«УТВЕРЖДЕНО»
Протоколом Правления
АО «Банк «Вологжанин»
от «11» мая 2023 года

Председатель Правления

_____ И.А. Моринова

ПОЛИТИКА
информационной безопасности
АО «Банк «Вологжанин»

г. Вологда
2023 г.

Содержание

1. Общие положения

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

1.2. Настоящая Политика является документом первого уровня АО «Банк «Вологжанин» (далее – Банк), доступным любому сотруднику Банка и пользователю его ресурсов, и представляет собой официально принятую руководством Банка систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.

1.3. Руководство Банка осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования банковской деятельности, а также развития реализуемых банковских технологий и ожиданий клиентов Банка и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать дополнительные конкурентные преимущества для Банка, обеспечить его финансовую стабильность и рентабельность, соответствие требованиям регуляторов.

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

1.5. Стратегия Банка в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

- российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, банковской тайны и других правовых актов;
- нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;
- национальных стандартов РФ, нормативных актов, положений и стандартов Банка России по обеспечению информационной безопасности.

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

1.7. Настоящая Политика распространяется на бизнес - процессы Банка и обязательна для применения всеми сотрудниками и руководством Банка, а также пользователями его информационной инфраструктуры.

1.8. Положения настоящей Политики должны быть учтены при разработке частных политик, других внутренних нормативных документов применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка, которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы Банка, разрабатываются, согласовываются и утверждаются в соответствии с установленным в Банке порядком.

2. Список терминов и определений

В настоящей Политике использованы термины с соответствующими определениями:

2.1. **Информационная инфраструктура**[1] **(ИИ)**: Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

2.2. **Процесс**: Совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы.

2.3. **Технология**: Совокупность взаимосвязанных методов, способов, приемов предметной деятельности.

2.4. **Технологический процесс (ТП):** Процесс, реализующий некоторую технологию.

2.5. **Авторизация**: Предоставление прав доступа.

2.6. **Идентификация**: Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2.7. **Аутентификация**: Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

2.8. **Регистрация:** Фиксация данных о совершенных действиях (событиях).

2.9. **Роль**: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом[2]**.**

2.10. **Угроза**: Опасность, предполагающая возможность потерь (ущерба).

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

2.12. **Актив**[3]: Все, что имеет ценность для Банка и находится в его распоряжении.

2.13. **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.

2.14. **Классификация информационных активов**: Разделение существующих информационных активов Банка по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

2.15. **Объект среды информационного актива**: Материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

2.16. **Ресурс**: Актив Банка, который используется или потребляется в процессе выполнения некоторой деятельности.

2.17. **Банковский технологический процесс**: Технологический процесс[4], реализующий операции по изменению и (или) определению состояния активов[5] Банка, используемых при функционировании или необходимых для реализации банковских услуг.

2.18. **Банковский платежный технологический процесс**: Часть банковского технологического процесса, реализующая действия с информацией, связанные с осуществлением переводов денежных средств, платежного клиринга и расчета, и действия с архивами указанной информации.

---

[1] Информационная инфраструктура:
- включает совокупность информационных центров, банков данных и знаний, систем связи;
- обеспечивает доступ потребителей к информационным ресурсам.

[2] К **субъектам** относятся лица из числа руководителей организации банковской системы Российской Федерации, 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.

[3] 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.

[4] В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.

[5] Операции над активами Банка могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

2.19. **Банковский информационный технологический процесс**: Часть банковского технологического процесса, реализующая действия с информацией, необходимые для выполнения Банком своих функций, и не являющаяся банковским платежным технологическим процессом.
2.20. **Платежная информация**: Информация, на основании которой совершаются операции, связанные с осуществлением переводов денежных средств.
2.21. **Неплатежная информация**: Информация, необходимая для функционирования Банка, не являющаяся платежной информацией, которая может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.
2.22. **Автоматизированная банковская система**: Автоматизированная система, реализующая банковский технологический процесс.
2.23. **Комплекс средств автоматизации автоматизированной банковской системы**: Совокупность всех компонентов автоматизированной банковской системы Банка за исключением людей.
2.24. **Контур безопасности**: Совокупность объектов информатизации, определяемая областью применения, используемых для реализации бизнес-процессов и (или) технологических процессов Банка единой степени критичности (важности), для которой применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации).
2.25. **Безопасность**: Состояние защищенности интересов (целей) Банка в условиях угроз.
2.26. **Информационная безопасность[6] (ИБ)**: Безопасность, связанная с угрозами в информационной сфере[7].
2.27. **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.
2.28. **Целостность информационных активов**: Свойство ИБ Банка сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.
2.29. **Конфиденциальность информационных активов**: Свойство ИБ Банка, состоящее в том, что обработка, хранение и передача информационных активов осуществляется таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.
2.30. **Система информационной безопасности (СИБ)**: Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.
2.31. **Система менеджмента информационной безопасности (СМИБ)**: Часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.
2.32. **Система обеспечения информационной безопасности (СОИБ)**: Совокупность СИБ и СМИБ Банка.
2.33. Область действия системы обеспечения информационной безопасности (область действия СОИБ): Совокупность информационных активов и элементов информационной инфраструктуры Банка.
2.34. **Защитная мера:** сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ Банка.
2.35. Угроза информационной безопасности (угроза ИБ): Угроза нарушения свойств ИБ - доступности, целостности или конфиденциальности информационных активов Банка.
2.36. **Уязвимость информационной безопасности (уязвимость ИБ):** Слабое место в инфраструктуре Банка, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.
2.37. **Ущерб:** Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре Банка, наступивший в результате реализации угроз ИБ через уязвимости ИБ.
2.38. **Инцидент информационной безопасности (инцидент ИБ):** Событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:
- нарушение или возможное нарушение работы средств защиты информации в составе СОИБ Банка;

---

[6] Защищенность достигается обеспечением совокупности свойств ИБ - **доступности, целостности, конфиденциальности информационных** активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) Банка.

[7] 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.

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

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

2.40. **Модель нарушителя информационной безопасности (модель нарушителя ИБ):** Описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

2.41. **Модель угроз информационной безопасности (модель угроз ИБ):** Описание актуальных для Банка источников угроз ИБ, методов реализации угроз ИБ, объектов, пригодных для реализации угроз ИБ, уязвимостей, используемых источниками угроз ИБ, типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов), масштабов потенциального ущерба.

2.42. **Риск нарушения информационной безопасности (риск нарушения ИБ):** Риск, связанный с угрозой ИБ.

2.43. **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.

2.44. **Обработка риска нарушения информационной безопасности:** Процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

2.45. **Остаточный риск нарушения информационной безопасности:** Риск, остающийся после обработки риска нарушения ИБ.

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

2.47. **Операционный риск:** Риск возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов Банка, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий.

2.48. Ключевые индикаторы риска: Количественные контрольные показатели риска информационной безопасности, направленные на измерение и контроль уровня операционного риска в определенный момент времени.

2.49. **Документация:** Совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

2.50. **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.

2.51. **Свидетельства выполнения деятельности по обеспечению информационной безопасности:** Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ Банка.

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

2.53. **Частная политика информационной безопасности (частная политика ИБ):** Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности БС РФ.

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

2.55. **Дистанционная (удаленная) работа:** Выполнение работником трудовой деятельности вне места нахождения стационарного рабочего места прямо или косвенно находящихся под контролем Банка при условии использования внешних информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей связи общего пользования.

2.56. **Уровень защиты информации**: Определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов Банка.

2.57. **Оценка соответствия защиты информации:** Процесс оценки выбора и реализации финансовой организацией организационных и технических мер защиты информации в соответствии с требованиями ГОСТ Р 57580.1, выполняемой проверяющей организацией[8].

2.58. Критерии оценки информационной безопасности (критерии оценки ИБ): Совокупность требований к обеспечению организационных и технических мер защиты информации в соответствии с установленными требованиями.

2.59. **Свидетельства оценки соответствия информационной безопасности установленным критериям:** Записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия защиты информации и могут быть проверены.

2.60. **Заключение по результатам оценки соответствия ЗИ:** Качественная или количественная оценка соответствия установленным критериям, представленная проверяющей группой.

2.61. **Область оценки соответствия ЗИ[9]:** Совокупность объектов информатизации, включая АС и приложения, используемые финансовыми организациями для выполнения бизнес-процессов и/или технологических процессов, связанных с предоставлением финансовых и банковских услуг, а также услуг по осуществлению переводов денежных средств.

2.62. Программа оценки соответствия ЗИ[10]: План деятельности по проведению одной или нескольких проверок соответствия ЗИ (и других проверок ИБ), запланированных на конкретный период времени и направленных на достижение конкретной цели.

2.63. Понятие банковская тайна применяется в соответствии со ст. 26, Федерального закона от 02.12.1990 № 395-1 "О банках и банковской деятельности".

2.64. **Коммерческая тайна -** режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

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

2.66. Термин защищаемая информация при переводе денежных средств используется в терминологии, приведенной в гл. 1 Положения Банка России от 04.06.2020 № 719-П [12].

Обозначения и сокращения

АБС	автоматизированная банковская система;
БС	банковская система;
ЖЦ	жизненный цикл;
ИБ	информационная безопасность;
ИСПДн	информационная система персональных данных;
НСД	несанкционированный доступ;
НРД	нерегламентированные действия в рамках предоставленных полномочий;
СКЗИ	средство криптографической защиты информации;
СМИБ	система менеджмента информационной безопасности;

[8] Сторонняя организация, имеющих лицензию на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации N 79 (далее - проверяющая организация).

[9] Область оценки соответствия ЗИ должна совпадать с областью применения ГОСТ Р 57580.1 и обычно включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются проверке, а также охватываемый период времени.

[10] Программа проверки включает всю деятельность, необходимую для планирования, проведения, контроля, анализа и совершенствования ЗИ.

СИБ	система информационной безопасности;
СОИБ	система обеспечения информационной безопасности;
ЭВМ	электронная вычислительная машина;
Банк	АО «Банк «Вологжанин»

3. Описание объекта защиты

Основными объектами защиты системы ИБ в Банке являются:

- информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
- информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
- сотрудники Банка, являющиеся разработчиками и пользователями информационных систем Банка;
- 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 такие системы.

4. Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению ИБ Банка является снижение угроз ИБ до приемлемого для Банка уровня.

Основные задачи деятельности по обеспечению ИБ Банка:

- выявление потенциальных угроз ИБ и уязвимостей[11] объектов защиты;
- предотвращение инцидентов ИБ;
- исключение либо минимизация выявленных угроз.

5. Угрозы информационной безопасности

Все множество потенциальных угроз ИБ делится на три класса по характеру их возникновения: природные, техногенные и антропогенные[12].

К **антропогенным угрозам** относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Банка и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К **техногенным угрозам** могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

---

[11] В настоящем документе под уязвимостью понимается слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами (ГОСТ Р ИСО/МЭК 13335-1-2006, статья 2.26).

[12] Данная классификация осуществляется независимо от классификации операционных рисков по риск-факторам, предусмотренной в Банке.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К **природным (естественным) угрозам** относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Возникновение природных (естественных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

Источники угроз по отношению к инфраструктуре Банка могут быть как внешними, так и внутренними.

В основе исходной концептуальной схемы ИБ Банка лежит противоборство собственника[13] и злоумышленника[14] с целью получения контроля над информационными активами. Однако другие, незлоумышленные действия или источники угроз также лежат в сфере рассмотрения настоящей Политики.

6. Модели угроз и нарушителей информационной безопасности

Модели угроз и нарушителей являются основным инструментом Банка при развертывании, поддержании и совершенствовании СОИБ. Степень детализации параметров моделей угроз и нарушителей ИБ может быть различной и определяется реальными потребностями. Модели угроз и нарушителей ИБ должны регулярного анализироваться и при необходимости пересматриваться.

Деятельность Банка поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

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

Главной целью злоумышленника является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например, путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через иные уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективно по соотношению «затраты/получаемый результат».

Другой целью злоумышленника может являться нарушение функционирования бизнес-процессов Банка, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;

---

[13] Под собственником здесь понимается субъект хозяйственной деятельности (Банк), имеющий права владения, распоряжения или пользования активами, который заинтересован или обязан (согласно требованиям законов или иных законодательных, или нормативно-правовых актов) обеспечивать защиту активов от угроз, которые могут снизить их ценность или нанести ущерб собственнику.

[14] Под злоумышленником здесь понимается лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий (адаптировано из ст. 27 УК РФ).Если злоумышленнику удается установить такой контроль, то как самому Банку, так и клиентам, которые доверили ему свои собственные активы, наносится ущерб.

- работники Банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники Банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками Банка, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

- внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;
- внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
- сбои, отказы, разрушения/повреждения программных и технических средств.

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

- внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;
- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре[15].

Наиболее актуальные источники угроз на уровне бизнес-процессов:

- внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;
- комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

Наибольшими возможностями для нанесения ущерба Банку обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри Банка.

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности информационного актива или параметры системы, которая этот актив поддерживает.

По отношению к Банку нарушители могут быть разделены на внешних и внутренних.

Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Банком рассматриваются:

- зарегистрированные пользователи информационных систем Банка;
- сотрудники Банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Банка, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства информационной системы Банка;
- сотрудники самостоятельных структурных подразделений Банка, задействованные в разработке и сопровождении программного обеспечения;
- сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность;
- руководители различных уровней.

[15] На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно без соучастия внутренних, практически невозможна.

Внешние нарушители.

В качестве потенциальных внешних нарушителей Банком рассматриваются:

- бывшие сотрудники Банка;
- представители организаций, взаимодействующих по вопросам технического обеспечения Банка;
- клиенты Банка;
- посетители зданий и помещений Банка;
- конкурирующие с Банком кредитные организации;
- 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).

В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников Банка;
- несанкционированные действия нарушителя 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, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7. Основные положения по обеспечению информационной безопасности

7.1. Требования об обеспечении ИБ Банка обязательны к соблюдению всеми работниками Банка и пользователями информационных систем.

7.2. Руководство Банка приветствует и поощряет в установленном порядке деятельность работников Банка и пользователей информационных систем по обеспечению ИБ.

7.3. Неисполнение или некачественное исполнение сотрудниками Банка и пользователей информационных систем обязанностей по обеспечению ИБ может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Банке порядком либо требованиями действующего законодательства.

7.4. Стратегия Банка в части противодействия угрозам ИБ заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Банка, до специализированных мер ИБ по каждому выявленному в Банке риску, основанных на оценке рисков ИБ.

7.5. Система ИБ Банка основывается на базовом составе мер защиты информации для следующих процессов (направлений) защиты информации в соответствии с разделами 7, 9 Национального стандарта РФ ГОСТ Р 57580.1:

процесс 1 "Обеспечение защиты информации при управлении доступом":

- управление учетными записями и правами субъектов логического доступа;
- идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
- защита информации при осуществлении физического доступа;
- идентификация, классификация и учет ресурсов и объектов доступа;

процесс 2 "Обеспечение защиты вычислительных сетей":

- сегментация и межсетевое экранирование вычислительных сетей;
- выявление сетевых вторжений и атак;
- защита информации, передаваемой по вычислительным сетям;
- защита беспроводных сетей;

процесс 3 "Контроль целостности и защищенности информационной инфраструктуры";

процесс 4 "Защита от вредоносного кода";

процесс 5 "Предотвращение утечек информации";

процесс 6 "Управление инцидентами защиты информации":

- мониторинг и анализ событий защиты информации;
- обнаружение инцидентов защиты информации и реагирование на них;

процесс 7 "Защита среды виртуализации";

процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств".

Базовый набор требований может быть расширен Банком путем выполнения деятельности в рамках процессов СМИБ.

7.6. С целью поддержки заданного уровня защищенности Банк придерживается процессного подхода в построении СМИБ.

СМИБ Банка основывается на осуществлении основных подходов, в том числе для каждого процесса п.7.5 настоящей Политики и раздела 9 Национального стандарта РФ ГОСТ Р 57580.1, (планирование, реализация и эксплуатация защитных мер, контроль (мониторинг и анализ), совершенствование (поддержка и улучшение)) соответствующих требованиям раздела 8 Национального стандарта РФ ГОСТ Р 57580.1, стандарта Банка России СТО БР ИББС–1.0.

Реализация этих мероприятий осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению ИБ Банка и повышение ее эффективности.

На всех этапах жизненного цикла управление ИБ Банка осуществляется с соблюдением нормативных документов, определяющих процессы управления операционными рисками[16] Банка.

7.7. При планировании мероприятий по обеспечению ИБ в Банке осуществляются:

7.7.1. Определение и распределение ролей персонала Банка, связанного с обеспечением ИБ (ролей ИБ).

7.7.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения ИБ.

7.7.3. Менеджмент рисков ИБ, включающий:

- анализ влияния на ИБ Банка применяемых в деятельности Банка технологий, а также внешних по отношению к Банку событий;
- выявление проблем обеспечения ИБ, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз ИБ;
- выявление, анализ и оценка значимых для Банка угроз ИБ;
- выявление возможных негативных последствий для Банка, наступающих в результате проявления факторов риска ИБ, в том числе связанных с нарушением свойств безопасности информационных активов Банка;
- идентификацию и анализ рисковых событий ИБ;
- оценку величины рисков ИБ и определение среди них рисков, неприемлемых для Банка;
- обработку результатов оценки рисков ИБ, базирующейся на методах управления операционными рисками, определенных в Банке;
- оптимизацию рисков ИБ за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Банка в случае наступления рисковых событий;
- оценку влияния защитных мер на цели основной деятельности Банка;
- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению ИБ;
- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Банка и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
- документальное оформление целей и задач обеспечения ИБ Банка, поддержание в актуальном состоянии нормативно – методического обеспечения деятельности в сфере ИБ.

---

[16] Требования к управлению операционными рисками, в том числе рискам ИБ, определены Положением БР № 716-П [13]. Рекомендации по оценке рисков информационной безопасности приведены в РС БР ИББС-2.2-2009 [16] и РС БР ИББС-2.7-2015[17]. Требования к операционной надежности в целях обеспечения непрерывности оказания банковских услуг определены Положением БР № 787-П [14].

7.8. В рамках реализации деятельности по обеспечению ИБ в Банке осуществляются:

7.8.1. Менеджмент инцидентов ИБ, включающий:

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

7.8.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
- применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
- применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.9. В целях проверки деятельности по обеспечению ИБ в Банке осуществляются:

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигурации систем и подсистем Банка;
- мониторинг факторов рисков и соответствующий их пересмотр;
- контроль реализации и исполнения требований сотрудниками Банка действующих внутренних нормативных документов по обеспечению ИБ Банка;
- контроль деятельности сотрудников и других пользователей информационных систем Банка, направленный на выявление и предотвращение конфликтов интересов.

7.10. В целях совершенствования деятельности по обеспечению ИБ в Банке осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения ИБ (при изменениях целей и задач основной деятельности Банка).

8. Организационная основа деятельности по обеспечению защиты информации

8.1. В целях выполнения задач по обеспечению ИБ Банка, в соответствии с действующим законодательством РФ и требований регуляторов по защите информации в Банке должны быть определены следующие роли:

- Куратор[17];
- Ответственное подразделение[18];
- Сотрудник банка.

При необходимости могут быть определены и другие роли по ИБ.

8.2. Основными функциями Куратора в вопросах ИБ являются:

- организация обеспечения ЗИ и управление структурой ИБ Банка, в том числе по обнаружению, предупреждению и ликвидаций последствий компьютерных атак и реагирования на компьютерные инциденты,
- координация и внедрение ИБ в Банке.

8.3. Оперативная деятельность и планирование деятельности по обеспечению ИБ Банка осуществляются и координируются Ответственным подразделением.

Задачами Ответственного подразделения являются:

- установление потребностей Банка в применении мер обеспечения ИБ, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
- соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов Банка России и стандартов Банка России по обеспечению ИБ, нормативных актов по обеспечению ИБ, приватности и неразглашению, принятых регуляторами рынков, на которых представлены интересы и бизнес Банка;
- разработка и пересмотр внутренних нормативных документов по обеспечению ИБ Банка, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы ИБ Банка;
- контролировать работников Банка в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- обучение, контроль и непосредственная работа с персоналом Банка в области обеспечения ИБ;
- планирование применения, участие в поставке и эксплуатации средств обеспечения ИБ на объекты и системы в Банке;
- осуществлять мониторинг событий, связанных с обеспечением ИБ;
- прогнозирование и предупреждение инцидентов ИБ;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ Банка;
- участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий;
- осуществлять контроль обеспечения ИБ на стадиях ЖЦ АБС, в том числе при тестировании и вводе в эксплуатацию подсистем ИБ АБС Банка;
- участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ Банка.
- пресечение несанкционированных действий нарушителей ИБ;

---

[17] Заместитель Председателя Правления, ответственный за обеспечение информационной безопасности Банка, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагированию на компьютерные инциденты.

[18] Структурное подразделение, либо специально выделенные сотрудники существующего структурного подразделения Банка, обеспечивающее осуществление функций по обеспечению информационной безопасности, в том числе обнаружение, предупреждение и ликвидация последствий компьютерных атак, и реагирование на компьютерные инциденты.

- типизация решений по применению мер и средств обеспечения ИБ и распространение типовых решений на филиалы и представительства Банка;

8.4. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов ИБ, возглавляемые сотрудником Ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других самостоятельных структурных подразделений Банка на основе совмещения работы в группе со своими основными должностными обязанностями.

8.5. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Банка, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.

8.6. Основными задачами работников Банка при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по ИБ безопасности Банка являются:

- соблюдение требований ИБ, устанавливаемых нормативными документами Банка;
- выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;
- выявление и реагирование на инциденты ИБ;
- информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях ИБ;
- прогнозирование и предупреждение инцидентов ИБ в пределах своей компетенции;
- мониторинг и оценка ИБ в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
- информирование своего руководства и Ответственного подразделения о выявленной угрозе в информационной среде Банка.

9. Защита персональных данных

9.1. Состав и содержание организационных и технических мер, связанных с защитой персональных данных должны соответствовать требованиям [5] и [15].

9.2. Для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных применяются правовые, организационные и технические меры.

9.3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных реализуется в соответствии с рекомендациями [18].

9.4. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности реализуется в соответствии с рекомендациями [19].

9.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений Банка обеспечивают безопасность персональных данных при обработке и хранении в ИСПДн, а также обеспечивают безопасность хранения материальных носителей персональных данных и несут персональную ответственность за невыполнение требований по безопасности персональных данных.

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

10. Ответственность за соблюдение положений Политики

Общее руководство обеспечением ИБ Банка осуществляет Куратор.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СМИБ Банка лежит на руководстве Ответственного подразделения.

Ответственность работников Банка за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками Банка, а также положениями внутренних нормативных документов Банка.

11. Контроль за соблюдением положений Политики

Общий контроль состояния ИБ Банка осуществляется Куратором.

Текущий контроль соблюдения настоящей Политики осуществляет Ответственное подразделение. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Банка, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Внешний аудит ИБ проводится не реже одного раза в два года с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации путем оценки соответствия защиты информации требованиям ГОСТ Р 57580.2-2018, положениям Банка России 683-П [11], 719-П [12], 802-П [10].

Банк обеспечивает ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, лицензированной сторонней организацией.

Отчеты, подготовленные проверяющей организацией по результатам оценки соответствия защиты информации, хранится не менее пяти лет начиная с даты его выдачи проверяющей организацией.

При проведении самооценки ИБ рекомендуется руководствоваться требованиями стандартов Банка России СТО БР ИББС-1.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности", 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", 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".

12. Заключительные положения

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

12.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Банка настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Банка. В этом случае Ответственное подразделение инициирует внесение соответствующих изменений.

12.3. Пересмотр и при необходимости внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе.

Периодически пересмотр не реже одного раза в 24 месяца, при условии внесения существенных изменений или уточнений.

Внепланово изменения могут вноситься по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внешнего и внутренних аудитов ИБ и других контрольных мероприятий.

12.4. Ответственным за внесение изменений в настоящую Политику является руководитель Ответственного подразделения.

Нормативные документы

1. Федеральный закон от 2 декабря 1990 года № 395-1 "О банках и банковской деятельности".
2. Федеральный закон от 29.07.2004 года № 98-ФЗ «О коммерческой тайне».
3. Федеральный закон от 27 декабря 2002 года № 184-ФЗ "О техническом регулировании".
4. Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
5. Национальный стандарт РФ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст).
6. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2014.
7. Стандарт Банка России СТО БР ИББС-1.4-2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге».
8. Указ Президента Российской Федерации «О Дополнительных мерах по обеспечению информационной безопасности Российской Федерации» №250 от 01.05.2022г.
9. Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
10. Положение Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России».
11. Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
12. Положение Банка России от 4 июня 2020 года № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
13. Положение Банка России от 08.04.2020 № 716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе".
14. Положение Банка России от 12.01.2022 № 787-П "Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг".
15. Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных".
16. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».
17. Рекомендации в области стандартизации Банка России РС БР ИББС-2.7-2015 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности».
18. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
19. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».