зрения последствий успешного нападения на её исполнителя.

Формирование и назначение ролей сотрудников Банка осуществляется с учётом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения должностных обязанностей.

При приёме на работу, а также при смене должности, сотрудник Банка ознакомляется с требованиями ИБ, а также со своими обязанностями в области обеспечения ИБ. Для проверки компетентности персонала в вопросах выполнения каждым сотрудником своих функций в области обеспечения ИБ Служба ИБ проводятся проверки знаний ИБ сотрудников.

Служба ИБ проводит контрольные проверки сотрудников (с документальной фиксацией результатов). Так же проводятся внеплановые проверки сотрудников (с документальной фиксацией результатов) при выявлении участия или подозрение на участие их в инцидентах ИБ, а также при выявлении фактов их внештатного поведения. Компетентность сотрудников в области обеспечения ИБ достигается путём обучения правилам безопасной (с точки зрения ИБ) работы, осведомлённости персонала об источниках потенциальных угроз и уязвимостях, а также периодическими проверками и оценкой его профессиональных знаний и навыков в рамках требований действующего законодательства Российской Федерации.

Для контроля исполнения требований ИБ в Банке функционирует Служба ИБ.

Банк обеспечивает регистрацию лиц, обладающих правами:

- по осуществлению доступа к защищаемой информации;
- по управлению криптографическими ключами;
- по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платёжных терминалов и электронных средств платежа.

Банк обеспечивает регистрацию своих сотрудников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств.

8.2 *Требования по обеспечению ИБ автоматизированных банковских систем Банка на стадиях жизненного цикла.*

Наиболее важные информационно-технологические процессы Банка реализуются АБС. В связи с этим обеспечение безопасности информации, циркулирующей в АБС на всех стадиях их жизненного цикла, является основной задачей процесса обеспечения ИБ Банка.

Доступ к АБС санкционируется руководителем структурного подразделения пользователя и согласовывается с Начальником Службы ИБ Банка, Начальником Службы ИТ и Председателем Правления Банка (Заместителем Председатель Правления Банка).

Все изменения АБС составляются совместно техническими специалистами (сотрудниками Службы ИТ или лицами, привлечёнными на экспертной основе), разработчиками АБС и конечными пользователями АБС с целью исключения неверных формулировок требований к АБС.

При составлении технических заданий разработчиком гарантируется защита от принятия неверных проектных решений, внесения дефектов на уровне архитектуры, внесения недокументированных возможностей в АБС, разработки некачественной документации, сборки АБС с нарушением требований. Предпринятые в отношении данных угроз защитные меры отражаются разработчиком в технической документации.

Не допускается существенных внесение изменений в рабочую АБС без предварительного их тестирования на другой базе.

Перед началом работы с вновь устанавливаемой или изменяемой АБС все пользователи проходят инструктаж у руководителей своих подразделений и, при необходимости, администратора АБС. Обо всех инцидентах ИБ, или при подозрении на них, пользователи обязаны незамедлительно сообщать об этом сотруднику Службы ИБ. Сотрудник Службы ИБ информирует Руководителя Службы ИБ Банка, который сообщает об этом Председателю Правления Банка (Заместителю Председателя Правления Банка).

Банк обеспечивает реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

Эксплуатируемая АБС и (или) её компоненты снабжены документацией, содержащей описание реализованных в АБС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер.

Банк проводит анализ принятия разработчиком АБС защитных мер, направленных на обеспечение безопасности разработки АБС и безопасности её поставки.

Приобретение и установка средств и систем защиты АБС (средства защиты от несанкционированного доступа, антивирусные программы и пр.) осуществляются по согласованию с Начальником Отдела ИТ и Руководителем Службы ИБ. Ввод в действие и снятие с эксплуатации систем защиты АБС осуществляются при участии Начальника Отдела ИТ и Руководителя Службы ИБ.

На стадии эксплуатации АБС определены, выполняться и регистрироваться процедуры:

- контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;
- контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС;
- контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер;
- контроля необходимого обновления ПО АБС, включая ПО технических защитных мер.

На стадии эксплуатации АБС определены, выполняются, регистрируются и контролируются процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ.

На стадии эксплуатации АБС определены, выполняются и регистрируются процедуры контроля, устанавливаемого и (или) используемого ПО АБС.

На стадии эксплуатации АБС определены, выполняются и контролируются процедуры, необходимые для обеспечения сохранности носителей защищаемой информации.

На стадии сопровождения (модернизации) определены, выполняются и регистрируются процедуры контроля, обеспечивающие защиту от:

- умышленного несанкционированного раскрытия, модификации или уничтожения информации;
- неумышленной модификации, раскрытия или уничтожения информации;
- отказа в обслуживании или ухудшения обслуживания.

На стадии снятия с эксплуатации определены, выполняются и регистрируются процедуры, обеспечивающие удаление информации с использованием алгоритмов и (или) методов, обеспечивающих невозможность восстановления удалённой информации, несанкционированное использование которой может нанести ущерб деятельности Банка, и информации, используемой техническими защитными мерами, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определённого срока предусмотрены законодательством РФ, нормативными актами Банка России и (или) договорными документами.

По факту выявленных нарушений и инцидентов ИБ в АБС Служба ИБ проводит служебные расследования.

С точки зрения обеспечения безопасности информации критическими компонентами АБС являются:

- сервер АБС, на котором располагается информация, подлежащая защите;
- администраторы АБС и операторов АБС, с которых происходит управление процессами обработки информации;
- сетевое оборудование и каналы связи.

Защита информации АБС от НСД используются как встроенные механизмы защиты информации, а также рекомендуются к использованию сертифицированные или разрешённые руководством Банка.

Для каждого участника, а также групп участников, информационно-технологического процесса, реализуемого АБС, создаётся уникальный идентификатор. Для аутентификации пользователя применяется данный идентификатор (логин) и секретное слово (пароль), известное только самому пользователю, что позволяет однозначно идентифицировать пользователя и обеспечить защиту от угрозы отказа от авторства.

Для обеспечения безопасности на уровне каналов связи используется прицеп резервирования каналов. Созданы резервные каналы, предоставляемые разными провайдерами.

Перед снятием с эксплуатации АБС или её отдельных компонентов вся информация с них переносится в архив и удаляется из постоянной памяти и внешних носителей АБС или её компонентов администратором АБС. Контроль за удалением информации осуществляет Служба

ИБ. После удаления информации составляется акт о снятии с эксплуатации АБС или её компонента.

Обязанности по контролю за соблюдением режима обеспечения безопасности информации на всем жизненном цикле АБС возложены на Службу ИБ.

8.3 *Требования по обеспечению информационной безопасности при управлении доступом и регистрации.*

Для обеспечения защиты от НСД к защищаемой информации, расположенной на ресурсах Банка, используется управление доступом к ресурсам. Создан и регулярно уточняется перечень ресурсов и определены владельцы каждого ресурса.

Обязанности по обеспечению ИБ в функциональных подразделениях возложены на руководителей структурных подразделений.

Назначение (изменение, лишение) полномочий по доступу пользователя к ресурсам санкционируется руководителем структурного подразделения пользователя и согласовывается с владельцем ресурса и Службой ИБ.

Чтобы обеспечить защиту информации от угроз НСД, противоправного изменения и удаления, пользователю назначаются минимальные полномочия, необходимые для выполнения своих должностных обязанностей.

В составе АБС используются сертифицированные и (или) разрешённые к применению средства защиты информации от НСД.

В Банке обеспечивается авторизация, контроль и управление доступом к информационным активам, в том числе:

- функционирование системы парольной защиты АРМ и ЛВС;
- назначение/лишение полномочий по доступу сотрудников Банка к ресурсам ЭВМ и/или ЛВС санкционируется руководителем структурного подразделения Банка, несущего персональную ответственность за обеспечение ИБ в данном подразделении;
- регистрация действий сотрудников и пользователей в электронных журналах регистрации событий системного и прикладного ПО. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несёт персональную ответственность за полноту и точность отражения в журнале имевших место событий;
- ежедневный мониторинг изменений и/или предоставление доступов сотрудникам Банка к АБС, а также регулярные проверки доступов, предоставленных всем сотрудникам Банка к ресурсам ЭВМ и/ или ЛВС, на предмет их соответствия установленным ролям сотрудников и производственной необходимостью наличия предоставленных доступов.

В Банке определены, выполняются, регистрируются и контролируются правила и процедуры:

- идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются сотрудниками организации БС РФ, и программных процессов (сервисов);
- разграничения доступа к информационным активам на основе ролевого метода, с определением для каждой роли полномочий по доступу к информационным активам;
- управления предоставлением/отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети;
- регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации;
- управления идентификационными данными, аутентификационными данными и средствами аутентификации;
- управления учётными записями субъектов доступа;
- выявления и блокирования неуспешных попыток доступа;

- блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы;
- ограничения действий пользователей по изменению настроек их автоматизированных мест (использование ограничений на изменение BIOS);
- управления составом разрешённых действий до выполнения идентификации и аутентификации;
- ограничения действий пользователей по изменению параметров настроек АБС и реализации контроля действий эксплуатационного персонала по изменению параметров настроек АБС;
- выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин;
- использования технологий беспроводного доступа к информации, в случае их применения, и защиты внутренних беспроводных соединений;
- использования мобильных устройств для доступа к информации в случае их применения.

Процедуры управления доступом исключают возможность «самосанкционирования».

В Банке определены, выполняются, регистрируются и контролируются правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции, для чего, среди прочего, следует:

- определить действия и операции, подлежащие регистрации;
- определить состав и содержание данных о действиях и операциях, подлежащих регистрации, сроки их хранения;
- обеспечить резервирование необходимого объёма памяти для записи данных;
- обеспечить реагирование на сбои при регистрации действий и операций, в том числе аппаратные и программные ошибки, сбои в технических средствах сбора данных;
- обеспечить генерацию временных меток для регистрируемых действий и операций и синхронизацию системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных.

В Банке реализовано ведение журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов и АБС с целью их использования при реагировании на инциденты ИБ.

Хранение данных о действиях и операциях не менее трёх лет, а для данных, полученных в результате выполнения банковского платёжного технологического процесса, - не менее пяти лет, если иные сроки хранения не установлены законодательством РФ, нормативными актами Банка России.

Для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях используется специализированные программные и (или) технические средства.

Процедуры мониторинга ИБ и анализа данных о действиях и операциях используются зафиксированные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга ИБ и анализа применяются на регулярной основе, например, ежедневно, ко всем выполненным действиям и операциям (транзакциям).

В Банке определены и контролируется выполнение требований:

- к разделению сегментов вычислительных сетей, в том числе создаваемых с использованием технологии виртуализации;
- к межсетевому экранированию;
- к информационному взаимодействию между сегментами вычислительных сетей.

Разделение сегментов вычислительных сетей осуществляется с целью обеспечения независимого выполнения банковских платёжных технологических процессов Банка, а также банковских информационных технологических процессов Банка разной степени критичности, в

том числе банковских информационных технологических процессов, в рамках которых осуществляется обработка персональных данных в ИСПДн.

В документах Банка регламентированы и контролируются процедуры внесения изменений в конфигурацию сетевого оборудования, предусматривающие согласование вносимых изменений со Службой ИБ. Сотрудникам Службы ИБ рекомендуется предоставлять доступ к конфигурации сетевого оборудования без возможности внесения изменений.

Определён, выполняется, регистрируется и контролируется порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов.

В Банке определён, выполняется и контролируется порядок использования съёмных носителей информации.

Передача защищаемых данных по каналам связи, имеющим выход за пределы контролируемой Банком зоны, в том числе банкоматов и платёжных терминалов, осуществляется только при условии обеспечения их защиты от раскрытия и модификации.

Работа всех пользователей АБС осуществляется под уникальными учётными записями.

В системах дистанционного банковского обслуживания должны быть реализованы механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имён.

8.4 *Требования по обеспечению защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.*

Все АРМ и сервер АБС защищаются от внедрения вредоносного и шпионского ПО официально приобретёнными и регулярно обновляемыми средствами антивирусной защиты. Дополнительная защита от вирусов достигается проверкой Интернет-трафика при прохождении его через пограничные маршрутизаторы (через которые происходит взаимодействие с информационно-телекоммуникационной сетью «Интернет»), корпоративной сети.

Использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (далее - технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники, включая банкоматы и платёжные терминалы, при наличии технической возможности.

На сервере АБС запрещена установка ПО, не предназначенного для реализации информационно-технологического процесса, реализуемого АБС. Контроль осуществляется Службой ИБ Банка во взаимодействии с сотрудником Отдела ИТ.

Установленное или изменяемое ПО должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

При обнаружении компьютерного вируса необходимо принять меры по устранению последствий вирусной атаки, проинформировать руководство и приостановить при необходимости работу (на период устранения последствий вирусной атаки).

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Банк обеспечивает информирование оператора платёжной системы.

Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в Банке должны контролироваться Службой ИБ Банка.

В Банке необходимо организовать антивирусную фильтрацию всего трафика электронного почтового обмена.

Ответственность за неисполнение или ненадлежащее исполнение требований антивирусной защиты возлагаются на каждого сотрудника Банка, имеющего доступ к АРМ и/или АБС.

Перед подключением съёмных носителей информации к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов,

проводится их антивирусная проверка на специально выделенном автономном средстве вычислительной техники.

В Банке разработаны и введены в действие частная политика, инструкции и рекомендации по антивирусной защите, учитывающие особенности банковских технологических процессов.
и содержащих описание вредоносных кодов и способы их обезвреживания;

Банк обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода: на сайте Банка, в договорах с клиентами при подключении к системе Клиент-Банк и по системе Клиент-Банк.

В целях защиты информационных активов в Банке необходимо организовывать эшелонированную центральную систему защиты от вредоносного кода, предусматривающую использование средств антивирусной защиты различных производителей и их раздельную установку на объектах информационной инфраструктуры Банка.

8.5 *Требования по обеспечению ИБ при использовании ресурсов информационно-телекоммуникационной сети «Интернет».*

Функционирование Банка без взаимодействия с информационно-телекоммуникационной сетью «Интернет» (далее сеть «Интернет») принципиально невозможно. Через сеть «Интернет» происходит взаимодействие между структурными подразделениями Банка, обеспечивается обслуживание клиентов по системе «Клиент-Банк», сотрудниками Банка используются ресурсы сети «Интернет» для выполнения своих должностных обязанностей, обмен электронными сообщениями между организациями БС РФ и иными субъектами НПС и т.д.

Взаимодействие с сетью «Интернет» создаёт дополнительные угрозы ИБ Банка, включая угрозы перехвата и НСД к защищаемой информации, вирусного заражения рабочих станций и серверов АБС, взлома пограничного маршрутизатора и проникновения злоумышленника в корпоративную сеть, утечки информации и пр.

В Банке предприняты следующие методы защиты от угроз:

- вся защищаемая информация, которая передаётся через сеть «Интернет», в обязательном порядке шифруется с помощью соответствующих средств криптографической защиты информации для обеспечения её защиты в случае перехвата;
- доступ к сети «Интернет» сотрудников Банка согласовывается с Руководителем Службы ИБ, Начальником Отдела ИТ и Председателем Правления Банка (Заместителем Председателя Правления Банка). Контроль использования ресурсов сети «Интернет» сотрудниками возложен на Службу ИБ. Все случаи нецелевого использования сети «Интернет» рассматриваются как нарушения ИБ Банка;
- сотрудникам запрещена передача информации, содержащей банковскую, коммерческую или персональные данные, а также другой защищаемой Банком информации, через сеть «Интернет». Контроль отправляемой в сети «Интернет» информации осуществляет Служба ИБ;
- на всех рабочих станциях и серверах, взаимодействующих с сетью «Интернет», стоят средства антивирусной защиты информации;
- для дополнительной защиты сервисов, предоставляемых через сеть «Интернет», на пограничных маршрутизаторах ограничивается количество точек подключения к сервису за счёт использования уникальных свойств клиента (например, IP-адрес, код аутентификации).

Сотрудники Банка не должны игнорировать предупреждения о возможном снижении уровня безопасности или опасности содержимого при передаче/получении информации через сеть «Интернет» и обязаны выполнять рекомендации администраторов.

Обо всех выявленных нарушениях ИБ Банка при работе с сетью «Интернет» сотрудник Службы ИБ сообщает Руководителю Службы ИБ, который информирует Председателя Правления Банка (Заместителя Председатель Правления Банка).

По факту нарушения ИБ Службой ИБ проводится служебное расследование.

Банк обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети "Интернет".

Банк на основании заявления клиента, переданного способом, определённым договором с клиентом, устанавливает ограничения по параметрам операций, которые могут осуществляться клиентом с использованием системы Клиент-Банк

Банк при передаче клиенту, являющемуся юридическим лицом, ПО, предназначенного для осуществления переводов денежных средств с использованием системы Клиент-Банк, доводит до клиента ПО контроля целостности указанного ПО и инструкцию по эксплуатации (эксплуатационную документацию) такого программного средства либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию).

Банк обеспечивает возможность оперативной блокировки доступа (прекращения использования с целью осуществления переводов денежных средств) клиента к системам Клиент-Банк на основании уведомления, переданного способом, определённым договором оператора по переводу денежных средств с клиентом.

Банк обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации, и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу денежных средств стало известно о признаках, указывающие на изменение.

Электронная почта должна архивироваться.

Целями создания архивов электронной почты являются:

- контроль информационных потоков, в том числе с целью предотвращение утечек информации;
- использование архивов при проведении разбирательств по фактам утечек информации.

Должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры доступа к информации архива и её изменения, предусматривающие возможность доступа сотрудникам Службы ИБ к информации архива.

Определён состав и порядок применения мер защиты, применяемых при взаимодействии с сетью «Интернет» и позволяющих обеспечить противодействие атакам злоумышленников и распространению спама.

8.6 *Требования по обеспечению защиты информации при использовании средств криптографической защиты информации».*

Для защиты информации, передаваемой через открытые каналы связи, Банк использует сертифицированные средства криптографической защиты информации (СКЗИ) уполномоченного государственного органа.

Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с законодательством Российской Федерации, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

Выбор и приобретение СКЗИ согласовывается с Руководителем Службы ИБ Банка.

При выборе и приобретении средств СКЗИ учитываются следующие требования:

- они допускают встраивание в технологическую схему обработки электронных сообщений, а также обеспечивают взаимодействие с прикладным программным обеспечением на уровне запросов на криптографические преобразования и выдачи результатов преобразования;
- они поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

- они реализованы на основе алгоритмов, соответствующих национальным стандартам РФ, условиям договора с контрагентом и (или) стандартам Банка;
- они имеют строгий регламент использования ключей, предполагающий контроль со стороны Службы ИБ за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);
- они обеспечивают реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей или при переходе АБС в нештатный режим работы;
- они не содержат требований по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
- они не требуют дополнительной защиты от утечки по побочным каналам электромагнитного излучения;
- они поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности ПО для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

Банк определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств;
- порядок эксплуатации СКЗИ;
- порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе;
- порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ;
- порядок снятия с эксплуатации СКЗИ;
- порядок управления ключевой системой;
- порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей.

Служба ИБ контролирует использование СКЗИ в структурных подразделениях Банка. Им осуществляется регистрация инцидентов ИБ, а также всех значимых событий в процессе обмена электронными сообщениями.

Криптографические ключи могут изготавливаться Банком и (или) клиентом Банка самостоятельно. Отношения, между ними регулируются заключаемыми договорами.

ИБ процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты, предусмотренных технической документацией на СКЗИ.

СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

8.7 *Требования по обеспечению защиты информации при использовании средств криптографической защиты информации».*

Система обеспечения ИБ банковского платёжного технологического процесса должна соответствовать требования Комплексу Стандарта Банка России СТО БР ИББС и иных нормативных документов по вопросам ИБ, действие которых распространяется на банковскую систему Российской Федерации.

Защита платёжных технологических процессов Банка включает в себя:

- защиту платёжной информации с использованием Автоматизированного рабочего места клиента Банка России (АРМ КБР);
- защита платёжной информации с использованием Автоматизированного рабочего места;
- защиту платёжной информации с использованием системы Банк-клиент;
- защиту обмена платёжной информацией между банками корреспондентами с использованием международной системы;
- защиту обмена платёжной информацией между банками с использованием системы платежей;
- защиту технологического процесса по управлению должностными обязанностями и полномочиями сотрудников Банка, задействованных в обеспечении платёжного технологического процесса Банка
- защита информации, отнесённую к защищаемой информации в соответствии с положением №719-П.

Порядок обмена платёжной информацией определён в договорах между Банком и клиентами: кредитными организациями, юридическими и физическими лицами.

При работе с платёжной информацией необходимо проводить авторизацию и контроль целостности данной информации.

Применяются средства защиты от несанкционированного доступа и средства криптографической защиты информации (СКЗИ) на средствах вычислительной техники, на которых осуществляются операции над платёжной информацией.

Подготовленная клиентами Банка платёжная информация, на основании которой совершаются расчётные и кассовые операции, предназначена для внутреннего использования Банком и может быть передана иным организациям только в соответствии с действующим законодательством Российской Федерации.

Система обеспечения ИБ платёжного технологического процесса Банка строится в соответствии с требованиями Политики и иных нормативных документов по вопросам ИБ, действие которых распространяется на банковскую систему Российской Федерации.

Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается путём: выбора организационных мер защиты информации; определения во внутренних документах Банка, порядка применения организационных мер защиты информации; определения лиц, ответственных за применение организационных мер защиты информации; применения организационных мер защиты; реализации контроля применения организационных мер защиты информации; выполнения иных необходимых действий, связанных с применением организационных мер защиты информации; выбора технических средств защиты информации; определения во внутренних документах Банка порядка использования технических средств защиты информации, включающего информацию о конфигурации, определяющую параметры работы технических средств защиты информации; назначения лиц, ответственных за использование технических средств защиты информации; использования технических средств защиты информации; реализации контроля за использованием технических средств защиты информации; выполнения иных необходимых действий, связанных с использованием технических средств защиты информации.

Сотрудники Банка, в том числе администраторы автоматизированных систем и средств защиты информации, не обладают всей полнотой полномочий для бесконтрольного создания, авторизации, уничтожения и изменения платёжной информации, а также проведения операций по изменению состояния банковских счетов.

Результаты технологических операций по обработке платёжной информации контролируются и удостоверяются уполномоченными работниками и/или автоматизированными процессами. Уполномоченные сотрудники и/или автоматизированные процессы, осуществляющие обработку платёжной информации и контроль (проверку) результатов обработки, не зависят друг от друга.

Обязанности по администрированию средств защиты платёжной информации, передаваемой по электронным каналам связи, возлагаются приказом по Банку на администраторов, соответствующих АРМ с отражением этих функций в их должностных обязанностях.

Комплекс мер по обеспечению ИБ банковского платёжного технологического процесса предусматривает:

- защиту платёжной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платёжных документов;
- минимально необходимый, гарантированный доступ сотрудника Банка только к тем ресурсам банковского платёжного технологического процесса, которые необходимы ему для выполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платёжной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платёжной информации;
- аутентификацию обрабатываемой платёжной информации;
- двустороннюю аутентификацию автоматизированных рабочих мест, участников обмена платёжной информацией;
- восстановление платёжной информации в случае её умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- авторизованный ввод платёжной информации в АБС двумя сотрудниками с последующей программной сверкой результатов ввода на совпадение (Dual Control, ISO TR 13569 (принцип «двойного управления»));
- сверку выходных платёжных сообщений с соответствующими поступившими платёжными сообщениями;
- гарантированную доставку платёжных сообщений участникам обмена.

Банк также выполняет требования международных платёжных систем по обеспечению ИБ в части выполняемых им операций.

Должны быть определены, выполняться и регистрироваться процедуры контроля отсутствия размещения на устройствах, задействованных в осуществлении банковского платёжного технологического процесса, находящихся в общедоступных местах вне зоны постоянного контроля Банка, в том числе банкоматов и платёжных терминалов, специализированных средств, используемых для несанкционированного съёма информации.

8.8 *Требования обеспечению информационной безопасности информационных технологических процессов Банка.*

Система обеспечения ИБ информационного технологического процесса Банка регулируется Политикой и иными нормативными документами по вопросам ИБ, действие которых распространяется на банковскую систему Российской Федерации.

Процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются и обеспечиваются инструктивными и методическими материалами.

В Банке следует провести классификацию неплатёжной информации и определить перечень её типов. Классификацию неплатёжной информации следует проводить в соответствии со степенью тяжести последствий потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности.

Для каждого из типов неплатёжной информации, полученных в результате классификации, документально определяется набор требований по её защите.

С целью контроля исполнения мероприятий по ИБ в Банке осуществляется периодическое тестирование всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ. В Банке разрабатывается и реализуется процедура восстановления системы обеспечения ИБ после технических сбоев или преднамеренных атак.

8.9 *Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств.*

Банк обеспечивает регистрацию лиц, обладающих правами:

- по осуществлению доступа к защищаемой информации;
- по управлению криптографическими ключами;
- по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платёжных терминалов и электронных средств платежа.

Банк обеспечивает регистрацию своих сотрудников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств. Банк обеспечивает реализацию запрета выполнения одним лицом в один момент времени несовместимых ролей. Банк обеспечивает контроль и регистрацию действий лиц, которым назначены роли в информационных системах Банка при наличии технической возможности.

8.10 *Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры.*

Банк обеспечивает включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств. Служба ИБ Банка участвует в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры. Служба ИБ Банка обеспечивает контроль соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

Банк обеспечивает эксплуатацию технических средств в соответствии с эксплуатационной документацией. Банк обеспечивает реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры. Банк на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивает выполнение требований ИБ.

8.11 Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа.

Банк обеспечивает учёт объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации.

Банк обеспечивает применение не криптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру

оценки соответствия. Допускается применение не криптографических средств защиты информации от несанкционированного доступа иностранного производства.

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации Банк обеспечивает выполнение требований ИБ: регистрации действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения обеспечивается Банком в объёме и порядке, установленном нормативными актами Банка России, операторами платёжной системы, Банка.

Банк обеспечивает хранение указанной информации не менее пяти лет.

При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации Банк обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов.

Банк обеспечивает:

- реализацию запрета несанкционированного расширения прав доступа к защищаемой информации;
- назначение своим сотрудникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации.

Банк фиксирует во внутренних документах необходимость применения и реализует исполнение, и контроль организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для выполнения требований ИБ.

Банк обеспечивает принятие мер, направленных на предотвращение хищений носителей защищаемой информации.

Банк обеспечивает возможность приостановления (блокирования) клиентом приёма к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента.

8.12 Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники.

Банк обеспечивает:

- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры, на средствах вычислительной техники, при наличии технической возможности;
- регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания;
- функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности.
- Банк обеспечивает формирование в договорных отношениях с клиентами рекомендаций для клиентов по защите информации от воздействия вредоносного кода.

Банк обеспечивает использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности.

При наличии технической возможности Банк обеспечивает выполнение:

- предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники;
- проверки на отсутствие вредоносного кода средств вычислительной техники, выполняемой после установки или изменения программного обеспечения.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Банк обеспечивает принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

Банк имеет право приостановить при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Банк обеспечивает информирование оператора платёжной системы.

8.13 Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании информационно-телекоммуникационной сети Интернет при осуществлении переводов денежных средств.

При использовании сети «Интернет» для осуществления переводов денежных средств Банк обеспечивает:

- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по информационно-телекоммуникационной сети «Интернет»;
- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием информационно-телекоммуникационной сети «Интернет»;
- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путём использования уязвимостей программного обеспечения;
- снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;
- фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью «Интернет».

Банк через договорные отношения формирует для клиентов рекомендации по защите информации от несанкционированного доступа путём использования ложных (фальсифицированных) ресурсов сети «Интернет».

8.14 Требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств.

Банк обеспечивает учёт и контроль установленного и (или) используемого на средствах вычислительной техники программного обеспечения.

Банк обеспечивает выполнение порядка применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств.

Распоряжение клиента, распоряжение участника платёжной системы и распоряжение платёжного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом.

Банк обеспечивает:

- защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации;
- контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;
- аутентификацию входных электронных сообщений;
- взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями;
- восстановление информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платёжных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчётов в платёжной системе;
- выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

8.15 Требования по обеспечению информационной безопасности информационных технологических процессов Банка.

Вся неплатёжная информация подразделяется на:

- *открытую*, в том числе доступную внешним пользователям, клиентам и контрагентам. К данному типу информации может относится публикуемая отчётность, данные о ставках по вкладам и иным видам банковских услуг, общая информация о Банке и т.п.; данная информация может распространяться путём размещения её на сайте Банка в информационно-телекоммуникационной сети «Интернет», выпуске рекламных проспектов, стендов и в операционных залах. Требованием ИБ к данному виду информации является её достоверность, которая обеспечивается лицами, ответственными за её распространение;
- *информацию ограниченного доступа*, к которой имеют право доступа только лица, которым такое право предоставлено в силу их должностных обязанностей; право работы с документами ограниченного доступа определяется должностной инструкцией указанных сотрудников и (или) внутренним нормативным или распорядительным документом. Информация ограниченного доступа может быть защищена программным путём и иметь отметку «Документ ограниченного пользования»;
- *информацию конфиденциального характера*, то есть доступную только сотрудникам Банка и на которую распространяются требования по сохранению конфиденциальности и (или) банковской тайны, а также персональные данные. К данному типу информации относятся сведения о структуре Банка, сведения о сотрудниках Банка, о внутренней нормативной базе, порядок работы с АБС и др. Данная информация должна храниться с

обеспечением требований к её сохранности в сейфах, запирающихся шкафах или ящиках. Для обеспечения сохранности такой информации и контроля за доступом к ней может вводиться режим ограничения распространения такой информации — запрет на снятие копий, ограничение физического выноса документов из мест их хранения и т.п. Информация конфиденциального характера, хранящаяся на электронных носителях, должна иметь не менее двух степеней защиты. Все сотрудники Банка при приёме на работу дают письменное Обязательство о неразглашении банковской и коммерческой тайн, а также персональных данных.

8.16 Требования по обработке персональных данных

В Банке необходимо документально зафиксировать цели обработки персональных данных (объем и содержание, сроки обработки, сроки хранения, необходимость получения согласия), а также определить необходимость уведомления Уполномоченный орган по защите субъектов персональных данных об обработке персональных данных.

В Банке определены, выполняются и контролируются процедуры учёта ресурсов ПДн, в том числе учёта ИСПДн.

Классификация персональных данных проводится в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных:

- специальные категории персональных данных;
- биометрические категории персональных данных;
- обезличенные персональные данные;
- другие (которые не могут быть отнесены к вышеизложенным категориям).

Передача персональных данных Банком третьему лицу должна осуществляться с согласия субъекта персональных данных. В том случае, если Банк поручает обработку персональных данных третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Следует прекратить обработку персональных данных и уничтожить собранные персональные данные, если иное не установлено законодательством Российской Федерации, в следующих случаях и в сроки, установленные законодательством Российской Федерации:

- по достижении целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством Российской Федерации;
- при невозможности устранения оператором допущенных нарушений при обработке персональных данных.

Необходимо определить и документально зафиксировать:

- порядок уничтожения или обезличивание персональных данных (в том числе и материальные носители персональных данных);
- порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных;
- порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных;
- порядок к отнесению АБС к информационным системам персональных данных (ИСПДн), перечень ИСПДн;

- перечень (список) сотрудников, осуществляющих обработку персональных данных в ИСПДн либо имеющих доступ к персональным данным;
- порядок доступа сотрудников Банка и иных лиц в помещения, в которых ведётся обработка персональных данных;
- порядок хранения материальных носителей персональных данных.

8.17 Требования к проведению оценки соответствия и аудита информационной безопасности.

Аудит ИБ Банка проводиться в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» и СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

Перед проведением самооценки необходимо документально определить и реализовать программу аудита ИБ, содержащую информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

Для аудита ИБ необходимо документально оформить план аудита, определяющий:

- цель аудита ИБ;
- критерии аудита ИБ;
- область аудита ИБ;
- дату и продолжительность проведения аудита ИБ;
- состав аудиторской группы (проводимой организацией, имеющей опыт проведения аудита ИБ и оценки соответствия требованиям стандарта Банка России СТО БР ИББС-1.0);
- описание деятельности и мероприятий по проведению аудита;
- распределение ресурсов при проведении аудита.

Также должны быть оформлены договоры с аудиторскими организациями, а также документально определены:

- порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;
- порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;
- порядок взаимодействия аудиторской группы и руководства Банка, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству Банка;
- порядок организации опроса сотрудников;
- порядок организации наблюдения за деятельностью сотрудников Банка со стороны представителей аудиторской организации.

По результатам проведения аудита должны быть подготовлены отчёты. Результаты аудитов, а также соответствующие отчёты должны быть доведены до руководства Банка.

Должен быть документально определён порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности, отчётов аудитов.

В Банке должны быть документально определены роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов, и назначаться ответственные за выполнение указанных ролей.

Оценка соответствия осуществляется на основе:

- информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;
- анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям настоящего Положения;
- результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

Оценка соответствия должна осуществляться Банком с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации N 79.

8.18 Требования к анализу функционирования системы обеспечения информационной безопасности.

В Банке должен проводиться анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри Банка, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах Банка;
- данные об изменениях вне Банка, например, данные об изменениях в законодательстве Российской Федерации, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах Банка.

Анализ функционирования СОИБ должен включать в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в Банке, требованиям законодательства Российской Федерации, требованиям стандартов Банка России;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ Банка, требованиям Политики ИБ;
- оценку адекватности модели угроз Банка существующим угрозам ИБ;
- оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска;
- проверку адекватности используемых защитных мер требованиям внутренних документов Банка и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

Результаты анализа функционирования СОИБ должны документироваться.

В Банке должны быть документально определены роли, связанные с процедурами анализа функционирования СОИБ, и назначаться ответственные за выполнение указанных ролей.

8.19 Требования к анализу системы обеспечения информационной безопасности со стороны руководства Банка.

Во внутренних документах Банка должен быть перечень документов (данных), необходимых для формирования информации, предоставляемой руководству Банка с целью проведения анализа СОИБ.

В частности, в указанный перечень документов должны входить:

- отчёты с результатами мониторинга СОИБ и контроля защитных мер;
- отчёты с результатами анализа функционирования СОИБ;
- отчёты с результатами аудита ИБ;
- отчёты с результатами самооценки ИБ;
- отчёт об оценке соответствия требованиям 719-П;
- 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 уязвимостях и угрозах ИБ;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществлённых руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России;
- документы, содержащие информацию по выявленным инцидентам ИБ;
- документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков;
- документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

В Банке должен быть определён и утверждён внутренний документ по выполнению деятельности по контролю и анализу СОИБ. В частности, указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес Банка.

В Банке определяются роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством, назначаются ответственные за выполнение указанных ролей и документально определяются.

8.20 Требования к принятию решений по тактическим улучшениям системы обеспечения информационной безопасности.

Для принятия решений, связанных с тактическими улучшениями СОИБ в Банке, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудита ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- стратегических улучшений СОИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

Решения по тактическим улучшениям СОИБ должны быть документально зафиксированы и должны либо содержать выводы об отсутствии необходимости тактических улучшений СОИБ,

либо указывать направления тактических улучшений СОИБ в виде корректирующих или превентивных действий, например,

- пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
- пересмотр процедур эксплуатации отдельных видов защитных мер;
- пересмотр процедур обнаружения и обработки инцидентов;
- уточнение описи информационных активов;
- пересмотр программы обучения и повышения осведомлённости персонала;
- пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
- пересмотр планов обработки рисков;
- вынесение санкций в отношении персонала;
- пересмотр процедур мониторинга СОИБ и контроля защитных мер;
- пересмотр программ аудита;
- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
- ввод новых или замена используемых защитных мер.

Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться Руководителем Службы ИБ Банка.

Должны быть документально определены и выполняться процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны фиксироваться результаты выполнения указанных процедур.

В случаях принятия решений по тактическим улучшениям СОИБ, должны быть назначены ответственные за их реализацию.

8.21 Требования к принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности.

Для принятия решений, связанных со стратегическими улучшениями СОИБ в Банке, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудита ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых информационных активов Банка или их типов;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций), а также изменения:
  - в законодательстве Российской Федерации;
  - в нормативных актах Банка России;
  - интересов, целей и задач бизнеса Банка;
  - контрактных обязательств Банка.

Решения по стратегическим улучшениям СОИБ должны быть документально зафиксированы и должны либо содержать выводы об отсутствии необходимости стратегических улучшений СОИБ, либо указывать направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например,

- уточнение/пересмотр целей и задач обеспечения ИБ, определённых в рамках политики ИБ или частных политики ИБ;
- изменение в области действия СОИБ;

- уточнение описи типов информационных активов;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

Деятельность, связанная с реализацией стратегических улучшений СОИБ, должна быть санкционирована и контролироваться руководством Банка.

В случае стратегических улучшений СОИБ должна быть выполнена деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов.

В частности, необходимо выполнить:

- выработку планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;
- уточнение процедур использования защитных мер.

Должны быть документально определены и выполняться процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

В случаях принятия решений по стратегическим улучшениям СОИБ должны быть назначены ответственные сотрудники Банка за их реализацию.

8.22 Требования по разработке и организации реализации программ по обучению и повышению осведомлённости.

Организуется санкционированная руководством Банка работа с персоналом и клиентами в направлении повышения осведомлённости и обучения в области ИБ.

Разрабатываются планы, программы обучения и повышения осведомлённости в области ИБ. По результатам выполнения указанных планов осуществляться проверка полученных знаний.

В планах обучения и повышения осведомлённости устанавливаются требования к периодичности обучения и повышения осведомлённости.

Программы обучения и повышения осведомлённости разрабатывается для различных групп сотрудников с учётом их должностных обязанностей и выполняемых ролей и включает информацию:

- по существующим политикам ИБ;
- по применяемым в Банке защитным мерам;
- по правильному использованию защитных мер в соответствии с документами Банка;
- о значимости и важности деятельности работников для обеспечения ИБ Банка.

В Банке определяется перечень свидетельств выполнения программ обучения и повышения осведомлённости в области ИБ.

В частности, такими свидетельствами являться:

- документы (журналы), подтверждающие прохождение руководителями и сотрудниками Банка обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;
- документы, содержащие результаты проверок обучения сотрудников Банка;
- документы, содержащие результаты проверок осведомлённости в области ИБ в Банке.

Для сотрудника, получившего новую роль, организуется обучение или инструктаж в области ИБ, соответствующее полученной роли.

В Банке определены роли по разработке, реализации планов и программ обучения и повышения осведомлённости в области ИБ и по контролю результатов, а также назначены ответственные за выполнение указанных ролей.

9 Организация системы управления информационной безопасностью.

СУИБ представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности, организационные, технические, программные и криптографические, с целью достижения требуемых показателей и норм защищенности, циркулирующей в ИБС Банка информации в условиях реализации основных внутренних и внешних угроз безопасности.

Главной целью организации СУИБ является повышение надежности защиты информации в процессе ее обработки, хранения и передачи.

СУИБ характеризует процессный подход, включающий в себя планирование, реализацию, проверку и совершенствование. Все эти процессы реализуются в рамках циклической модели управления.

Задачами СУИБ являются:

- *на этапе планирования* – разработка и реализация научно-технических программ и координационных планов создания нормативно-правовых основ и технической базы, обеспечивающей использование передовых средств и информационных технологий в интересах обеспечения ИБ АБС; организация и координация взаимодействия в этой области разработчиков АБС, концентрация кадровых, финансовых и иных ресурсов заинтересованных сторон при разработке и поэтапном вводе в действие системы; создание действенной организационной структуры, обеспечивающей комплексное решение задач ИБ при функционировании АБС, оснащенной необходимыми программно-аппаратными средствами управления и контроля;
- *на этапе реализации* – обязательное и неукоснительное выполнение предусмотренных на этапе создания АБС правил и процедур, направленных на обеспечение ИБ, всеми задействованными в системе участниками, эффективное пресечение посягательств на информационные ресурсы, технические средства и информационные технологии;
- *на этапе проверки* – аудит СУИБ, выявление недостатков обеспечения ИБ, негативных тенденций в сфере ИБ;
- *на этапе совершенствования* – выработка и принятие корректирующих и превентивных мер, основанных на результатах анализа, для достижения непрерывного усовершенствования СУИБ Банка.

К компетенции *Службы ИБ Банка* относятся:

- сбор и анализ информации о внешних источниках угроз ИБ Банка;
- определение необходимости приобретения средств ИБ;
- проведение аттестации сотрудников Банка на предмет знания требований ИБ;
- расследование всех случаев нарушения ИБ и разработка рекомендаций по итогам расследований;
- координация физических процессов обеспечения ИБ в целом (в том числе обеспечение соблюдение требований ИБ в обособленных подразделениях).

К физическим процессам обеспечения ИБ относятся:

- ограничение физического доступа в Банк;
- организация функционирования охранных и сигнализационных, противопожарных и противоугонных систем и т.п.;
- контроль за соблюдением принципов хранения информации конфиденциального характера и информации ограниченного доступа;
- контроль за системами идентификации сотрудников Банка;
- разработка моделей угроз и проведение профилактических мероприятий по их недопущению;
- анализ возникающих рисков и разработка мер по минимизации возможностей нарушения ИБ;
- ведение журналов регистрации инцидентов ИБ.

Из состава Службы ИБ назначается лицо, ответственное за обеспечение ИБ (сотрудник, выполняющий роль администратора ИБ).

В его функции входит:

- управлять всеми планами по обеспечению ИБ Банка;
- разрабатывать и вносить предложения по оптимизации Политики ИБ;
- систематизировать информацию о возникающих рисках ИБ, вести журнал инцидентов ИБ;
- организовывать работу структурных подразделений Банка по обеспечению ИБ;
- контролировать соблюдение сотрудниками Банка принципов ИБ;
- расследовать события, связанные с нарушением ИБ.

СУИБ реализуется специализированной подсистемой, представляющей собой совокупность органов управления, технических, программных и криптографических средств и организационных мероприятий, и взаимодействующих друг с другом пунктов управления различных уровней.

Органом управления специализированной подсистемы является Служба ИБ Банка.

Существуют информационная, управляющая и вспомогательная функции подсистемы управления.

Информационная функция заключается в непрерывном контроле состояния системы защиты, проверке соответствия показателей защищенности допустимым значениям и немедленном информировании сотрудников Службы ИБ о возникающих в АБС ситуациях, способных привести к нарушению ИБ. К контролю состояния системы защиты предъявляются два требования: полнота и достоверность. Полнота характеризует степень охвата всех средств защиты и параметров их функционирования. Достоверность контроля характеризует степень адекватности значений контролируемых параметров их истинному значению. В результате обработки данных контроля формируется информация состояния системы защиты, которая обобщается и передается на вышестоящие пункты управления.

Управляющая функция заключается в формировании планов реализации технологических операций ИБС с учетом требований ИБ в условиях, сложившихся для данного момента времени, а также в определении места возникновения ситуации уязвимости информации и предотвращении ее утечки за счет оперативного блокирования участков АБС, на которых возникают угрозы ИБ. К управляющим функциям Управление ИБ относятся учет, хранение, и выдача документов и информационных носителей, паролей и ключей. При этом генерация паролей, ключей, сопровождение средств разграничения доступа, приемка включаемых в программную среду АБС новых программных средств, контроль соответствия программной среды эталону, а также контроль за ходом технологического процесса обработки информации конфиденциального характера возлагается на администратора автоматизированной системы (базы данных) и сотрудника Управления ИБ.

К *вспомогательным функциям* подсистемы относятся учет всех операций, выполняемых в АБС с защищаемой информацией, формирование отчетных документов и сбор статистических данных с целью анализа и выявления потенциальных каналов утечки информации.

10 Оценка и контроль обеспечения требуемого уровня защищенности информации.

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет НСД, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Контроль в процессе организационного, информационного и технического взаимодействия в АБС проводится сотрудником Службы ИБ Банка.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Контроль может осуществляться администратором ИБ как с помощью штатных средств системы защиты информации от НСД, так и с помощью специальных программных средств контроля.

Контроль эффективности СУИБ осуществляется Руководством Банка (в части общего контроля) и Службы внутреннего контроля (в части осуществления проверок).

В случае выявления текущих угроз ИБ Службы ИБ, Служба внутреннего контроля, а также Президент Банка, могут вырабатывать экстренные меры по обеспечению устранения угроз ИБ.

Банк по результатам оценки соответствия в целях ее документального подтверждения формирует отчет, который утверждается исполнительными органами управления и хранится в порядке, установленном в Банке.

Сотрудник Службы ИБ:

- обеспечивают текущий анализ затрат и результатов, обеспечивается их оптимизация;
- последовательно выполняют анализ ИБ Банка и рисков нарушения ИБ, а также возможных негативных воздействий;
- проводят краткие занятия с сотрудниками Банка по вопросам обеспечения ИБ;
- проводят аттестации персонала по вопросам обеспечения ИБ;
- осуществляют регулярные стандартизованные проверки на возможность вторжения в ИБС;
- совершенствуют защитные меры с учетом накопленного в Банке практического опыта, а также на основе опыта других кредитных организаций.

11 Порядок утверждения, внесения изменений и дополнений

Политика является документом общего доступа и предназначена для ознакомления каждым сотрудником Банка.

Политика подлежит пересмотру при изменении целей и задач Банка в области обеспечения ИБ, функций подразделений, выполняющих функции управления ИБ, или изменении требований законодательства, нормативных актов Банка России в сфере ИБ в кредитных организациях на территории Российской Федерации. Пересмотр и изменение политики проводит администратор ИБ Банка.

Для дополнения Политики могут использоваться политики по направлениям и положения ИБ, разрабатываемые Службы ИБ Банка, согласованные и утвержденные в порядке, установленном в Банке.

Председатель Правления КБ «Максима» (ООО) Г.Л. Быковский

Прошито, пронумеровано и скреплено печатью
на 53 (пятьдесят три) листах
Председатель Правления КБ «Максима (ООО)
_____ Быковский Г.Л.
«___» _____ 202 г.

Коммерческий Банк "Максима" "Maxima Bank" Limited