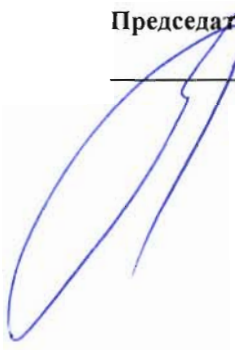
«УТВЕРЖДЕНО»
Правлением
“ИНТЕРПРОГРЕССБАНК”
(Акционерное общество)
Протокол №14 от «18» 04 2016г.
Председатель Правления
_____ Д.А. Яковлев



ПОЛИТИКА
информационной безопасности
«ИНТЕРПРОГРЕССБАНК” (Акционерное общество)

г. Москва
2016 г.

Оглавление

1. Общие положения

Политика информационной безопасности (далее - Политика) «ИНТЕРПРОГРЕССБАНК” (Акционерное общество) определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется «ИНТЕРПРОГРЕССБАНК” (Акционерное общество) (далее – Банк) в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Банке.

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.

Основные положения и требования данного документа распространяются на все структурные подразделения Банка. Основные вопросы Политики также распространяются на другие организации и учреждения, взаимодействующие с Банком в качестве поставщиков и потребителей информационных ресурсов Банка в том или ином качестве (с включением в договор требований информационной безопасности (далее - ИБ).

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации.

Настоящая Политика подготовлена на основании:

- Стандарта Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;
- Стандарта Банка России СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности»;
- Стандарта Банка России СТО БР ИББС-1.2 «Обеспечение информационной безопасности организации банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»;
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»;
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»;
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»;
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.5 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»;

- Рекомендации в области стандартизации Банка России РС БР ИББС-2.6 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».

- Рекомендации в области стандартизации Банка России РС БР ИББС-2.7 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности».

- Рекомендации в области стандартизации Банка России РС БР ИББС-2.8 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации».

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.

Руководству Банка необходимо инициировать, поддерживать и контролировать выполнение процессов системы обеспечения информационной безопасности (далее – СОИБ). Степень выполнения указанной деятельности со стороны руководства Банка определяется осознанием необходимости обеспечения ИБ Банка. Осознание необходимости обеспечения ИБ Банка проявляется в использовании руководством Банка бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса Банка с допустимыми рисками.

Осознание необходимости обеспечения ИБ должно являться побудительным мотивом руководства Банка постоянно инициировать, поддерживать, анализировать и контролировать СОИБ, т.е. принимать решения о выполнении деятельности по обеспечению информационной безопасности Банка до возникновения угроз ИБ.

Осознание необходимости обеспечения ИБ Банка выражается посредством выполнения в рамках системы менеджмента информационной безопасности (далее – СМИБ) деятельности со стороны руководства, направленной на инициирование, поддержание, анализ и контроль СОИБ Банка.

2. Термины, определения и сокращения

Автоматизированная банковская система (АБС) - Автоматизированная система, реализующая технологию выполнения функций Банка.

Автоматизированная система (АС) - Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) - Программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. АРМ объединяет программно-аппаратные средства, обеспечивающие взаимодействие человека с компьютером.

Авторизация - Предоставление прав доступа.

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

Администратор ИБ - 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 и находится в его распоряжении (Примечание: К активам Банка могут относиться: работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства

и пр.; различные виды банковской информации платежная, финансово–аналитическая, служебная, управляющая, персональные данные и пр.; банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы); банковские продукты и услуги, предоставляемые клиентам).

Атака на информационную систему - Любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы.

Аудит информационной безопасности (аудит ИБ) - Систематический, независимый и документируемый процесс получения свидетельств деятельности Банка по обеспечению ИБ, установления степени выполнения в Банке критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ Банка (Примечание: Аудит ИБ выполняется работниками организации, являющейся внешней по отношению к Банку).

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

Банковская система Российской Федерации - Банк России и кредитные организации, а также филиалы и представительства иностранных банков.

Банковский информационный технологический процесс (БИТП) - Часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования Банка и не являющихся платежной информацией (Примечание: Платежная информация - информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой; Неплатежная информация, необходимая для функционирования Банка, может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию).

Банковский платежный технологический процесс (БПТП) - Часть банковского технологического процесса, реализующая банковские операции над информационными активами Банка, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

Банковский технологический процесс - Технологический процесс, реализующий операции по изменению и (или) определению состояния активов Банка, используемых при функционировании или необходимых для реализации банковских услуг (Примечание: Операции над активами Банка могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем; В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.).

Безопасность - Состояние защищенности интересов (целей) Банка в условиях угроз.

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

Безопасность информационной технологии - Защищенность технологического процесса переработки информации.

Безопасность субъектов информационных отношений - Защищенность жизненно важных интересов субъектов информационных отношений от нанесения им материального, морального или иного вреда путем воздействия на информацию и/или средства ее обработки и передачи. Безопасность достигается путем реализации единой политики 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 измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы.

Выводы аудита информационной безопасности (выводы аудита ИБ) - Результат оценки собранных свидетельств аудита ИБ.

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

Дистанционное банковское обслуживание (ДБО) - предоставление банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом, с использованием линий связи.

Документ - Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (Примечание: Под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.).

Документация - Совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

Допустимый риск нарушения информационной безопасности - Риск нарушения ИБ, предполагаемый ущерб от которого Банк в данное время и в данной ситуации готов принять.

Доступ к информации - Ознакомление с информацией или получение возможности ее обработки. Доступ к информации регламентируется ее правовым режимом и должен сопровождаться строгим соблюдением его требований. Доступ к информации, осуществленный с нарушениями требований ее правового режима, рассматривается как несанкционированный доступ.

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

Доступность информации – Важнейшее свойство системы, в которой циркулирует информация, 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, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Естественные угрозы - это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

Жизненно важные интересы - Совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта.

Заключение по результатам аудита информационной безопасности (аудиторское заключение/заключение по результатам аудита ИБ) - Качественная или количественная оценка соответствия установленным критериям аудита ИБ, представленная аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.

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 правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

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

Защищаемая информация - Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

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.

Информационная безопасность (ИБ) - Безопасность, связанная с угрозами в информационной сфере (Примечания: Защищенность достигается обеспечением совокупности свойств ИБ - доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) Банка; Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений).

Информационная инфраструктура - Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия (Примечание: Информационная инфраструктура - включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам).

Информационная система - Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных (ИСПДн) - 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.

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

Информационные ресурсы - Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

Информационные способы нарушения безопасности информации - Действия включающие: 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.

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

Информация - Сведения (сообщения, данные) независимо от формы их представления.

Инфраструктура - Комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи).

Инцидент информационной безопасности (инцидент ИБ) - Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ (Примечания: Реализация угрозы ИБ - реализация нарушения свойств ИБ информационных активов Банка; Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов).

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 ее 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.

Коммерческая тайна - конфиденциальные сведения, составляющие коммерческую тайну Банка, согласно утвержденному перечню сведений, составляющих коммерческую тайну Банка.

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

Комплекс средств автоматизации автоматизированной банковской системы - Совокупность всех компонентов автоматизированной банковской системы Банка, 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 конфиденциальной 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.

Конфиденциальные сведения (данные) - Персональные данные, банковская, коммерческая, служебная и другие виды тайн Банка.

Корпоративная информационная система - Автоматизированная система обработки информации Банка.

Критерии оценки (аудита) информационной безопасности (критерии оценки (аудита) ИБ) - Совокупность требований в области ИБ, определенных стандартом Банка России СТО БР ИББС-1.0 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" или его частью.

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 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.

Модель угроз ИБ - Описание 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.

Мониторинг - Постоянное наблюдение за объектами и субъектами, влияющими на ИБ Банка, а также сбор, анализ и обобщение результатов наблюдений.

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, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Нарушитель - Это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных 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.

Нарушитель информационной безопасности (нарушитель ИБ) - Субъект, реализующий угрозы ИБ Банка, нарушая предоставленные ему полномочия по доступу к активам Банка или по распоряжению ими.

Несанкционированное действие - Действие субъекта в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ (НСД) - Доступ субъекта к объекту в нарушение

установленных в системе правил разграничения доступа.

Область аудита информационной безопасности (область аудита ИБ) - Содержание и границы аудита ИБ (Примечание: Область аудита ИБ обычно включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются аудиту ИБ, а также охватываемый период времени).

Область действия системы обеспечения информационной безопасности (область действия СОИБ) - Совокупность информационных активов и элементов информационной инфраструктуры Банка.

Обработка риска нарушения информационной безопасности - 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 обеспечивается защита 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 и т.д.).

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 соответствия полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Осознание необходимости обеспечения информационной безопасности (осознание 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. (Примечание: Осознание ИБ является внутренней побудительной причиной для руководства банковской системы Российской Федерации инициировать и поддерживать деятельность по обеспечению ИБ, в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по обеспечению ИБ определяется соответственно либо возникшими проблемами организации, либо внешними факторами, например, требованиями законов).

Остаточный риск нарушения информационной безопасности - Риск, остающийся после обработки риска нарушения ИБ.

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

Пароль - Набор символов (состоящий из цифр, букв и прочих символов) известен

узкому кругу лиц (одному лицу) предназначенный для подтверждения личности или полномочий и используется для ограничения доступа к информации.

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

План работ по обеспечению информационной безопасности - 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.

Политика информационной безопасности (ПИБ) - Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для Банка в целом.

Пользователь - Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Правила разграничения доступа - Совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

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

Программа аудита информационной безопасности (программа аудита ИБ) - План деятельности по проведению одного или нескольких аудитов ИБ (и других проверок ИБ), запланированных на конкретный период времени и направленных на достижение конкретной цели. (Примечание: Программа аудита ИБ включает всю деятельность, необходимую для планирования).

Программно-математические способы нарушения безопасности информации - Включают: внедрение программ-вирусов; внедрение программных закладок как на стадии проектирования системы (в том числе путем заимствования «зараженного» закладками программного продукта), так и на стадии ее эксплуатации, позволяющих осуществить несанкционированный доступ или действия по отношению к информации и системам ее защиты (блокирование, обход и модификация систем защиты, извлечение, подмена идентификаторов и т.д.) и приводящих к компрометации системы защиты информации.

Процесс - Совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы.

Радиоэлектронные способы нарушения безопасности информации - Включают: перехват информации в технических каналах ее 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, путем 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 - Порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Регистрация - Фиксация данных о совершенных действиях (событиях).

Рекомендации в области стандартизации - Документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего стандарта.

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

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

Риск нарушения информационной безопасности (риск нарушения ИБ) - Риск, связанный с угрозой ИБ.

Роль - Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом (Примечания: К субъектам относятся лица из числа руководителей Банка, ее 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 информационной безопасности - Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ Банка.

Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям (свидетельства оценки соответствия (аудита) ИБ) - Записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия (самооценки соответствия, аудита) ИБ и могут быть проверены. (Примечание: Свидетельства оценки соответствия (самооценки соответствия, аудита) ИБ могут быть качественными или количественными).

Секретная информация - Речевая информация, информация, циркулирующая в средствах вычислительной техники и связи, телекоммуникациях, а также другие информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, представленные в виде информативных акустических и электрических сигналов, физических полей, материальных носителей (в том числе на магнитной и оптической основе), информационных массивов и баз данных.

Система - Множество (совокупность) материальных объектов (элементов) любой, в том числе различной физической, природы и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающее системным свойством (свойствами). (Примечание: Системным свойством (свойствами) является свойство, которое не имеет ни один из элементов и ни одно из подмножеств элементов при любом способе членения. Системное свойство не выводимо непосредственно из свойств элементов и частей).

Система ИБ (СИБ) - Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента ИБ (СМИБ) - Часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

Система обеспечения ИБ (СОИБ) - Совокупность СИБ и СМИБ Банка.

Средство защиты информации (СЗИ) - Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

Средство криптографической защиты информации (СКЗИ) – Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Стандарт - Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. (Примечание: Стандарт также может

содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения).

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, приемов предметной деятельности.

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

Угроза - Опасность, предполагающая возможность потерь (ущерба).

Угроза безопасности информации - Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее 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.

Угроза информационной безопасности (угроза ИБ) - Угроза нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов Банка.

Уровень защиты (класс и категория защищенности) - Характеристика, описываемая в нормативных документах определенной группой требований к данному классу и категории защищенности.

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 информационной безопасности (уязвимость ИБ) - Слабое место в инфраструктуре Банка, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

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 ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Целостность информационных активов - Свойство ИБ Банка сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

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.

Частная политика информационной безопасности (частная политика ИБ) - Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка.

Электронная цифровая подпись (ЭЦП) - Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

БС - банковская система;
ЖЦ - жизненный цикл;
НРД - нерегламентированные действия в рамках предоставленных полномочий;
ПО - программное обеспечение;
РФ - Российская Федерация;
ЭВМ - электронная вычислительная машина.

3. Объекты защиты

Основными объектами системы информационной безопасности в Банке являются:

- информационные *ресурсы* с ограниченным доступом, составляющие конфиденциальную информацию, в том числе 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 ее 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;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее 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 объектов защиты, информационные связи

Информационная среда Банка является распределенной структурой, объединяющей информационные подсистемы Головного офиса и внутренних структурных подразделений, включая Дополнительные офисы и ОКВКУ в единую информационную систему Банка.

К основным особенностям информационной среды Банка относятся:

- широкая территориальная распределенность компонентов информационной системы (Головной офис, Дополнительные офисы и другие внутренние структурные подразделения);

- значительное расширение сферы использования автоматизированных систем обработки информации;

- разнообразие решаемых задач (от подготовки и отправки платежей до внедрения дистанционного банковского обслуживания);

- значительная важность и ответственность решений, принимаемых на основе автоматизированной обработки данных (подготовка отчетности, подготовка рейсов, отправка денежных переводов и др.);

- объединение в единых базах 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) (сеть Интернет и другие специализированные компьютерные сети);

- интенсивность информационных потоков между подразделениями Банка;

- разнообразие категорий доступа обслуживающего персонала к эксплуатируемым системам.

3.2. Категории информационных ресурсов, подлежащих защите

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

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

- сведения, составляющие банковскую тайну, доступ к которым ограничен в соответствии с Федеральным законом от 02.12.1990 № 395-I «О банках и банковской деятельности»;

- сведения, составляющие коммерческую тайну, доступ к которым ограничен в соответствии с Федеральным законом от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»;

- сведения являющиеся персональными данными, доступ к которым регулируется

Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- прочие виды тайн, а также открытая информация, необходимая для обеспечения функционирования Банка.

3.3. Классификация информационных активов, подлежащих защите

По природе существования активы (ценности) классифицируются:

- материальные – ценности, существующие в виде предметов. Например: системные блоки ЭВМ и мониторы, носители информации (жесткие диски, съемные накопители, гибкие диски), провода ЛВС, маршрутизаторы и другое сетевое оборудование, договоры с печатями и атрибутами сторон в бумажном виде, принтеры, ксероксы, многофункциональные устройства, банкоматы, терминалы;
- нематериальные – ценности, содержащие сведения, которые хранятся на специальных носителях, в файловых контейнерах или каталогах, передаются по проводным и беспроводным каналам связи, обрабатываются техническими и программными средствами. Например:
- информация о клиентах;
- состояние счетов клиентов;
- операции, проводимые по счетам;
- настройки систем защиты информации;
- ключевая информация для расшифровывания и создания ЭЦП;
- операции, проводимые без открытия счетов;
- имена, пароли и другая информация, используемая для получения доступа к ЭВМ, ЛВС или к техническим и программным средствам.

Материальные активы (ценности) должны защищаться организационными, инженерными и техническими способами, методами физической охраны и периодической проверкой наличия и исправности.

Нематериальные активы (ценности) должны защищаться техническими и программными способами, методами распределения прав доступа, регистрации доступа и выполняемых операций.

Допускается использование иных способов, методов и технологий, позволяющих обеспечить защиту материальных и нематериальных активов, если существует возможность проверки правильности их функционирования.

По степени значимости активы (ценности) классифицируются, в порядке убывания приоритета:

- корпоративные - имеющие большую ценность или значимость для всех подразделений Банка, клиентов и контрагентов. Например: документация бухгалтерского учета, АТС (автоматическая телефонная станция), сервер хранения данных АБС, сервер приложений АБС, абонентский пункт системы «АСБР-Москва», абонентский пункт и сервер системы «S.W.I.F.T», почтовый сервер домена «ipb.ru», web-сервер домена «ipb.ru», первичный и вторичный контроллеры домена «ipb.dom», предоставляющие доступ в локальную сеть и т.д.;
- актив (ценность) подразделения – имеющие значение для всего подразделения. Например: файловое хранилище рабочей и отчетной информации, технические и программные средства, используемые всем подразделением, не относящиеся к активам других приоритетов;
- должностные – имеющие значимость для определенных должностных лиц. Например: ЭВМ, закрепленная за каждым из сотрудников, инструкции и справочные материалы, набор рабочих документов сотрудника, почтовый ящик с хранящейся в нем корреспонденцией и пароль на доступ к нему, пароль на доступ к ЭВМ и в локальную сеть;
- общие – имеющие небольшую материальную ценность, но имеющие значимость для всех подразделений Банка. Например: приказы, положения, политики, процедуры,

журналы, описи, реестры и другие внутренние (банковские) или внешние (не банковские) документы, определяющие порядок проведения работ, содержащие параметры настроек систем, указания о накладываемых ограничениях или хранящие свидетельства выполнения какой-либо деятельности.

В других корпоративных или частных политиках активы (ценности) могут классифицироваться по другим признакам. Политики в качестве приложения должны содержать списки активов (ценностей), требования по защите которых она определяет.

Во внутренних документах Банка модель Угроз и модель Нарушителя определена в нормативном документе «Модель Угроз «ИНТЕРПРОГРЕССБАНК” (Акционерное общество)».

3.4. Информационные ценности Банка, подлежащие защите

Информационными ценностями Банка считаются:

- платежная информация об осуществленных расчетах;
- контактная информация о сотрудниках Банка;
- информация о клиентах и контрагентах Банка;
- программные и аппаратные системы;
- настройки программных и аппаратных систем;
- системы обеспечения безопасности;
- настройки систем обеспечения безопасности;
- носители информации и каналы связи;
- знания и умения сотрудников Банка;
- оригиналы юридически значимых документов.

3.5. Информационные интересы Банка

Информационные интересы Банка:

- хранение информационных активов;
- безопасная обработка информационных активов;
- организация системы контроля доступа к информационным активам;
- выявление рисков и угроз информационным активам.

4. Цели и задачи обеспечения безопасности информации

4.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении информационной безопасности 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 (ее доступности);
- достоверности (полноты, точности, адекватности, целостности) информации;
- конфиденциальности (сохранения в тайне) определенной части информации; защиты от навязывания им ложной (недостоверной, искаженной) 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 ее 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, ее носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации Банка, правовой риск и т.д.).

Для достижения указанной цели необходимо обеспечить и постоянно поддерживать следующие свойства информации и самой АБС, ее обрабатывающей:

- доступность информации и операций с ней для зарегистрированных пользователей, устойчивое функционирование АБС Банка, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;

- обеспечение конфиденциальной информации, хранимой, обрабатываемой в АБС и передаваемой по каналам связи;

- целостность и аутентичность информации, хранимой и обрабатываемой в АБС и передаваемой по каналам связи;

- ответственность субъектов информационных отношений за допущенные нарушения порядков и инструкций безопасности, повлекшие за собой ущерб для одного или нескольких субъектов информационных отношений.

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

4.3. Основные задачи системы обеспечения безопасности информации Банка

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

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, 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 служебных 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» криптографических средств защиты информации.

4.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом 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 утвержденных Правлением Банка организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- полнотой, реальной выполнимостью и непротиворечивостью требований регламентирующих документов Банка по вопросам обеспечения информационной безопасности;
- назначением и подготовкой должностных лиц (сотрудников Банка), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности и процессов её обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к ресурсам Банка;
- четким знанием и строгим соблюдением всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АБС, требований регламентирующих документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных 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 защищенности 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 незащищенным каналам связи;
- эффективным контролем со стороны Департамента безопасности 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. Область действия Политики

Область действия Политики распространяется на все виды деятельности, в процессе выполнения которых осуществляется хранение и обработка электронной информации программными и техническими средствами (формирование, прием, передача, модификация), а также, если информация не обрабатывается техническими или программными средствами (содержится на носителях информации не позволяющих обрабатывать ее такими средствами), но подлежит защите.

Настоящая Политика обязательна для использования всеми сотрудниками Банка при разработке документации, касающейся информационной безопасности Банка, путем ссылок на ее цели, ценности, принципы и требования. Этот документ обязателен для соблюдения всеми сотрудниками, клиентами и контрагентами.

Для любого программного или технического средства, используемого или планируемого к использованию, может быть разработана частная политика ИБ, определяющая:

- цели ИБ и способы их достижения;
- конкретные требования ИБ, выполняемые при работе с этим средством;
- список документов процедурного уровня и уровня достигнутых результатов;
- порядок формирования документов уровня достигнутых результатов;
- должностных лиц, ответственных за исполнение и контроль;
- меры ответственности за неисполнение и отсутствие контроля;
- порядок исполнения и контроля;
- список уязвимостей;
- модель угроз и нарушителей.

Порядок соблюдения принципов Политики сотрудниками Банка:

- выполнение должностных инструкций;
- выполнение инструкций по работе с техническими и программными комплексами;
- выполнение правил техники безопасности;
- выполнение общих обязанностей по обеспечению информационной безопасности.

Порядок соблюдения принципов ПИБ клиентами и контрагентами Банка:

- выполнение обязательств, установленных договорами;
- выполнение инструкций по соблюдению информационной безопасности, прилагаемых к договорам на предоставление услуг.

Клиенты могут не выполнять требования ИБ Банка на свой страх и риск (т.е. имеют право принимать на себя такой риск), что должно быть указано в договорах с клиентами на предоставление услуг.

5. Основные угрозы безопасности информации Банка

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 ее 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 ее 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 ее отдельных компонентов;

- воздействия из внутренней сети Банка со стороны сотрудников подразделений Банка, а также удаленное несанкционированное вмешательство посторонних лиц из внешних сетей общего назначения (сети Интернет), используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам Банка;

- ошибки, допущенные при проектировании АБС и ее системы защиты, ошибки в программном обеспечении, 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 персональных данных.

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 правил, инструкций, регламентов и порядков.

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

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 ее 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 путем, используя халатность пользователей, путем 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 съемка для несанкционированного съема 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. Пути реализации основных естественных угроз безопасности информации

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;
- выход из строя или невозможность использования линий связи;
- пожары, наводнения и другие стихийные бедствия.

5.5. Неформальная модель возможных нарушителей

СОИБ Банка строится исходя из предположений о следующих возможных типах нарушителей (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и т.д.):

- Некомпетентный (невнимательный) пользователь - сотрудник Банка (или подразделения другой организации, являющийся сотрудником информационной системы Банка), который может предпринимать попытки выполнения запрещенных 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 сотрудник другой 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 запрещенных 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 разрешенных средств). Помимо 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 нанесенную 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 подразделений обеспечения безопасности Банка;
- 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 определенных полномочий по доступу к информационным ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций.

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 Департамента безопасности.

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.

5.6. 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 внедренных в помещения Банка специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных 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 счет 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 ее 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 внедренные электронные и программные средства («закладки»).

Перехват информации ограниченного распространения или воздействие на нее 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 нее 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 приема 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. Основные принципы обеспечения информационной безопасности Банка

6.1. Основные принципы обеспечения информационной безопасности

- Своевременность обнаружения проблем. Банком своевременно обнаруживаются проблемы, потенциально способные повлиять на его бизнес-цели;
- Прогнозируемость развития проблем. Банк выявляет причинно-следственную связь возможных проблем и строит на этой основе точный прогноз их развития;
- Оценка влияния проблем на бизнес-цели. Банк адекватно оценивает степень влияния выявленных проблем на ее бизнес-цели;
- Адекватность защитных мер. Банк выбирает защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз;
- Эффективность защитных мер. Банк стремится эффективно реализовывать принятые защитные меры;
- Использование опыта при принятии и реализации решений. Банк накапливает, обобщает и использует как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения;
- Непрерывность принципов безопасного функционирования. Банк стремится обеспечивать непрерывность реализации принципов безопасного функционирования;
- Контролируемость защитных мер. Банком применяются только те защитные меры, правильность работы которых может быть проверена, при этом Банк стремится регулярно

оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели Банка.

6.2. Специальные принципы обеспечения информационной безопасности

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

- Определенность целей. Функциональные цели и цели ИБ Банка определяются настоящей Политикой;
- Знание своих клиентов и сотрудников. Банк придерживается принципа «знай своего клиента» в соответствии с «Правилами внутреннего контроля «ИНТЕРПРОГРЕССБАНК»(Акционерное общество) в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Банк стремится осуществлять набор квалифицированных кадров, а также поддерживать высокий уровень корпоративной этики, что приводит к формированию благоприятной и доверительной среды для деятельности Банка;
- Персонификация и адекватное разделение ролей и ответственности. Ответственность должностных лиц Банка за решения, связанные с его активами, персонифицируется и осуществляется на основании принятых Банком нормативных документов и правил преимущественно в форме поручительства. Банк стремится к ее адекватной степени влияния на цели организации, фиксированию в политиках, контролю и совершенствованию;
- Адекватность ролей функциям, процедурам и их сопоставимость с критериями и системой оценки. Роли адекватно отражают исполняемые функции и процедуры их реализации, принятые в Банке. При назначении взаимосвязанных ролей учитывается необходимая последовательность их выполнения. Роль согласуется с критериями оценки эффективности ее выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки;
- Доступность услуг и сервисов. Банк стремится обеспечить доступность для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и (или) иными документами;
- Наблюдаемость и оцениваемость обеспечения ИБ. Любые предлагаемые защитные меры устраиваются так, чтобы результат их применения был явно виден (прозрачен) и мог быть оценен подразделением Банка, имеющим соответствующие полномочия.

7. Основные требования по обеспечению информационной безопасности Банка

Требования ИБ формулируются для следующих областей:

- назначение и распределение ролей и доверия к персоналу;
- стадий ЖЦ АБС;
- защиты от НСД, управления доступом и регистрацией в АБС;
- антивирусной защиты;
- использования ресурсов Интернет;
- использования средств криптографической защиты информации;
- защиты банковских платежных и информационных технологических процессов;
- защиты от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи;
- обработки персональных данных.

7.1. Требования по обеспечению информационной безопасности при назначении и распределении 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 информационной безопасности Банка и, как следствие, привести к различным потерям.

В связи с этим, при приеме нового сотрудника на работу в Банк, должны выполняться следующие действия:

- проверка идентичности личности сотрудника;
- проверка квалификации сотрудника;
- проверка полноты указанных биографических фактов;
- изучение и проверка рекомендаций и характеристик с предыдущих мест работы, если таковые имеются.

При приеме на работу, каждый сотрудник должен ознакомиться под роспись с обязательством о соблюдении конфиденциальности и приверженности правилам корпоративной этики Банка и с требованиями по обеспечению ИБ (пройти вводный инструктаж по ИБ). Каждый сотрудник должен подписать согласие на обработку своих 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 (документы) должны быть подшиты в личное дело сотрудника.

На основании бизнес-процессов Правлением Банка должны быть определены и персонифицированы роли персонала с учетом целей Банка, имеющихся ресурсов, функциональных и процедурных требований, а также критериев оценки эффективности выполнения правил для данных ролей.

При определении ролей не допускается создание критичных ролей, концентрирующих в себе все или большинство наиболее важных функций, необходимых для реализации целей Банка.

Департамент безопасности Банка может проводить контрольные проверки сотрудников на предмет выполнения требований ИБ (с документальной фиксацией результатов). Также могут проводиться внеплановые проверки сотрудников (с документальной фиксацией результатов) при выявлении – фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии.

При взаимодействии с внешними организациями и клиентами требования по обеспечению ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

Обязанности персонала по выполнению требований по обеспечению ИБ включаются в должностные инструкции.

7.2. Требования по обеспечению информационной безопасности 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 ЖЦ, является основной задачей процесса обеспечения ИБ Банка.

При заказе АБС выбор модели ЖЦ АБС производится с учетом требований участников его процессов (конечных пользователей АБС, администраторов АБС, администратора ИБ Банка и других возможных участников процессов ЖЦ АБС).

В целях исключения неверных формулировок требований к АБС, технические задания на разработку АБС составляются техническими специалистами (сотрудниками Департамента информационных технологий и/или лицами, привлеченными на экспертной основе), совместно с разработчиками АБС и конечными пользователями АБС.

При составлении технических заданий разработчиком гарантируется защита от принятия неверных проектных решений, внесения ошибок 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.

При приобретении готовых АБС и их компонентов используются те же требования к документации, что и при разработке.

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

Перед началом работы с вновь устанавливаемой или изменяемой АБС все пользователи проходят инструктаж у руководителей своих подразделений и, при необходимости, у администратора АБС. Обо всех инцидентах ИБ или при подозрении на них, пользователи обязаны незамедлительно сообщать об этом администратору АБС и администратору ИБ Банка. Администратор ИБ информирует начальника Управления ИБ, который сообщает об этом директору Департамента безопасности Банка.

По факту выявленных нарушений и инцидентов ИБ в АБС Департамент безопасности Банка проводит служебное расследование.

С точки зрения обеспечения безопасности информации критическими компонентами АБС являются:

- серверы АБС, на которых располагается информация, подлежащая защите;
- АРМ администраторов АБС и операторов АБС, с которых происходит управление процессами обработки информации;
- сетевое оборудование и каналы связи.

Защита информации АБС от НСД производится как встроенными в АБС средствами защиты информации, так и другими сертифицированными или разрешенными руководством Банка средствами.

Для каждого участника, а так же группы участников, информационно-технологического процесса, реализуемого АБС, создается уникальный идентификатор (логин). Для аутентификации пользователя применяется данный логин и пароль, известный только пользователю, что позволяет однозначно идентифицировать пользователя и обеспечить защиту от угрозы отказа от авторства.

Безопасность информации на уровне каналов связи достигается путем организации резервных каналов предоставляемых разными провайдерами.

Перед выведением из эксплуатации АБС или ее отдельных компонентов вся хранимая ими информация переносится администратором АБС в архив и удаляется из постоянной памяти и с внешних носителей АБС. Контроль за удалением информации осуществляют сотрудники Департамента безопасности Банка. После удаления информации из постоянной памяти АБС и/или с внешних носителей составляется акт. Выведение из эксплуатации АБС или ее компонентов, также оформляется соответствующим актом.

7.3. Требования по обеспечению информационной безопасности при управлении доступом и регистрации

Для обеспечения защиты информации от НСД используется управление доступом к её ресурсам. Создается и регулярно уточняется перечень ресурсов и определяются владельцы каждого ресурса.

Обязанности по обеспечению ИБ в структурных подразделениях Банка возлагаются на руководителей подразделений.

Назначение (изменение, лишение) полномочий по доступу пользователя к ресурсам АБС санкционируется руководителем структурного подразделения пользователя и согласовывается с Департаментом безопасности Банка.

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

7.4. Требования по обеспечению информационной безопасности средствами антивирусной защиты

Все АРМ Банка и серверы защищаются от внедрения вредоносного и шпионского ПО официально приобретенными и регулярно обновляемыми средствами антивирусной защиты.

На АРМ и серверах Банка запрещена установка ПО, не предназначенного для реализации их основного предназначения – организации и поддержки информационно-технологических процессов Банка. Контроль несанкционированной установки ПО осуществляют сотрудники Департамента информационных технологий Банка.

Вновь устанавливаемое или изменения в установленное ПО должно быть предварительно проверено на отсутствие вирусов. После установки нового ПО или изменений в ранее установленное ПО должна быть выполнена полная антивирусная проверка.

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

Отключение или несвоевременное обновление антивирусных средств не допускается.

В Банке необходимо поддерживать в актуальном состоянии организованную антивирусную фильтрацию всего трафика электронного почтового обмена.

7.5. Требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет

Функционирование Банка без взаимодействия с сетью Интернет принципиально невозможно. Основными целями использования сети Интернет являются:

- ведение ДБО;
- получение и распространение информации, связанной с банковской деятельностью;
- информационно-аналитическая работа в интересах Банка;
- обмен электронными сообщениями и т.д.

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

В Банке предпринимаются следующие методы защиты от угроз:

- Все рабочие станции и серверы, взаимодействующие с сетью Интернет, находятся изолированно от остальных банковских информационных ресурсов.
- Вся защищаемая информация, которая передается через сеть Интернет, в обязательном порядке шифруется с помощью соответствующих средств криптографической защиты информации для обеспечения ее защиты в случае перехвата;
- Доступ сотрудников к ресурсам сети Интернет осуществляется на основании служебных записок руководителей структурных подразделений Банка.
- Контроль использования ресурсов Интернет пользователями возложен на ответственных сотрудников Департамента безопасности Банка. Все случаи использования сети Интернет не являющимися необходимыми для работы, рассматриваются как нарушения ИБ Банка;
- Сотрудникам предоставляются минимально необходимые права доступа к сервисам и ресурсам сети Интернет в соответствии с назначенными сотрудникам ролями. В соответствии с должностными инструкциями сотрудников Банка использование ресурсов сети Интернет в неустановленных целях запрещено.

- Запрещена передача конфиденциальной информации, содержащей банковскую, коммерческую тайну или персональные данные, а также другой защищаемой Банком информации в открытом виде через сеть Интернет;

- На всех рабочих станциях и серверах, взаимодействующих с сетью Интернет должны быть установлены средства антивирусной защиты информации.

Обо всех выявленных нарушениях ИБ Банка при работе с сетью Интернет, Администратор ИБ сообщает начальнику Управления ИБ, который информирует директора Департамента безопасности Банка.

7.6. Требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

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

Выбор и приобретение СКЗИ согласовывается с Департаментом безопасности 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 России;

- они имеют строгий регламент использования ключей, предполагающий контроль со стороны администратора ИБ Банка за действиями пользователя при работе 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.

Дополнительная информация о работе Банка с СКЗИ отражена во внутренних положениях и инструкциях пользователей Банка, связанных с СКЗИ.

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

7.7. Требования по обеспечению информационной безопасности платежных технологических процессов Банка

Система обеспечения информационной безопасности банковского платежного технологического процесса должна соответствовать требованиям Стандарта Банка России СТО БР ИББС-1.0 и иных нормативных документов по вопросам информационной безопасности, действие которых распространяется на банковскую систему Российской Федерации.

Порядок обмена платежной информацией должен быть определен в договорах между Банком и клиентами: кредитными организациями, юридическими и физическими лицами.

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

Необходимо применять средства защиты от НСД и СКЗИ на средствах вычислительной техники, на которых осуществляются операции с платежной информацией.

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

Комплекс мер по обеспечению информационной безопасности банковского платежного технологического процесса предусматривает:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов;
- минимально необходимый, гарантированный доступ сотрудника Банка только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию обрабатываемой платежной информации;
- двустороннюю аутентификацию АРМ (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- сверку выходных платежных сообщений с соответствующими поступившими платежными сообщениями;
- гарантированную доставку платежных сообщений участникам информационного обмена.

Банк также выполняет требования международных платежных систем по обеспечению информационной безопасности в части выполняемых им операций.

7.8. Требования по обеспечению информационной безопасности информационных технологических процессов Банка

СИБ информационного технологического процесса Банка должна соответствовать требованиям пунктов 7.1-7.6, 7.8 настоящей Политики.

Неплатежная информация Банка подразделяется на:

- общедоступную, т.е. доступную сотрудникам Банка, внешним пользователям, клиентам и контрагентам. К данному типу информации может относиться публикуемая отчетность, данные о ставках по вкладам и иным видам банковских услуг, общая информация о Банке и т.п.; данная информация может распространяться путем размещения ее на сайте Банка, выпуске рекламных проспектов, стендов в операционных залах. Требованием ИБ к данному виду информации является ее достоверность, которая обеспечивается лицами, ответственными за ее распространение;
- информацию ограниченного доступа (конфиденциальную), т.е. доступ к которой ограничивается в соответствии с законодательством РФ и с внутренними нормативными документами Банка. Данная информация должна храниться с обеспечением требований к ее сохранности — в сейфах, запирающихся шкафах или ящиках. Для обеспечения сохранности такой информации и контроля за доступом к ней могут назначаться ответственные сотрудники Банка; может вводиться режим ограничения распространения такой информации — запрет на снятие копий, ограничение физического выноса документов из мест их хранения и т.п. Конфиденциальная информация, хранящаяся

исключительно на электронных носителях, должна быть защищена комплексом технических и программных мер.

Обязанности по администрированию средств защиты неплатежной информации необходимо возлагать приказом или распоряжением на соответствующих сотрудников Банка с отражением этих обязанностей в их должностных инструкциях.

Все сотрудники Банка при приеме на работу дают письменное обязательство о соблюдении конфиденциальности.

7.9. Требования по обработке персональных данных в Банке

В Банке необходимо документально зафиксировать и утвердить цели обработки ПДн, а также определить необходимость уведомления Уполномоченного органа по защите субъектов персональных данных об обработке ПДн.

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

- специальные категории ПДн;
- биометрические категории ПДн;
- общедоступные и обезличенные ПДн;
- иные ПДн (ПДн которые не могут быть отнесены к вышеперечисленным категориям).

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

Банк должен прекратить обработку ПДн и уничтожить собранные ПДн, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

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

В Банке необходимо определить и документально зафиксировать:

- порядок уничтожения ПДн (в том числе и материальных носителей ПДн);
- порядок обработки обращений субъектов ПДн (или их законных представителей) по вопросам обработки их ПДн;
- порядок действий в случае запросов Уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн;
- подход к отнесению АБС или его частей к ИСПДн;
- перечень ИСПДн;
- список должностей Банка, участвующих в технологических процессах, в раках которых обрабатываются ПДн;
- порядок доступа сотрудников Банка и иных лиц в помещения, в которых ведется обработка ПДн;
- порядок хранения материальных носителей ПДн.

Для каждой ИСПДн Банка должны быть определены и документально зафиксированы:

- цель обработки ПДн;

- объем и содержание обрабатываемых ПДн;
- перечень действий с ПДн и способы их обработки.

Объем и содержание персональных данных, а также перечень действий и способы обработки ПДн должны соответствовать целям обработки. В том случае, если для выполнения банковского информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных ПДн, эти ПДн должны быть удалены.

В Банке должен быть определен и документально зафиксирован перечень (список) сотрудников, осуществляющих обработку ПДн в ИСПДн либо имеющих доступ к ПДн. Допускается указание сотрудников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью.

Доступ сотрудников Банка к ПДн и обработка ПДн сотрудниками Банка должны осуществляться только для выполнения их должностных обязанностей.

Сотрудники Банка, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых ПДн, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

При обработке в Банке ПДн на бумажных носителях, в частности, при использовании в Банке типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, должны соблюдаться требования, установленные "Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденным Постановлением Правительства РФ от 15.09.2008 г. №687.

8. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных

8.1. Общие требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных любого класса

Требования по обеспечению безопасности ПДн в ИСПДн в общем случае реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

Организация выполнения и (или) реализация требований по обеспечению безопасности ПДн должна осуществляться Департаментом безопасности Банка, либо на договорной основе организацией — контрагентом, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Реализация требований по обеспечению безопасности ПДн осуществляется по согласованию и под контролем Департамента безопасности Банка.

Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в эксплуатацию ИСПДн должны осуществляться по согласованию и под контролем Департамента безопасности Банка.

Сотрудники, осуществляющие обработку ПДн в ИСПДн, должны действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования документов Банка по обеспечению ИБ.

Параметры конфигурации средств защиты и механизмов защиты информации от НСД определяются в эксплуатационной документации на ИСПДн. Порядок и периодичность проверок установленных параметров конфигурации устанавливаются в эксплуатационной документации или регламентируются внутренним документом Банка.

Пользователи и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование ПДн.

8.2. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки общедоступных и (или) обезличенных персональных данных

Процессы обработки ПДн, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн в проектной и эксплуатационной документации.

Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю.

Передача ПДн должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию с Департаментом безопасности.

8.3. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным

Для ИСПДн, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным, применяются все требования по обеспечению безопасности, определенные в разделе 8.2, а также следующие требования.

Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время входа в систему (выхода из системы) субъекта доступа;
- идентификатор субъекта, предъявленный при запросе доступа;
- результат попытки входа: успешная или неуспешная (несанкционированная);
- идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журнале регистрации событий.

Снятие с учета машинных носителей, на которых были размещены ПДн, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения.

Сохранность и целостность программных средств ИСПДн и ПДн являются обязательными и обеспечиваются в том числе за счет создания резервных копий.

Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, восстановления, учета, хранения, использования (для восстановления) и уничтожения резервных копий, регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

Выполнение функций обеспечения безопасности ПДн в ИСПДн должно обеспечиваться средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия(когда применение таких средств необходимо для нейтрализации актуальных угроз), а также комплексом встроенных механизмов защиты ЭВМ, операционных систем, систем управления базами данных, ПО.

8.4. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки биометрических персональных данных

Для информационных систем обработки биометрических персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 8.3, а также требования, установленные Постановлением Правительства от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8.5. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки специальных категорий персональных данных

Для информационных систем обработки специальных категорий ПДн применяются все требования по обеспечению безопасности, определенные в разделе 8.3, а также следующие требования:

- Идентификация информационных ресурсов (например, информационных массивов, баз данных, файлов, обрабатывающих их программ), содержащих ПДн, должна осуществляться по логическим именам.
- Контроль доступа субъектов к защищаемым информационным ресурсам в соответствии с правами доступа указанных субъектов является обязательным.
- Регистрация печати материалов, содержащих персональные данные, является обязательной.
- Регистрация запуска программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам, является обязательной.
- Регистрация изменений полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов) является обязательной.
- В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журналах регистрации событий.
- Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.
- Должно быть исключено использование программных средств, предназначенных для разработки и отладки ПО (либо содержащих средства разработки, отладки и тестирования программно-аппаратного обеспечения) с целью недопущения изменения состава ПО ИСПДн.
- Передача ПДн между подразделениями Банка должна осуществляться только при обеспечении их защиты с помощью организации виртуальных частных сетей (Virtual Private Network — VPN) или иных защитных мер, механизмов и средств.
- Передача ПДн по телекоммуникационным каналам и линиям связи между подразделениями Банка, с одной стороны, и внешними организациями, с другой стороны, должна осуществляться с использованием сертифицированных СКЗИ или иных защитных механизмов.
- Подключение ИСПДн к ИСПДн другого класса или к сети Интернет должно осуществляться с использованием средств межсетевого экранирования (межсетевых экранов), которые должны иметь подтвержденный сертификатом класс защиты не ниже четвертого при возможности информационного обмена между всеми компонентами защищаемой ИСПДн без использования компонентов других АБС (в иных случаях - не ниже третьего класса).

9. Требования к проведению самооценки информационной безопасности

Самооценка ИБ проводится в соответствии со стандартом Банка России 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» не реже одного раза в три года. Порядок проведения самооценки ИБ организовывается в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

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

Перед проведением самооценки необходимо документально определить:

- порядок формирования, сбора и хранения свидетельств самооценки ИБ;
- периодичность проведения самооценки ИБ;
- порядок хранения и использования результатов самооценки ИБ.

Так же необходимо документально оформить план проведения самооценки, определяющий:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- порядок и сроки выполнения мероприятий самооценки ИБ;
- распределение ролей среди работников Банка, связанных с проведением самооценки ИБ.

По результатам проведения самооценки ИБ должны быть подготовлены отчеты. Результаты самооценок ИБ, а также соответствующие отчеты должны быть доведены до руководства Банка в формах, представленных в Стандарте 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».

В Банке должны быть документально определены роли, связанные с выполнением программы самооценки ИБ, и назначены ответственные за выполнение указанных ролей.

Результаты самооценки Банка должны быть оформлены в виде «Подтверждения соответствия Банка требованиям стандарта Банка России СТО БР ИББС-1.0» с указанием соответствия в целом и по направлениям Регуляторов - Роскомнадзора, ФСБ России и ФСТЭК России (в пределах их полномочий). Данный документ направляется в адрес Банка России и территориальных органов Регуляторов.

10. Требования к проведению аудита информационной безопасности

Аудит ИБ Банка должен 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 аудита необходимо документально определить и реализовать программу аудита ИБ, содержащую информацию, необходимую для планирования и

организации аудита ИБ, его контроля, анализа и совершенствования, а также обеспечения его ресурсами, необходимыми для эффективного и результативного проведения указанного аудита 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.

В Банке 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 Банка;
- порядок организации наблюдения за деятельностью сотрудников Банка со стороны представителей аудиторской организации.

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

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

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

11. Требования к системе обеспечения информационной безопасности

11.1. Требования к принятию руководством Банка решений о реализации и эксплуатации системы обеспечения информационной безопасности

Решения о реализации и эксплуатации СОИБ должны утверждаться руководством Банка. В частности, требуется документально оформить решения руководства:

- об анализе и принятии остаточных рисков нарушения ИБ;
- о планировании этапов внедрения СОИБ;
- о распределении ролей в области обеспечения ИБ Банка;
- о принятии со стороны руководства планов внедрения защитных мер и снижение рисков ИБ;
- о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

Все планы внедрения СОИБ, планы обработки рисков нарушения ИБ и внедрения защитных мер должны быть утверждены руководством Банка. Указанные планы должны документально фиксировать:

- последовательность выполнения мероприятий в рамках указанных планов;
- сроки начала и окончания запланированных мероприятий;
- должностных лиц (подразделения), ответственных за выполнение каждого указанного мероприятия.

Должен быть документально определен порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ Банка.

11.2. Требования к организации реализации планов внедрения системы обеспечения информационной безопасности

В Банке должны быть документально определены и выполняться проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер СИБ, предусмотренных планами реализаций требований по обеспечению ИБ.

Для построения элементов СИБ применительно к конкретной области или сфере деятельности Банка должны быть реализованы конкретные защитные меры, применяемые к объектам среды.

В Банке должны быть документально определены роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер, и назначены ответственные за выполнение указанных ролей.

11.3. 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 организации 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 Банка, 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 назначены ответственные за выполнение указанных ролей.

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

В Банке должен быть утвержден перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ. В частности, в указанный перечень документов должны входить:

- отчеты с результатами мониторинга СОИБ и контроля защитных мер;
- отчеты с результатами анализа функционирования СОИБ;
- отчеты с результатами аудита ИБ;
- отчеты с результатами самооценки ИБ;
- документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
- документы, содержащие информацию о новых, выявленных уязвимостях и угрозах ИБ;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве 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 определен и утвержден руководством план выполнения 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 должны быть документально определены роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством, и назначены ответственные за выполнение указанных ролей.

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

К тактическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ Банка и не требующие пересмотра политики ИБ и частных политик ИБ Банка. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа "планирование" СМИБ.

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

- аудитов ИБ;
- самооценок 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 Банка;
- анализа успешных практик в области ИБ (собственных или других организаций).

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

Вся деятельность по реализации тактических улучшений должна документально регистрироваться. Должны быть определены документы, содержащие планы реализации тактических улучшений СОИБ, и документы, в которых фиксируются результаты выполнения указанных планов.

Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться директором Департамента безопасности Банка (или лицом замещающим его).

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 быть документально зафиксированы результаты выполнения указанных процедур.

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

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

К стратегическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром политики ИБ и частных политик ИБ Банка, с последующим выполнением соответствующих тактических улучшений СОИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа "планирование" СМИБ.

Для принятия решений, связанных со стратегическими улучшениями СОИБ в Банке, необходимо рассмотреть среди прочего документально оформленные результаты:
- аудитов ИБ;
- самооценок 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 Банка;
- анализа успешных практик в области ИБ (собственных или других организаций);

а также изменения:
- в законодательстве РФ;

- в нормативных актах Банка России, в частности, в требованиях СТО БР ИББС-1.0;
- интересов, целей и задач бизнеса Банка;
- контрактных обязательств Банка.

Решения по стратегическим улучшениям СОИБ должны быть документально зафиксированы и содержать либо 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, определенных в рамках политики ИБ или частных политик ИБ Банка;
- 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.

Вся деятельность по реализации стратегических улучшений должна документально регистрироваться. Должны быть определены документы, содержащие планы реализации стратегических улучшений СОИБ и документы, в которых фиксируются результаты выполнения указанных планов.

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 за их реализацию.

12. Силы и средства для обеспечения информационной безопасности

В необходимых случаях, могут привлекаться сотрудники структурных подразделений, обладающие знаниями определенного уровня и непосредственно работающие с техническими, программными средствами, или данными (ресурсами), к части деятельности по обеспечению их информационной безопасности. Деятельность этих сотрудников должна контролироваться сотрудниками Департамента безопасности Банка.

О том, какой вид деятельности будет выполняться сотрудниками Департамента безопасности Банка, а какой будет выполняться другими сотрудниками Банка, под контролем сотрудников Департамента безопасности Банка – принимает решение директор Департамента безопасности (или сотрудник, выполняющий его обязанности).

Директор Департамента безопасности Банка имеет право привлекать для настройки технических и программных средств, а также для проверки правильности настроек технических и программных средств сторонние организации. Для разработки внутренних документов Банка могут привлекаться сторонние организации, обладающие соответствующим опытом в сфере ИБ. При этом с вышеуказанными организациями должно быть заключено соглашение о конфиденциальности.

13. 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.

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

Департамент безопасности Банка проводит самооценку по СТО БР ИББС-1.2 («Обеспечение ИБ организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0») не реже чем 1 раз в три года.

В случае обнаружения нарушений или наличия негативных происшествий, ответственный сотрудник Департамента безопасности Банка в день обнаружения предоставляет отчет в подразделение Банка осуществляющее управление рисками в соответствии с «Положением об организации управления рисками «ИНТЕРПРОГРЕССБАНК»(Акционерное общество)».

В случае выявления текущих угроз ИБ сотрудник Департамента безопасности Банка, сотрудник Службы внутреннего контроля Банка, а также при необходимости Председатель Правления Банка, могут вырабатывать экстренные меры по обеспечению устранения угроз ИБ.

14. Порядок утверждения, внесения изменений и дополнений

Данная Политика является документом общего доступа и предназначена для ознакомления каждым сотрудником Банка, партнерами Банка и заинтересованными третьими лицами.

Настоящая Политика подлежит пересмотру при изменении целей и задач Банка в области обеспечения ИБ, функций подразделений, выполняющих задачи управления информационной безопасностью, или при изменении требований законодательства, нормативных актов Банка России в сфере информационной безопасности в кредитных организациях на территории Российской Федерации.

Ответственным за разработку и обновление Политики назначается начальник Управления ИБ (или сотрудник, выполняющий его обязанности).

Для дополнения данной Политики могут использоваться частные политики ИБ, положения и другие внутренние документы Банка.

15. Контроль реализации Политики

Контроль за организацией мероприятий по обеспечению ИБ и за исполнением требований ИБ осуществляет Департамент безопасности Банка. В соответствии с подчиненностью начальник Управления ИБ регулярно доводит до сведения директора Департамента безопасности Банка состояние дел по ИБ в Банке.

В случае необходимости по согласованию с Руководителем соответствующего подразделения назначаются лица ответственные за информационную безопасность на конкретном участке, которые осуществляют наблюдение за выполнением требований безопасности и докладывают о нарушениях, происшедших на порученном им участке.

16. Последствия нарушений требований Политики информационной безопасности

Последствиями нарушений требований Политики являются: утрата, блокирование, искажение или разглашение информации. Величина ущерба может оцениваться только после наступления последствий в каждом конкретном случае. Вид и величина наказания, применяемого к виновному в причинении ущерба лицу, должны быть пропорциональны величине нанесенного ущерба.

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

Клиенты и контрагенты Банка несут ответственность в соответствии с заключенными договорами (например: денежный штраф, равный размеру ущерба, причиненного ценности Банка; отказ в предоставлении продукта или услуги; отказ в приобретении продукта или пользовании услугой)