КОММЕРЧЕСКИЙ БАНК «РЕСПУБЛИКАНСКИЙ КРЕДИТНЫЙ АЛЬЯНС»

(общество с ограниченной ответственностью)

УТВЕРЖДЕНО

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

Протокол № 22-12/2021 от «22 » декабря 2021 г.

Председатель Правления

_____ И.В. Карлинский

«22 » декабря 2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Коммерческого Банка «Республиканский Кредитный Альянс»

(общество с ограниченной ответственностью)

Новая редакция 2

Москва 2021 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная банковская система: Автоматизированная система, реализующая банковский технологический процесс Коммерческого Банка «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью) (далее - Банк).

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

Авторизация: Предоставление прав доступа.

Актив: Все, что имеет ценность для Банка и находится в распоряжении Банка.

Архитектура объектов информатизации: Совокупность основных структурно функциональных характеристик и свойств объектов информационной инфраструктуры, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Аудит информационной безопасности: Независимая оценка соответствия информационной безопасности, выполняемая работниками организации, являющейся внешней по отношению к Банку, допускающая возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности.

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

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.

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.

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

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

Выводы аудита информационной безопасности: Результат оценки собранных свидетельств аудита информационной безопасности.

Документ: Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Документация: Совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

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

Доступность информационных активов: Свойство информационной безопасности 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.

Защитная мера: Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения информационной безопасности Банка.

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

Информационная безопасность: Безопасность, связанная с угрозами в информационной сфере.

Информационная инфраструктура: Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

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: Событие или комбинация событий, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы безопасности информации, результатом которой являются:

- нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности Банка;
- нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Банка в области обеспечения информационной безопасности, нарушение или возможное нарушение в выполнении процессов системы обеспечения информационной безопасности Банка;
- нарушение или возможное нарушение в выполнении банковских технологических процессов Банка;
- нанесение или возможное нанесение ущерба Банку и (или) его клиентам.

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

Конфиденциальность информационных активов: Свойство информационной безопасности 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.

Информационная система: Система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Менеджмент: Скоординированная деятельность по руководству и управлению.

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

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

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

Нарушитель информационной безопасности: Субъект, реализующий угрозы безопасности информации Банка, нарушая предоставленные ему полномочия по доступу к активам Банка или по распоряжению ими.

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

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

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

Оценка соответствия информационной безопасности: Систематический и документируемый процесс получения свидетельств деятельности Банка по реализации требований информационной безопасности и установлению степени выполнения в Банке критериев оценки (аудита) информационной безопасности.

Политика информационной безопасности: Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению информационной безопасности, предназначенная для Банка в целом.

Поставщик услуг: Лицо, предоставляющее Банку на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

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

Регистрация: Фиксация данных о совершенных действиях (событиях).

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

Риск нарушения информационной безопасности: Риск, связанный с угрозой безопасности информации.

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

Роль: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Система информационной безопасности: Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента информационной безопасности: Часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности.

Система обеспечения информационной безопасности информационной безопасности**:** Совокупность системы информационной безопасности и системы менеджмента информационной безопасности Банка.

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).

Технологический процесс: Процесс, реализующий некоторую технологию.

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

Угроза информационной безопасности: Угроза нарушения свойств информационной безопасности – доступности, целостности или конфиденциальности информационных активов Банка.

Угроза: Опасность, предполагающая возможность потерь (ущерба).

Ущерб: Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Банка или другой вред активам и (или) инфраструктуре Банка, наступивший в результате реализации угроз безопасности информации через уязвимости информационной безопасности.

Уязвимость информационной безопасности: Слабое место в инфраструктуре Банка, включая систему обеспечения информационной безопасности, которое может быть использовано для реализации или способствовать реализации угрозы безопасности информации.

Целостность: Свойство информационной безопасности Банка сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБС	Автоматизированная банковская система
ООО	Общество с ограниченной ответственностью
АРМ	Автоматизированное рабочее место
БИТП	Банковский информационный технологический процесс
БПТП	Банковский платежных технологический процесс
БТ	Банковская тайна
БТП	Банковских технологический процесс
ИБ	Информационная безопасность
ИС	Информационная система
КБ	Коммерческий Банк
КТ	Коммерческая тайна
ЛВС	Локальная вычислительная сеть
НРД	Нерегламентированные действия в рамках предоставленных полномочий
НСД	Несанкционированный доступ
ОИ	Открытая информация
ОС	Операционная система
ПДн	Персональные данные
СВР	Степень возможной реализации
СКЗИ	Средство криптографической защиты информации
СМИБ	Система менеджмента информационной безопасности
СИБ	Система информационной безопасности
СОИБ	Система обеспечения информационной безопасности
СТП	Степень тяжести последствий
СУБД	Система управления базами данных
ЭВМ	Электронная вычислительная машина

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (далее - Политика ИБ) Коммерческого Банка «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью) (далее – «Банк») определяет высокоуровневые цели и задачи обеспечения информационной безопасности в Банке, включая содержание, назначение и требования к деятельности по обеспечению информационной безопасности, а также способы контроля реализации требований настоящей Политики.

1.2. Нормативной основой настоящей Политики являются законодательство Российской Федерации и нормы права в части обеспечения информационной безопасности, требования нормативных актов Центрального Банка Российской Федерации, Федерального органа исполнительной власти, уполномоченного в области безопасности, Федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается, в том числе:

− Федеральный закон от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

− Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных»;

− Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе»;

− Федеральный закон от 02.12.1990 г. № 395-1 «О банках и банковской деятельности»;

− Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»;

− Положение Банка России от 04.06.2020 г. № 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»;

− Положение Банка России от 23.12.2020 г. № 747-П «О требованиях к защите информации в платежной системе»;

− Положение Банка России от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств»;

− Положение Банка России от 08.04.2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»;

− Указание Банка России от 09.06.2012 г. №2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств»;

− Стандарты Банка России (СТО БР ИББС);

− Рекомендации в области стандартизации Банка России (РС БР ИББС);

− Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасности финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

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

1.4. Настоящая Политика утверждается Правлением Банка.

1.6. Настоящая 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.

1.7. Основные положения и требования настоящей Политики распространяются на процессы Банка, в которых осуществляется обработка информации, содержащей сведения, составляющие банковскую и коммерческую тайну, персональные данные, иную информацию конфиденциального характера, информацию необходимую для обеспечения деятельности Банка, а также на структурные подразделения Банка, принимающие участие в вышеуказанных процессах. Основные вопросы Политики также распространяются на другие организации и учреждения, взаимодействующие с Банком в качестве поставщиков и потребителей информационных активов Банка в том или ином качестве.

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

1.9. Настоящая Политика является методологической основой для:

− формирования и проведения единой политики в области обеспечения безопасности информации в Банке;

− принятия управленческих решений и разработке практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

− координации деятельности структурных подразделений Банка при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;

− разработки частных политик, положений, регламентов, инструкций и других внутренних документов Банка, касающихся вопросов обеспечения информационной безопасности;

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

1.10. Документами, детализирующими положения настоящей Политики применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности Банка, являются частные политики по обеспечению информационной безопасности, которые являются документами по информационной безопасности второго уровня, оформляются как отдельные внутренние нормативные документы Банка, разрабатываются, согласовываются и утверждаются в соответствии с установленными в Банке порядке.

1.11. Документы, содержащие положения информационной безопасности, применяемые к процедурам обеспечения информационной безопасности (документы третьего уровня), содержат правила и параметры, устанавливающие способ осуществления и выполнения конкретных действий, связанных с информационной безопасностью, в рамках технологических

процессов, используемых в Банке, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер, в используемых технологических процессах.

1.12. Документы, содержащие свидетельства выполненной деятельности по обеспечению информационной безопасности (документы четвертого уровня), отражают достигнутые результаты, относящиеся к обеспечению информационной безопасности.

1.13. В целях совершенствования деятельности по обеспечению информационной безопасности осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Банка).

1.14. Руководство Банка проводит совещания, посвященные проблемам обеспечения информационной безопасности с целью формирования четких указаний, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению информационной безопасности.

2. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Целью обеспечения информационной безопасности является реализация, эксплуатация и совершенствование совокупности защитных мер, защитных средств и процессов, включая ресурсное и административное (организационное) обеспечение (далее — система обеспечения информационной безопасности), а также части менеджмента Банка, предназначенного для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности.

2.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной информационной системы, ее обрабатывающей:

− доступности информации и операций с ней для зарегистрированных пользователей, устойчивого функционирования информационных систем Банка, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;

− обеспечения конфиденциального характера информации, хранимой и обрабатываемой в информационных системах и передаваемой по каналам связи;

− целостности и аутентичности информации, хранимой и обрабатываемой в информационных системах и передаваемой по каналам связи;

− предотвращение и (или) снижение ущерба от инцидентов информационной безопасности.

2.3. Основными задачами обеспечения информационной безопасности являются:

− постоянный анализ и изучение информационной инфраструктуры Банка с целью выявления и устранения уязвимостей информационной безопасности;

− обеспечение требуемого уровня защиты информации в условиях штатного функционирования защитных мер и процессов их эксплуатации, а также в условиях реализации угроз, учтенных в частных моделях угроз Банка и приводящих к возникновению:

- локальных инцидентов информационной безопасности;

- широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношения к информационной безопасности;

− поддержание системы защиты на должном уровне, с помощью мониторинга событий и инцидентов информационной безопасности. Менеджмент событий и инцидентов информационной безопасности, полученных в результате мониторинга, позволяет избежать деградации систем защиты и обеспечить требуемый уровень безопасности объектов информационной инфраструктуры;

− оценка состояния информационной безопасности объектов информационной инфраструктуры и выявление признаков деградации используемых защитных мер, с помощью оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (подробней приведено в разделе12 Политики);

− реализация четырех групп процессов (которые составляют систему менеджмента информационной безопасности), в целях реализации и поддержания должного уровня защиты информации в Банке:

- планирование системы обеспечения информационной безопасности;
- реализация системы обеспечения информационной безопасности;
- мониторинг и анализ системы обеспечения информационной безопасности («проверка»);
- поддержка и улучшение системы обеспечения информационной безопасности («совершенствование»).

− обеспечение непрерывности бизнеса и его восстановления после прерываний;

− обеспечение соответствия требованиям Федерального законодательства и нормативно-методических документов ФСБ России, ФСТЭК России в области защиты информации.

2.4. Основополагающие принципы функционирования системы обеспечения информационной безопасности Банка:

− законность: соблюдение законодательства Российской Федерации;

− приоритетность: предварительное категорирование информационных активов Банка по степени важности, и оценка реальных угроз этим активам;

− комплексный подход: согласование мероприятий, проводимых в области обеспечения информационной безопасности Банка;

− оптимальное сочетание проводимых мероприятий;

− единая политика: координация деятельности подразделений Банка по поддержанию и совершенствованию уровня защиты информации, определению обязанностей и ответственности подразделений (и их руководителей);

− целесообразность (адекватность): затраты на обеспечение информационной безопасности должны быть обоснованы, и не должны превышать потери, которые может понести Банк при реализации угроз;

− конфиденциальность: обеспечение защиты информации от преднамеренного или непреднамеренного разглашения;

− целостность: обеспечение сохранения неизменности свойств информационных активов;

− доступность: обеспечение доступности информационных активов для подразделений;

− достоверность: обеспечение соответствия предусмотренному поведению или результату;

− аутентичность: обеспечение гарантии того, что субъект или ресурс идентичны заявленным;

− контроль: проведение регулярного аудита информационной безопасности, мониторинг;

− своевременность обнаружения проблем, потенциально способных повлиять на бизнес-цели Банка;

− прогнозируемость развития проблем: выявление причинно-следственной связи возможных проблем и построение на этой основе точного прогноза их развития;

− адекватная оценка степени влияния выявленных проблем на бизнес-цели Банка;

− эффективность защитных мер;

− накопление, систематизация и использование опыта при принятии и реализации решений;

− непрерывность принципов безопасного функционирования;

− понимание Руководством Банка на основе принятых ценностей и накопленных знаний, необходимости самостоятельно формировать и учитывать в рамках основной деятельности прогноз результатов от деятельности по обеспечению информационной безопасности, а также поддерживать эту деятельность в соответствии с прогнозом.

2.5. Каждый Руководитель подразделения Банка несет ответственность за поддержание конфиденциальности, целостности и доступности своих информационных активов и должен соблюдать все действующие политики, стандарты и инструкции, касающиеся защиты информационных активов Банка. Все сотрудники Банка обязаны поддерживать и соблюдать все политики, стандарты и инструкции Банка, управляющие защитой информационных активов.

3. ОБЛАСТЬ ПРИМЕНЕНИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Область применения процесса обеспечения информационной безопасности определяется в соответствии с положениями нормативных актов Банка России.

3.2. К основным намерениям обеспечения информационной безопасности, направленным на достижение указанных целей, относятся:

− назначение и распределение функциональных прав и обязанностей ролей, обеспечение доверия к персоналу;

− защита информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;

− управление доступом к объектам информационной инфраструктуры:

- организация и контроль использования учетных записей;
- организация и контроль предоставления, отзыва и блокирование доступа;
- идентификация, аутентификация, авторизация (разграничение доступа) субъектов доступа при осуществлении логического доступа;
- организация управления и защиты идентификационных и аутентификационных данных;

- организация и контроль физического доступа к объектам информационной инфраструктуры;
- организация учета и контроль состава ресурсов и объектов доступа;

− контроль целостности и защищенности информационной инфраструктуры Банка;

− организация защиты от воздействий вредоносного кода (антивирусная защита);

− предотвращение утечек информации;

− организация защиты вычислительных сетей:

- сегментация и межсетевое экранирование вычислительных сетей;
- защита внутренних вычислительных сетей при взаимодействии с сетью Интернет;
- регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей;
- мониторинг и контроль содержимого сетевого трафика (выявление сетевых вторжений и атак);
- защита информации, передаваемой по вычислительным сетям;

− безопасное использование ресурсов электронной почтовой системы;

− криптографическая защита информации;

− защита банковских платежных и информационных технологических процессов, в том числе банковских технологических процессов, в рамках которых обрабатываются персональные данные;

− использование взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации;

− организация и функционирование подразделения (сотрудников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации;

− оценка и обработка рисков нарушения информационной безопасности;

− организация и реализация программ по обучению и повышению осведомленности сотрудников и клиентов Банка в области обеспечения защиты информации;

− управление инцидентами информационной безопасности:

• мониторинг и анализ событий защиты информации;

• обнаружение инцидентов информационной безопасности и реагирование на них;

− организация обеспечения непрерывности бизнеса и его восстановления;

− мониторинг состояния информационной безопасности и контроль защитных мер;

− проведение аудита (оценки соответствия) информационной безопасности и анализ функционирования системы обеспечения информационной безопасности;

− определение, классификация информационных активов, подлежащих защите, определение их ценности и степени тяжести последствий от потери свойств информационной безопасности для рассматриваемых типов информационных активов;

− определение и актуализация списков возможных негативных воздействий на защищаемые активы, способов реализации и степени вероятности реализации этих угроз.

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1. Основными объектами защиты, входящими в область применения процесса обеспечения информационной безопасности в Банке, являются:

− информационные активы, 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 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;

− сотрудники Банка, являющиеся 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 компоненты информационной системы Банка.

4.2. Структура, состав и размещение объектов защиты.

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

4.2.2. К основным особенностям информационной среды Банка относятся:

− территориальная распределенность компонентов информационных систем;

− разнообразие решаемых задач (от подготовки и отправки платежей до ведения дистанционного банковского обслуживания);

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

− объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности.

4.3. Основные типы защищаемых информационных активов.

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

4.3.2. Защите подлежит вся информация и информационные активы 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 г. № 395-1 «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»;

− информация, отнесенная к защищаемой в соответствии с положением Банка России от 04.06.2020 г. № 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»;

− информация в платежной системе Банка России, отнесенная к защищаемой в соответствии с положением Банка России от 23.12.2020 г. № 747-П «О требованиях к защите информации в платежной системе Банка России»;

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

4.3.3. Перечень типов информационных активов формируется на основе результатов выполнения классификации информационных активов. Состав перечня типов информационных активов соответствует нормам законодательства Российской Федерации, в том числе нормативным актам Банка России. В Банке используется следующий перечень типов информационных активов:

− информация ограниченного доступа:

- информация, содержащая сведения, составляющие банковскую тайну;
- платежная информация (информация, предназначенная для проведения расчетных, кассовых и других банковских операций);
- информация, содержащая сведения, составляющие коммерческую тайну;
- персональные данные;
- управляющая информация платежных, информационных и телекоммуникационных систем (информация, используемая для технической настройки программно-аппаратных комплексов обработки, хранения и передачи информации);

− открытая (общедоступная) информация.

4.3.4. В целях защиты информационных активов производится регулярное повышение осведомленности сотрудников в области обеспечения защиты информации. Порядок повышения осведомленности описан во внутренних нормативных документах Банка.

5. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ

5.1. Настоящий раздел Политики является методикой моделирования угроз безопасности информации и разработан с учетом условий и особенностей функционирования информационных систем Банка, обрабатывающих различные информационные активы, с учетом требований законодательства Российской Федерации в области обеспечения информационной безопасности и Базы данных угроз безопасности информации ФСТЭК России.

5.2. Целью моделирования угроз безопасности информации является выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств её обработки), а также к нарушению или прекращению функционирования объектов информационной инфраструктуры.

5.3. В качестве угроз безопасности информации, подлежащих определению при моделировании угроз безопасности информации, рассматриваются неправомерные действия и (или) воздействия на объекты информационной инфраструктуры, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий.

5.4. В результате моделирования угроз безопасности информации формируется перечень актуальных угроз безопасности информации, реализуемых в информационной инфраструктуре Банка.

5.5. Процесс моделирования угроз безопасности информации включает (таблица 1):

− определение возможных негативных последствий от реализации угроз безопасности информации;

− определение условий для реализации угроз безопасности информации;

− определение источников угроз безопасности информации и оценку возможностей нарушителей;

− определение сценариев реализации угроз безопасности информации;

− оценку уровня опасности угроз безопасности информации.

Таблица 1 – Процесс моделирования угроз безопасности информации

ВХОДНЫЕ ДАННЫЕ	ЭТАП	ПОЛУЧАЕМЫЙ РЕЗУЛЬТАТ
Требования законодательства Российской Федерации	**Определение возможных негативных последствий от реализации угроз безопасности информации**	Перечень возможных негативных последствий
Сведения о структурно-функциональных характеристиках информационной инфраструктуры		Информационные активы
Результаты оценки рисков		Виды неправомерного доступа и (или) воздействий
Сведения об информационных активах		Перечень угроз безопасности информации
Сведения о структурно-функциональных характеристиках информационной инфраструктуры	**Определение условий для реализации угроз безопасности информации**	Типы уязвимостей и (или) недекларированных возможностях
Сведения об уязвимостях		Варианты возможного доступа нарушителей информационной безопасности к объектам информационной инфраструктуры
Сведения о доступе к объектам информационной инфраструктуры		
Особенности организации банковских технологических процессов	**Определение источников угроз безопасности информации и оценку**	Виды источников угроз безопасности информации
Сведения о сервисах, предоставляемых сторонними организациями		Возможные цели реализации угроз безопасности информации нарушителями

Сведения о типах внутренних и внешних пользователей.	**возможностей нарушителей**	Категории, виды и возможности нарушителей
Сведения об объектах информационной инфраструктуры и особенностях их функционирования	**Определение сценариев реализации угроз безопасности информации**	Перечень сценариев угроз безопасности информации
Условия реализации угроз безопасности информации		
Категории, виды и возможности нарушителей		
Перечень сценариев реализации угроз безопасности информации	**Оценка уровня опасности угроз безопасности**	Уровни опасности угроз безопасности информации
Сведения о типе доступа к объектам		
информационной инфраструктуры	**информации**	
Сведения о сложности реализации сценария		
Сведения об уровне значимости объектов информационной инфраструктуры		

5.6. При моделировании угроз безопасности информации определяется граница процесса моделирования, в которую включаются объекты информационной инфраструктуры, обрабатывающие, хранящие информацию и (или) обеспечивающие реализацию основных бизнес-процессов, интерфейсы их взаимодействия с пользователями, со смежными (взаимодействующими) объектами информационной инфраструктуры, а также инженерные системы (системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны, системы охраны), средства, каналы и услуги связи, другие услуги и сервисы, предоставляемые сторонними организациями, от которых зависит функционирование объектов информационной инфраструктуры.

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

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

5.9. На каждом из уровней информационной инфраструктуры, приведенных в таблице 2, угрозы (таблица 3) и их источники, методы и средства защиты и подходы к оценке эффективности являются различными.

Таблица 2 – Иерархия уровней информационной инфраструктуры

Уровни информационной инфраструктуры	**Объекты среды**
Физический уровень	Физические носители информации, в составе системы хранения данных
	Физические носители информации, в составе системы резервного копирования
	Физические носители информации, в составе автоматизированных рабочих мест
	Съемные носители информации
	Каналы связи

	Мониторы
	Помещения/здания/сооружения
	Технические средства информационных систем
Сетевой уровень	Коммуникационное оборудование
Уровень сетевых приложений и сервисов	Сетевые приложения и сервисы
Уровень операционных систем	Файлы данных с информацией ограниченного распространения
	Общесистемные программные средства
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
	Файлы данных с открытой информацией
Уровень систем управления базами данных	Базы данных информационных систем
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
Уровень банковских технологических	Программное обеспечение, предназначенное для обработки защищаемой информации
процессов и приложений	Программное обеспечение, предназначенное для обработки открытой информации
	Информация, необходимая для идентификации, аутентификации и (или) авторизации
	Ключевые носители
	Бумажные документы
Уровень бизнеспроцессов	Информационные активы (сведения ограниченного доступа)
	люди

Таблица 3 – Способы реализации угроз безопасности информации

Уровни информационной инфраструктуры	**Способы реализации угроз**
Физический уровень	Хищение/кража
	Утрата
	Уничтожение/разрушение
	Несанкционированный физический доступ
	Утечка видовой информации
	Утечка информации по каналам ПЭМИН
Сетевой уровень	Атаки типа «отказ в обслуживании»
	Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа
	Нарушение штатных режимов работы сетевого оборудования
	Внедрение аппаратных закладок
Уровень сетевых приложений и сервисов	Внедрение вредоносного программного обеспечения
	Анализ трафика
	Атаки типа «отказ в обслуживании»
	Использование специализированных программ
	Нарушение штатных режимов работы сетевых приложений
	Отказ от авторства
	Сканирование сети, направленное на выявление открытых портов и служб, открытых соединений
Уровень операционных	Кража (утеря, компрометация) пароля

систем	Копирование
	Модификация/удаление
	Нарушение штатных режимов работы ОС
	Распространение вредоносных программ
	Неправильное (не полное) конфигурирование СЗИ
	Несанкционированный доступ в ОС с использованием специализированного ПО
Уровень систем управления базами данных	Копирование
	Неправильное (не полное) конфигурирование СЗИ
	Модификация/удаление
	Нарушение штатных режимов работы СУБД
	Подмена пользовательских идентификаторов
	Несанкционированный логический доступ к СУБД
	Распространение вредоносных программ
	Кража пароля
Уровень банковских технологических процессов и приложений	Отказ от авторства
	Модификация/удаление
	Распространение/передача
	Печать документов
	Нарушение штатных режимов работы приложений
	Кража документов и пластиковых карт
	Кража пароля
Уровень бизнеспроцессов	Непреднамеренное нарушение бизнес-процесса
	Преднамеренное нарушение бизнес-процесса

5.9.1. В зависимости от архитектуры и условий функционирования объектов информационной инфраструктуры для реализации угроз безопасности информации может быть использован удаленный, локальный или физический доступ к объектам информационной инфраструктуры.

5.9.1.2. Удаленный доступ при реализации угроз безопасности информации осуществляется нарушителем из-за границ контролируемой зоны при его взаимодействии с сетями связи общего пользования, в первую очередь с сетью Интернет. При удаленном доступе воздействия на объекты информационной инфраструктуры реализуются посредством сетевых протоколов.

5.9.1.3. Локальный доступ при реализации угроз безопасности информации может осуществляться нарушителем в пределах границ контролируемой зоны. При локальном доступе неправомерный доступ и (или) воздействие на объекты информационной инфраструктуры реализуются при наличии и использовании локальной учетной записи пользователя, зарегистрированной в системе. Удаленное использование нарушителем локальной учетной записи пользователя, в том числе из взаимодействующей (смежной) системы или сети Интернет, при реализации угрозы безопасности информации относится к локальному доступу.

5.9.1.4. Физический доступ для реализации угроз безопасности информации может осуществляться нарушителями в пределах границ контролируемой зоны и при наличии у них непосредственного физического доступа к объектам информационной инфраструктуры. Целью физического доступа нарушителя также может являться получение локального доступа для реализации локальных угроз безопасности информации. В этом случае оценке подлежат

угрозы безопасности информации, связанные с локальным доступом к объектам информационной инфраструктуры.

5.9.2. Для непреднамеренных угроз безопасности информации условием их возникновения является наличие у внутреннего нарушителя локального и (или) физического доступа к системам и сетям. При этом внутренний нарушитель может иметь привилегированные или непривилегированные права по доступу к объектам информационной инфраструктуры.

5.10. При моделировании угроз безопасности информации оценке подлежат угрозы безопасности информации, связанные со всеми типами источников. В целях создания и эксплуатации адекватной эффективной системы защиты необходимо уделять внимание оценке антропогенных источников угроз, связанных с действиями нарушителей. Оценка возможностей нарушителей включает определение категорий, видов нарушителей, их компетенции и оснащенности, которыми они могут обладать для реализации угроз безопасности информации.

5.10.1. Модель нарушителя содержит описание предположений о возможностях нарушителя (злоумышленника), которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

5.10.2. Нарушитель может действовать на различных этапах жизненного цикла информационных систем, обрабатывающих информационные активы Банка.

5.10.3. Главной целью нарушителя является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов более эффективно для нарушителя и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, но при этом более сложное для реализации, в связи с чем, атаки злоумышленника на объекты среды уровня бизнеспроцессов рассматриваются как совокупность атак на более низкие уровни информационной инфраструктуры.

5.10.4. Все физические лица, имеющие доступ к техническим и программным средствам, разделяются на следующие категории:

− категория I – лица, не имеющие права доступа в помещения, где расположены технические и программные средства;

− категория II – лица, имеющие право постоянного или разового доступа в помещения, где расположены технические и программные средства.

5.10.5. Все потенциальные нарушители подразделяются на:

− внешних нарушителей, осуществляющих атаки вне пределов контролируемой зоны Банка;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны Банка.

5.10.6. Таким образом, внешними нарушителями могут быть как лица категории I, так и лица категории II, а внутренними нарушителями могут быть только лица категории II.

5.10.7. Основные источники угроз безопасности информации приведены в Таблице 4.

Таблица 4 – Перечень источников угроз безопасности информации

Типы источников угроз безопасности информации	**Источники угроз безопасности информации**
Компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том	Хакер

числе использование компьютерных вирусов и других типов вредоносных	Компьютерный хулиган
Сотрудники Банка, являющиеся легальными участниками процессов в информационных системах и действующие в рамках предоставленных полномочий	Пользователи информационных систем
	Администраторы информационных систем
	Технический персонал, имеющий доступ к аппаратному обеспечению
	Администраторы средств защиты информации
Сотрудники Банка, являющиеся легальными участниками процессов в информационных системах и действующие вне рамок предоставленных полномочий	Администраторы средств защиты информации
	Пользователи информационных систем
	Администраторы информационных систем
	Технический персонал, имеющий доступ к аппаратному обеспечению
Неблагоприятные события природного и техногенного характера	Пожары
	Наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.
	Техногенные катастрофы
	Нарушение внутриклиматических условий
	Нарушение или снижение качества электропитания.
	Сбои и аварии в системах водоснабжения, канализации, отопления
Террористы, криминальные элементы	Террористы
	Криминальные элементы
	Недобросовестные конкуренты
Провайдеры	Провайдер канала связи
	Интернет-провайдер
Подрядчики, осуществляющие монтаж, пусконаладочные работы	Сотрудник технической поддержки
	Сервисный инженер
оборудования и его ремонт	Разработчик программного обеспечения
	Разработчик технических средств
Внешние нарушители, имеющие доступ к ИС	Аудитор
	Партнер
	Клиент
	Сотрудник Надзорного ведомства

5.11. Моделирование угроз безопасности информации носит систематический характер и осуществляться как на этапе создания объектов информационной инфраструктуры и формирования требований по их защите, так и в ходе их эксплуатации. Систематический подход к моделированию угроз безопасности информации позволяет поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных активов. Учет изменений угроз безопасности информации способствует своевременной выработке адекватных мер защиты информации.

5.12. На этапе создания объектов информационной инфраструктуры моделирование угроз безопасности информации проводится на основе их предполагаемой архитектуры и направлено на обоснованный выбор организационных мер, функциональных возможностей и настроек средств защиты информации. На этапе эксплуатации – моделирование угроз безопасности информации проводится для реальной архитектуры объектов информационной инфраструктуры и условий их функционирования и направлено на выявление изменений угроз безопасности информации и оценку эффективности применяемых мер и средств защиты информации.

5.13. Моделирование угроз безопасности информации проводится с учетом применяемых на объектах информационной инфраструктуры в соответствии с требованиями нормативных правовых актов Российской Федерации и (или) технических заданий средств защиты информации. Однако при этом учитывается возможность наличия в организации работ и применяемых средствах защиты информации уязвимостей, которые могут использоваться для реализации угроз безопасности информации.

5.14. Моделирование угроз безопасности информации проводится отделом автоматизации и информационного сопровождения. К моделированию угроз безопасности информации могут привлекаться организации, имеющие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

5.15. Результаты моделирования угроз безопасности информации отражаются в модели угроз, которая представляет собой формализованное описание актуальных угроз безопасности информации.

5.16. Модель угроз безопасности информации формируется применительно ко всем объектам информационной инфраструктуры, которые были включены в границу процесса моделирования угроз безопасности информации. По решению Руководства Банка модель угроз безопасности информации может разрабатываться для отдельной системы или сети.

5.17. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования объектов информационной инфраструктуры.

5.18. Модель угроз применяется при решении следующих задач:

− анализа защищенности от угроз безопасности информационных активов Банка в ходе организации и выполнения работ по обеспечению безопасности информации;

− разработки системы защиты информации, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты информации;

− проведения мероприятий, направленных на предотвращение несанкционированного доступа в информационные системы и к обрабатываемым в них информационным активам, включая предотвращение несанкционированного воздействия на технические и программные средства информационных систем;

− контроля за обеспечением уровня защищенности информационных активов;

− определения совокупности условий и факторов, создающих опасность нарушения характеристик безопасности;

− определения типов источников угроз.

5.19. Изменение модели угроз безопасности информации осуществляется в случаях:

− изменения требований нормативных правовых актов Российской Федерации и методических документов ФСТЭК России, в том числе нормативных актов Банка России, регламентирующих вопросы моделирования угроз безопасности информации;

− изменения архитектуры и условий функционирования объектов информационной инфраструктуры, порядка обработки информации, влияющих на угрозы безопасности информации;

− выявления, в том числе по результатам внешнего или внутреннего контроля эффективности защиты информации (аудита, тестирований на проникновение), новых угроз безопасности информации или новых сценариев реализации существующих угроз.

− выявление уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

− появления сведений и фактов о новых возможностях нарушителей.

5.20. При проведении внутреннего или внешнего контроля эффективности защиты информации (аудита, тестирований на проникновение) перед организациями, проводящими такие работы, должна ставиться задача по выявлению максимально возможного числа сценариев реализации существующих угроз безопасности информации, а также задача выявления новых угроз безопасности информации, приводящих к наступлению негативных последствий.

6. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В результате воздействия угроз безопасности информации на уязвимости могут возникнуть следующие последствия, влияющие на состояние информационной безопасности Банка и его нормальное функционирование:

− финансовые потери, связанные с утратой, утечкой или недоступностью информации;

− финансовые потери, связанные с уничтожением и последующим восстановлением информации;

− ущерб от дезорганизации деятельности Банка и потери, связанные с невыполнением им своих обязательств;

− ущерб репутации Банка;

− юридические и финансовые санкции со стороны регуляторов;

− другие потери.

6.2. Уязвимость информационной безопасности создает предпосылки к реализации угрозы через нее. Реализация угрозы нарушения информационной безопасности приводит к утрате защищенности интересов (целей) Банка в информационной сфере, в результате чего Банку может быть нанесен ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента информационной безопасности определяют величину риска.

6.3. Риски нарушения информационной безопасности включают в себя риск преднамеренных действий со стороны сотрудников Банка и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой указанными объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа (киберриск) и другие виды риска, связанных с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры.

6.4. Порядок управления рисками информационной безопасности определяется во внутренних нормативных документах Банка.

6.5. Риски нарушения информационной безопасности являются неотъемлемой частью операционных рисков и определяется на основании качественных оценок:

− степени возможности реализации угроз безопасности информации выявленными и (или) предполагаемыми источниками угроз безопасности информации в результате их воздействия на объекты среды рассматриваемых типов информационных активов;

− степени тяжести последствий от потери свойств информационной безопасности для рассматриваемых типов информационных активов.

6.6. Оценка степени возможности реализации угроз безопасности информации и степени тяжести последствий нарушения информационной безопасности базируется на экспертной оценке, выполняемой начальником Службы информационной безопасности с привлечением сотрудников Департамента автоматизации банковских операций. Для оценки степени тяжести последствий от потери свойств информационной безопасности дополнительно привлекаются сотрудники профильных подразделений, использующих рассматриваемые типы информационных активов. Взаимодействие сотрудников указанных подразделений осуществляется в рамках постоянно действующей или создаваемой на время проведения оценки рисков нарушения информационной безопасности рабочей группы.

6.7. Настоящий раздел содержит порядок (методику) оценки рисков нарушения информационной безопасности.

6.8. Исходными данными для оценки рисков нарушения информационной безопасности является информация, определенная в п. 4.3 настоящей Политики.

6.9. Для проведения оценки рисков нарушения информационной безопасности выполняются следующие процедуры:

− Процедура 1. Определение перечня типов информационных активов, для которых выполняются процедуры оценки рисков нарушения информационной безопасности (далее — область оценки рисков нарушения информационной безопасности).

− Процедура 2. Определение перечня типов объектов среды, соответствующих каждому из типов информационных активов области оценки рисков нарушения информационной безопасности.

− Процедура 3. Определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения процедуры 2.

− Процедура 4. Определение степени вероятности реализации угроз безопасности информации применительно к типам объектов среды, определенных в рамках выполнения процедуры 2.3.

− Процедура 5. Определение степени тяжести последствий нарушения информационной безопасности для типов информационных активов области оценки рисков нарушения информационной безопасности.

− Процедура 6. Оценка рисков нарушения информационной безопасности.

6.10. Область оценки рисков нарушения информационной безопасности определяется как:

− перечень типов информационных активов в целом;

− перечень типов информационных активов подразделений Банка;

− перечень типов информационных активов, соответствующих отдельным процессам деятельности Банка в целом или подразделения Банка.

6.10.1. Для каждого из типов информационных активов определяется перечень свойств информационной безопасности, поддержание которых необходимо обеспечивать в рамках системы обеспечения информационной безопасности: конфиденциальность, целостность и доступность.

6.10.2. При необходимости для конкретных типов информационных активов могут определяться другие (дополнительные) свойства информационной безопасности.

6.11. Для каждого из выделенных типов информационных активов составляется перечень типов объектов среды. При составлении данного перечня рассматриваемые типы объектов среды разделяются по уровням информационной инфраструктуры.

6.12. Для каждого из определенных типов объектов среды составляется перечень источников угроз, воздействие которых может привести к потере свойств информационной безопасности соответствующих типов информационных активов. Типы объектов среды и выявляемые для них источники угроз должны соответствовать друг другу в рамках иерархии информационной инфраструктуры.

6.12.1. Перечень источников угроз формируется на основе модели угроз. При этом возможно расширение первоначального перечня источников угроз, зафиксированных в модели угроз (или же его дополнительная структуризация путем составления новых моделей угроз для некоторых из выделенных типов объектов среды или отдельных объектов среды).

6.12.2. При формировании перечня источников угроз необходимо рассматривать возможные способы их воздействия на объекты среды, в результате чего возможна потеря свойств информационной безопасности соответствующих типов информационных активов (способы реализации угроз безопасности информации). Степень детализации и порядок группировки для рассмотрения способов реализации угроз безопасности информации определяются Банком.

6.13. Для выполнения оценки степени вероятности реализации угроз безопасности информации используются результаты выполнения процедур 1, 2, 3 и проводится анализ возможности потери каждого из свойств информационной безопасности для каждого из типов информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз.

6.13.1. Основным фактором для оценки степени вероятности реализации угроз безопасности информации является информация соответствующих моделей угроз, в частности:

− данные о расположении источника угрозы безопасности информации относительно соответствующих типов объектов среды;

− информация о мотивации источника угрозы безопасности информации (для источников угроз безопасности информации антропогенного характера);

− предположения о квалификации и (или) ресурсах источника угрозы безопасности информации;

− статистические данные о частоте реализации угрозы безопасности информации ее источником в прошлом;

− информация о способах реализации угроз безопасности информации;

− информация о сложности обнаружения реализации угрозы безопасности информации рассматриваемым источником;

− данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих априорных защитных мер.

6.13.2. Для оценки степени вероятности реализации угроз безопасности информации используется следующая качественная шкала степеней:

− нереализуемая;

− минимальная;

− средняя;

− высокая;

− критическая.

6.14. Для выполнения оценки степени тяжести последствий нарушения информационной безопасности используются результаты выполнения процедур 1, 2, 3 и проводится анализ последствий потери каждого из свойств безопасности информации для каждого из типов информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз.

6.14.1. Основными факторами для оценки степени тяжести последствий нарушения информационной безопасности являются:

− степень влияния на непрерывность деятельности;

− степень влияния на деловую репутацию;

− объем финансовых и материальных потерь;

− объем финансовых и материальных затрат, необходимых для восстановления свойств безопасности информации для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;

− объем людских ресурсов, необходимых для восстановления свойств безопасности информации для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;

− объем временных затрат, необходимых для восстановления свойств информационной безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;

− степень нарушения законодательных требований и (или) договорных обязательств;

− степень нарушения требований, регулирующих и контролирующих (надзорных) органов в области информационной безопасности, а также требований нормативных актов Банка России;

− объем хранимой, передаваемой, обрабатываемой, уничтожаемой информации, соответствующей рассматриваемому типу объекта среды;

− данные о наличии у рассматриваемых типов объектов среды организационных, технических и прочих апостериорных защитных мер.

6.14.2. Для оценки степени тяжести последствий нарушения информационной безопасности вследствие реализации угроз безопасности информации используется следующая качественная шкала степеней:

− минимальная;

− средняя;

− высокая;

− критическая.

6.15. Оценка рисков нарушения информационной безопасности проводится на основании сопоставления оценок степени вероятности реализации угроз безопасности информации и оценок степени тяжести последствий нарушения информационной безопасности вследствие реализации соответствующих угроз.

6.15.1. Оценка рисков проводится для всех свойств информационной безопасности выделенных типов информационных активов и всех соответствующих им комбинаций типов объектов среды и воздействующих на них источников угроз безопасности информации.

6.15.2. Для выполнения оценки рисков нарушения информационной безопасности необходимо использовать результаты выполнения процедур 4 и 5.

6.15.3. Для оценки рисков нарушения информационной безопасности используется следующая качественная шкала:

- допустимый;
- недопустимый.

6.15.4. Для сопоставления оценок степени вероятности реализации угроз безопасности информации и оценок степени тяжести последствий нарушения информационной безопасности заполняется таблица допустимых/недопустимых рисков нарушения информационной безопасности (таблица 5).

Таблица 5 – Допустимые/недопустимые риски нарушения информационной безопасности

Степень вероятности реализации угроз безопасности информации	**Степень тяжести последствий нарушения информационной безопасности**			
	Минимальная	**Средняя**	**Высокая**	**Критическая**
Нереализуемая	допустимый	допустимый	допустимый	допустимый
Минимальная	допустимый	допустимый	допустимый	**недопустимый**
Средняя	допустимый	допустимый	**недопустимый**	**недопустимый**
Высокая	допустимый	**недопустимый**	**недопустимый**	**недопустимый**
Критическая	**недопустимый**	**недопустимый**	**недопустимый**	**недопустимый**

6.16. Результаты выполнения процедур, данные, на основании которых проводится оценка степени вероятности реализации угроз безопасности информации и оценка степени тяжести последствий нарушения информационной безопасности, и результаты самой оценки документально фиксируются в Отчетах по обеспечению информационной безопасности и Отчетах по событиям риска информационной безопасности, порядок и сроки составления которых установлены в разделе 11 Политики.

6.17. По результатам оценки рисков определяется способ обработки для каждого из рисков, реализация которого является недопустимым.

6.18. Цели обработки рисков:

- добиться значительного уменьшения рисков при относительно низких затратах;
- поддерживать принятые риски на допустимом, низком уровне.

6.19. Обработка рисков информационной безопасности заключается в комплексе организационных мероприятий, направленном на снижение операционных рисков за счет увеличения надежности и защищенности автоматизированных систем Банка.

6.20. Негативное влияние риска информационной безопасности определяется в виде потерь. Виды потерь от реализации событий риска информационной безопасности подразделяются на прямые и непрямые потери. Банк использует следующие дополнительные (специфические) виды прямых и непрямых потерь от реализации риска нарушения информационной безопасности для классификации событий риска нарушения информационной безопасности в дополнение к установленным в Положении Банка России № 716-П.

6.20.1. Детализация видов потерь установлена в приложении 4 к Политике управления операционным риском.

6.21. Инциденты, приведшие к фактической реализации риска информационной безопасности, в том числе киберриска, обусловленные источниками риска информационной безопасности, в том числе инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных в соответствии с Положением Банка России 719-П и Положением Банка России № 683-П, вследствие которых возникли прямые и непрямые потери Банка, фиксируются в базе событий с присвоением вида операционного риска в соответствии с Положением Банка России 716-П.

6.22. Сигнальные и контрольные значения контрольных показателей уровня риска информационной безопасности.

Базовый набор показателей системы управления операционным риском информационной безопасности включает количественные и качественные показатели, сигнальные и контрольные значения. Методика их расчета установлена в приложении 3 к Положению по управлению операционным риском.

6.23. Требования к внешним контрагентам, выполняющим функции обеспечения информационной безопасности (аутсорсингу), а также определение порядка взаимодействия и распределения ответственности между ними.

6.23.1. Аутсорсинг информационной безопасности рассматривается в качестве альтернативы реализации, поддержки и улучшения СОИБ силами работников Службы информационной безопасности.

6.23.2. Целью Банка при аутсорсинге процессов СОИБ является привлечение квалифицированного персонала и получение готовых процессов и развитой методологии, а также средств, систем и технологий обеспечения информационной безопасности, необходимых для организации и эксплуатации СОИБ.

6.23.3. Поставщик услуг аутсорсинга информационной безопасности может использовать уже применяемые в Банке средства и системы обеспечения информационной безопасности - принимать их на эксплуатацию и (или) администрирование.

6.23.4. Основными целями, при использовании аутсорсинга информационной безопасности в Банке является:

- кадровое обеспечение;
- экономическая эффективность;
- техническое и технологическое обеспечение.

6.23.5. На аутсорсинг не могут передаваться функции, связанные с выбором требуемого уровня защищенности, а также функции, связанные с принятием рисков нарушения информационной безопасности.

7. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Под ресурсным обеспечением информационной безопасности понимается процесс управления, обеспечивающий определение потребностей в ресурсах информационной

безопасности и контроль эффективности использования ресурсов информационной безопасности.

7.2. Основными целями реализации ресурсного обеспечения информационной безопасности являются:

− обеспечение процессов системы информационной безопасности финансовыми средствами;

− обеспечение Банка кадровыми ресурсами, необходимыми и достаточными для реализации процессов системы обеспечения информационной безопасности;

− контроль эффективности использования ресурсов информационной безопасности.

7.3. Потребности в обеспечении процессов системы информационной безопасности ресурсами информационной безопасности определяются на основе предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) в случае реализации актуальных рисков нарушения информационной безопасности.

7.4. Банком обеспечивается надлежащий баланс между актуальными рисками информационной безопасности, связанными с наличием уязвимостей в выполнении процессов системы обеспечения информационной безопасности, и ресурсами информационной безопасности, используемыми для обеспечения целевого уровня защиты информации и, соответственно, направленными на снижение указанных рисков.

7.5. Для реализации ресурсного обеспечения информационной безопасности:

− устанавливается оценка уровня зрелости, выполнения процессов системы обеспечения информационной безопасности;

− устанавливается оценка рисков информационной безопасности с учетом данных о реализованном уровня зрелости, выполнения процессов системы обеспечения информационной безопасности;

− обеспечивается целевой уровень защиты информации путем повышения уровня зрелости выполнения процессов системы обеспечения информационной безопасности до значения, реализующего снижение рисков информационной безопасности до допустимого уровня. Повышение уровня зрелости выполнения процессов системы обеспечения информационной безопасности достигается путем:

• инвестирования необходимых финансовых средств в обеспечение процессов системы обеспечения информационной безопасности. При этом инвестирование не предполагает получение дохода от выполнения процессов системы обеспечения информационной безопасности, а приводит к снижению предполагаемой величины возможного ущерба (финансового эквивалента возможных потерь) в случае реализации актуальных рисков информационной безопасности;

• обеспечения необходимых и достаточных кадровых ресурсов;

− проводится контроль эффективности инвестирования в обеспечение процессов системы обеспечения информационной безопасности путем установления и мониторинга целевых (контрольных) показателей, выраженных в количественной (денежной) форме.

7.6. Определение потребности Банка в кадровых ресурсах заключается в установлении необходимого и достаточного количества, а также требуемой компетенции сотрудников, ответственных за обеспечение информационной безопасности, выполняемой на основе:

− анализа задач и функций, возложенных на указанных сотрудников;

− уровня автоматизации процессов системы обеспечения информационной безопасности и централизации управления средствами автоматизации;

− прогноза возможного расширения состава задач и функций указанных сотрудников в соответствии с планами совершенствования процессов системы обеспечения информационной безопасности вследствие развития бизнес-процессов, совершенствования процессов информатизации, развития Банка.

7.6.1. При планировании (совершенствовании) процессов системы обеспечения информационной безопасности необходимо обеспечить выделение ресурсов информационной безопасности для эффективной реализации требований законодательства Российской Федерации, нормативных актов Банка России, требований к обеспечению информационной безопасности, установленных Банком.

7.6.2. Банку необходимо установить состав задач и функций сотрудников, ответственных за обеспечение информационной безопасности, для каждого уровня полноты и качества выполнения процессов системы обеспечения информационной безопасности, оценив при этом трудозатраты на их выполнение.

7.6.3. Банком определяется минимальная необходимая и достаточная численность сотрудников, ответственных за обеспечение информационной безопасности, исходя из следующих показателей:

− трудозатраты на выполнение задачи и функций обеспечения информационной безопасности;

− количество реализуемых процессов системы обеспечения информационной безопасности;

− масштаб выполнения управляемых процессов системы обеспечения информационной безопасности, в том числе:

- количество подразделений Банка;
- количество автоматизированных банковских систем;
- количество сотрудников Банка;
- расположение подразделений Банка.

7.6.4. Сотрудники Банка, ответственные за обеспечение информационной безопасности, должны обладать компетенцией, необходимой для выполнения их функциональных обязанностей. Определение компетенции сводится к установлению требований в отношении знаний, практических навыков и опыта работы в соответствующей области указанных сотрудников. К основным требованиям, определяющим необходимую компетенцию указанных сотрудников, следует среди прочего относить:

− наличие высшего профессионального образования в области информационной безопасности и (или) информационных технологий;

− опыт работы в области информационной безопасности не менее двух лет;

− регулярное прохождение дополнительного (специализированного) обучения (повышения квалификации) в области информационной безопасности;

− знание требований законодательства Российской Федерации, в том числе нормативных актов Банка России, необходимых для надлежащего выполнения функций, возложенных на указанных сотрудников;

− знание внутренних нормативно-методических и организационно-распорядительных документов в области информационной безопасности;

− осведомленность по вопросам, касающимся средств, систем и технологий обеспечения информационной безопасности, а также способов и практик их применения.

7.7. Достижение надлежащего баланса между величинами рисков информационной безопасности, связанных с наличием уязвимостей при выполнении процессов системы обеспечения информационной безопасности и ресурсным обеспечением информационной безопасности, направленным на снижение указанных рисков путем обеспечения необходимого и достаточного уровня зрелости выполнения процессов системы обеспечения информационной безопасности, обеспечивается путем определения и анализа целевых (контрольных) показателей эффективности использования финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов системы обеспечения информационной безопасности.

7.7.1. Показатели эффективности делятся на две группы:

− показатели, подлежащие анализу на этапе планирования инвестирования в повышение уровня зрелости выполнения процессов системы обеспечения информационной безопасности;

− показатели, подлежащие анализу на этапе оценки результатов инвестирования в уровень зрелости выполнения процессов системы обеспечения информационной безопасности.

7.7.2. В качестве основных показателей эффективности инвестирования в выполнение процессов системы обеспечения информационной безопасности на этапе планирования рассматриваются:

− ожидаемые результаты от снижения уровня рисков информационной безопасности, связанных с повышением уровня зрелости выполнения процессов системы обеспечения информационной безопасности;

− срок получения ожидаемых результатов по повышению уровня зрелости выполнения процессов системы обеспечения информационной безопасности;

− согласованность со стратегией информационного развития Банка.

7.7.3. Указанные показатели эффективности оцениваются экспертным путем с привлечением профильных подразделений Банка и включаются в оценку финансовых средств, инвестированных в повышение уровня зрелости выполнения процессов системы обеспечения информационной безопасности.

7.7.4. В качестве основного показателя эффективности инвестирования финансовых средств в повышение уровня зрелости выполнения процессов системы обеспечения на этапе оценки результатов инвестирования рассматривается соотношение фактического ущерба (финансового эквивалента понесенных потерь) от инцидентов информационной безопасности, в том числе непосредственных финансовых потерь от инцидентов информационной безопасности, финансовых потерь от нарушения непрерывности деятельности Банка, финансовых потерь от негативного влияния инцидентов информационной безопасности на деловую репутацию, финансовые средства, затраченные для ликвидации последствий инцидентов информационной безопасности, по отношению к предполагаемой на этапе планирования величине возможного ущерба (финансового эквивалента возможных потерь).

7.7.5. При превышении фактических финансовых потерь от инцидентов информационной безопасности значений, предполагаемых на этапе планирования, определяются основные факторы возникновения рисковых событий, приводящих к ущербу (финансовым потерям) и вырабатываются планы, элементами которых могут являться:

− пересмотр модели угроз и нарушителя, применяемых требований к обеспечению информационной безопасности;

− установление новых процессов системы обеспечения информационной безопасности, в том числе связанных с изменениями состава актуальных угроз;

− повышение уровня зрелости выполнения установленных процессов системы обеспечения информационной безопасности.

7.7.6. В качестве дополнительного показателя эффективности инвестирования в повышение уровня зрелости выполнения процессов системы обеспечения информационной безопасности на этапе оценки результатов инвестирования рассматривается соответствие фактических сроков реализации планов по повышению уровня зрелости выполнения процессов системы обеспечения информационной безопасности планируемым срокам.

7.7.7. Банком выполняются с установленной периодичностью:

− анализ эффективности выполнения процессов системы обеспечения информационной безопасности, в том числе выполняемый на основе показателей, установленных в пункте 7.7.1. настоящего раздела;

− анализ рисков информационной безопасности с целью определения приоритетных направлений совершенствования процессов системы обеспечения информационной безопасности.

8. ОСНОВНЫЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. К основным требованиям обеспечения информационной безопасности объектов информационной инфраструктуры Банка относятся:

− требования к управлению информационной безопасностью в Банке;

− требования к обеспечению информационной безопасности при назначении и распределении ролей и обеспечения доверия к персоналу;

− требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла;

− требования по обеспечению информационной безопасности при управлении доступом и регистрации;

− требования по обеспечению информационной безопасности средствами антивирусной защиты;

− требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

− требования по обеспечению информационной безопасности банковских (платежных и информационных) технологических процессов;

− требования по обеспечению информационной безопасности при обработке персональных данных;

− требования по обеспечению соответствия законодательным актам, нормативным документам Российской Федерации в области обеспечения информационной безопасности и нормативным актам Банка России;

− требования по обеспечению (управлению) непрерывности бизнеса;

− требования к организации обнаружения и реагирования на инциденты информационной безопасности;

− к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности.

8.2. Конкретизация требований оформляется отдельными документами и производится на основании:

− результатов оценки рисков нарушения информационной безопасности;

− требований законодательства Российской Федерации, нормативно-методических документов Банка России, ФСБ России, ФСТЭК России;

− особенностей обработки информационных активов в конкретных информационных системах.

8.3. На основе сформированных требований выбираются меры по обеспечению информационной безопасности Банка.

8.4. Основными мерами по обеспечению информационной безопасности являются:

− административно-правовые и организационные меры;

− технические, основанные на использовании аппаратно-программных средств;

− режимные;

− комбинированные – на основе первых трёх типов.

9. СОСТАВ И СОДЕРЖАНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

9.1. Полнота и качество применения мер защиты информации достигается планированием, реализацией, проверкой и совершенствованием системы защиты информации, осуществляемыми в рамках системы организации и управления защитой информации, а также применением мер защиты информации на этапах жизненного цикла автоматизированных систем и приложений.

9.2. Настоящий раздел определяет состав, содержание и порядок применения организационных и технических мер защиты информации, реализуемых в рамках процесса системы обеспечения информационной безопасности в Банке.

9.3. Все меры защиты информации, реализуемые в рамках процесса системы защиты информации, определяются в соответствии с Положением Банка России № 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», Положением Банка России № 747-П «О требованиях к защите информации в платежной системе», Положением Банка России от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств» и национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций.
Базовый состав организационных и технических мер».

9.4. В качестве основных мер защиты информации применяются:

− документальное оформление перечня сведений конфиденциального характера с учетом отраслевой специфики этих сведений;

− реализация разрешительной системы допуска пользователей и эксплуатационного персонала к информации и связанным и ее использованием работам, документам;

− ограничение доступа сотрудников Банка и посторонних лиц в помещения, где размещены объекты информационной инфраструктуры, а также хранятся носители информации;

− регистрация действий пользователей и эксплуатационного персонала, контроль за несанкционированным доступом и действиями пользователей, эксплуатационного персонала и посторонних лиц;

− учет и надежное хранение бумажных и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее их хищение, подмену и уничтожение;

− необходимое резервирование технических средств и дублирование массивов и носителей информации;

− использование сертифицированных средств защиты информации;

− размещение объектов информационной инфраструктуры на максимально возможном расстоянии относительно границы контролируемой зоны;

− использование защищенных каналов связи и средств криптографической защиты информации;

− размещение мониторов и других средств отображения информации, исключающее несанкционированный просмотр информации;

− организация физической защиты помещений и объектов информационной инфраструктуры с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здание, помещения посторонних лиц, хищение документов и носителей информации, самих объектов информационной инфраструктуры, исключающих нахождение внутри контролируемой зоны посторонних лиц (без сопровождения);

− предотвращение внедрения в автоматизированные системы вредоносного кода.

9.5. Назначение и распределение ролей и обеспечение доверия к персоналу.

9.5.1. «Ролевое» управление является основным механизмом управления полномочиями пользователей и эксплуатационного персонала.

9.5.2. Роли персонифицируются и формируются с учетом принципа минимальности полномочий, необходимых для выполнения служебных обязанностей.

9.5.3. Не допускается совмещение следующих функций в рамках роли одним субъектом: администратора системы и администратора информационной безопасности; выполнения операций в системе и контроля их выполнения; эксплуатации и (или) контроль эксплуатации ресурсов доступа и использования по назначению ресурса доступа в рамках системы обеспечению информационной безопасности; создания и (или) модернизации ресурса доступа и использования по назначению ресурса доступа в рамках системы обеспечению информационной безопасности; эксплуатации и контроля эксплуатации средств и систем защиты информации; управления учетными записями и управления правами учетных записей.

9.5.4. Критичные технологические процессы защищаются от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления выполняются через специальные роли в системах.

9.5.5. Должностные обязанности сотрудников и трудовые договоры предусматривают их обязанности по выполнению требований по обеспечению информационной безопасности, включая обязательства по неразглашению конфиденциальной информации.

9.5.6. Приказы, распоряжения, нормативные документы по обеспечению информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников Банка.

9.5.7. Все сотрудники Банка дают письменное обязательство о соблюдении конфиденциальности, включая требования по недопущению конфликта интересов.

9.5.8. При взаимодействии с внешними организациями и клиентами Банка требования по обеспечению информационной безопасности регламентируются положениями, включаемыми в договоры (соглашения) с ними.

9.5.9. Невыполнение сотрудниками Банка требований по обеспечению информационной безопасности приравнивается к невыполнению должностных обязательств и приводит, как минимум, к дисциплинарной ответственности.

9.6. Управление жизненным циклом автоматизированных банковских систем.

9.6.1. Правила и процедуры управления жизненным циклом автоматизированных банковских систем регламентируются в организационно распорядительных документах по информационной безопасности.

9.6.2. Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных банковских систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации. Все действия с автоматизированными банковскими системами на стадиях жизненного цикла должны осуществляться при участии администратора информационной безопасности.

9.6.3. Разработка и тестирование программного обеспечения автоматизированных банковских систем проводятся в выделенном сегменте локальной вычислительной сети, на выделенных физически или логически средствах вычислительной техники, доступ из которого к промышленным системам ограничивается.

9.6.4. Эксплуатируемые автоматизированные банковские системы и (или) их компоненты снабжаются документацией, содержащей описание реализованных в автоматизированных банковских системах защитных мер, в том силе описание состава и требований к реализации организационных мер защиты, состава и эксплуатации технических мер защиты.

9.6.5. В договорах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к финансовому ущербу Банка, а также соблюдение конфиденциальности.

9.6.6. При разработке технических заданий на системы дистанционного банковского обслуживания учитывается, что защита данных должна обеспечиваться в условиях:

− попыток несанкционированного доступа к информации анонимных, неавторизованных злоумышленников с использованием сетей общего пользования;

− возможности ошибок авторизованных пользователей систем;

− возможности ненамеренного или неадекватного использования защищаемой информации авторизованными пользователями.

9.6.7. На стадии эксплуатации автоматизированной банковской системы определяются, выполняются и регистрируются процедуры:

− контроля работоспособности (функционирования, эффективности) реализованных в автоматизированной банковской системе защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;

− контроля отсутствия уязвимостей в оборудовании и программном обеспечении автоматизированной банковской системы;

− контроля внесения изменений в параметры настройки автоматизированной банковской системы и применяемых технических защитных мер;

− контроля необходимого обновления программного обеспечения автоматизированной банковской системы, включая программное обеспечение технических защитных мер.

9.6.8. Применяется прикладное программное обеспечение автоматизированных банковских систем, сертифицированное на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

9.6.9. Все изменения, вносимые в автоматизированные банковские системы, включая обновление программного обеспечения, контролируются и документируются.

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

− умышленного несанкционированного раскрытия, модификации или уничтожения информации;

− неумышленной модификации, раскрытия или уничтожения информации;

− отказа в обслуживании или ухудшения обслуживания.

9.6.11. При выводе автоматизированных банковских систем из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление защищаемой информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов баз данных.

9.7. Управление доступом к информационным активам и регистрация событий.

9.7.1. Правила и процедуры управления доступом к информационным активам и регистрации событий регламентируются в организационно распорядительных документах по информационной безопасности.

9.7.2. Все объекты информационной инфраструктуры (информационные активы) Банка идентифицируются, классифицируются, учитываются и имеют своих владельцев.

9.7.3. Доступ к информационным активам всем сотрудникам Банка предоставляется только на основании заявок.

9.7.4. Применяются различные защитные меры: встроенные, сертифицированные средства защиты информации от несанкционированного доступа и нерегламентированных действий в рамках предоставленных полномочий.

9.7.5. Процедуры управления доступом исключают возможность бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа, самостоятельного изменения параметров настроек средств защиты информации.

9.7.6. Учетные записи пользователей персонифицируются.

9.7.7. При доступе в информационную систему осуществляется идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

9.7.8. Аутентификация пользователей осуществляется с использованием паролей, аппаратных средств, в случае многофакторной аутентификации – определенной комбинацией указанных средств.

9.7.9. В Банке определяется, выполняется и контролируется парольная политика для пользователей.

9.7.10. Для идентификационных и аутентификационных данных организуется и обеспечивается защита.

9.7.11. Доступ к информационным ресурсам, программным средствам обработки (передачи) и защиты информации для пользователей и эксплуатационного персонала разграничивается в соответствии с их служебными обязанностями.

9.7.12. Доступ к информационным активам прекращается в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника.

9.7.13. Проводится периодический контроль соответствия согласованных и реальных прав доступа к информационным активам текущему статусу пользователя.

9.7.14. Доступ ко всем информационным активам Банка осуществляется только после авторизации пользователей.

9.7.15. В автоматизированных банковских системах, в том числе системе дистанционного банковского обслуживания, регистрируются:

− операции с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов;

− проводимых транзакций, имеющих финансовые последствия;

− операции, связанные с назначением и распределением прав пользователей.

9.7.16. В системе дистанционного банковского обслуживания применяется электронная подпись для подтверждения авторства проводимых клиентами операций.

9.7.17. Журналы аудита действий пользователей и эксплуатационного персонала информативны, защищаются от модификации и хранятся в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов информационной безопасности. Автоматизированные банковские системы содержат штатные средства анализа аудит-файлов и формирования отчетов по заданным критериям.

9.8. Антивирусная защита.

9.8.1. Порядок обеспечения антивирусной защиты регламентируется в организационной распорядительной документации.

9.8.2. На всех автоматизированных рабочих местах и серверах применяются средства антивирусной защиты.

9.8.3. Каждый сотрудник Банка обязан выполнять правила эксплуатации антивирусного программного обеспечения и требования по антивирусной защите в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать отдел автоматизации и информационного сопровождения при подозрениях на вирусное заражение.

9.8.4. Техническая возможность подключения пользователями к рабочим станциям внешних накопителей информации должна максимально ограничиваться.

9.8.5. Антивирусная защита должна обеспечиваться использованием специализированного сертифицированного антивирусного программного обеспечения. Должно организовываться построение эшелонированной централизованной антивирусной защиты. Средства антивирусной защиты и их базы должны регулярно обновляться.

9.8.6. Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств защиты, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизовано в автоматическом режиме. При этом должен обеспечиваться минимально возможный период обновления.

9.9. Использование ресурсов сети Интернет.

9.9.1. Порядок использования ресурсов сети Интернет регламентируется в организационной распорядительной документации.

9.9.2. Использование ресурсов сети Интернет в Банке должно осуществляться исключительно в служебных целях.

9.9.3. При обмене почтовыми сообщениями:

− обеспечивается антивирусная фильтрация всего трафика электронного почтового обмена;

− используются необходимые защитные меры (установка межсетевых экранов, организация демилитаризированной зоны и т.д.).

9.9.4. Подключение к рабочим станциям мобильных телефонов запрещается.

9.9.5. Доступ сотрудников Банка к ресурсам сети Интернет санкционируется руководством и предоставляется администратором информационной безопасности.

9.9.6. На узлах доступа в сеть Интернет должны приниматься необходимые меры для противодействия хакерским атакам и распространению спама.

9.10. Использование средств криптографической защиты информации.

9.10.1. Применение средств криптографической защиты информации для обеспечения безопасности информационных активов Банка и взаимодействия с клиентами производится в соответствии с порядком, установленным государственными уполномоченными органами.

9.10.2. Использование средств электронной подписи обеспечивает целостность электронного документа и подтверждает авторство.

9.10.3. В информационных системах Банка электронная подпись и (или) другие механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности, а также в случаях, когда необходимо разделить ответственность между подразделениями или сотрудниками Банка**.**

9.10.4. Конфиденциальность защищаемой информации при передаче по внешним каналам связи обеспечивается обязательным применением шифрования. В отдельных случаях информация, составляющая коммерческую тайну, может также шифроваться при ее передаче в локальной вычислительной сети и хранении на средствах вычислительной техники.

9.10.5. Передаваемые клиентам Банка средства шифрования обеспечивают возможность их использования только для организации защищенного взаимодействия с Банком.

9.10.6. Риски, связанные с возможной компрометацией криптографических ключей и доступом к защищаемой информации в обход средств криптографической защиты, минимизируются специальными техническими и организационными мерами.

9.11. Защита банковских (платежных и информационных) технологических процессов.

9.11.1. Порядок обмена платежной информацией фиксируется в договорах между участниками, осуществляющими обмен платежной информацией.

9.11.2. Технологические процессы максимально автоматизированы и обеспечивают возможность выполнения массовых и потенциально опасных операций без участия персонала за счет реализации эффективных процедур контентного контроля и защиты.

9.11.3. Выполнение критичных операций подтверждается самим клиентом при условии его надежной аутентификации.

9.11.4. Для защиты технологических процессов по результатам анализа рисков информационной безопасности применяются как штатные средства безопасности операционных систем, систем управления базами данных, так и дополнительные программные и программно-аппаратные комплексы и средства криптографической защиты информации, в совокупности обеспечивающие достаточный уровень безопасности на всех участках и этапах технологического процесса.

9.11.5. Меры безопасности, реализованные в системах дистанционного банковского обслуживания и рекомендуемые клиентам, обеспечивают при их выполнении адекватный с Банком уровень контроля за рисками информационной безопасности при той же модели нарушителя.

9.12. Обеспечение защиты персональных данных.

9.12.1. Порядок обеспечения защиты персональных данных регламентируется законодательством Российской Федерации и организационно-распорядительными документами Банка по защите информации.

9.12.2. Защита персональных данных осуществляется исходя их целей обработки. Для каждой цели должны быть утверждены руководством Банка: объем и содержание персональных данных, сроки обработки и хранения персональных данных, необходимость получения согласия субъектов персональных данных.

9.12.3. При достижении целей обработки персональных данных, либо по требованию субъекта персональных данных, персональные данные подлежат уничтожению в сроки, установленные законодательством Российской Федерации.

9.12.4. Перечень информационных систем персональных данных должен включать категории систем, перечень работников, допущенных к обработке персональных данных и должен быть актуален.

9.13. Обеспечение непрерывности бизнеса и восстановления после сбоев.

9.13.1. В Банке утвержден и введен в действие план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, в котором определены требования по обеспечению информационной безопасности, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в том числе требования к мероприятиям по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи. При разработке плана учитываются результаты оценки рисков нарушения информационной безопасности применительно к объектам

информационной инфраструктуры, существенным для обеспечения непрерывности бизнеса и его восстановления после сбоев.

9.13.2. Непрерывность критичных бизнес-процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности.

9.14. Разработка и организация реализации программ по обучению и повышению осведомленности в области информационной безопасности.

9.14.1. Начальник Службы информационной безопасности организует работу с сотрудниками Банка и клиентами в области информационной безопасности, разрабатываются планы, программы обучения и повышения осведомленности в области информационной безопасности. Начальник Службы информационной безопасности формирует свидетельства выполнения программ обучения и повышения осведомленности в области информационной безопасности.

9.14.2. Для сотрудника, получившего новую роль, организовывается обучение или инструктаж по информационной безопасности, соответствующие полученной роли.

9.14.3. Процедуры по обучению и повышению осведомленности регламентируются в соответствующих нормативных документах Банка.

9.15. Обнаружение и реагирование на инциденты информационной безопасности.

9.15.1. В Банке определяются, выполняются, регистрируются и контролируются процедуры обработки инцидентов, а также процедуры хранения и распространения информации об инцидентах информационной безопасности.

9.15.2. До сотрудников Банка доводятся документы, описывающие порядок действий при обнаружении нетипичных событиях, связанных с информационной безопасностью и информировании о данных событиях.

9.15.3. Процедуры расследования инцидентов информационной безопасности учитывают законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов Банка. Решения принимаются по всем выявленным инцидентам информационной безопасности.

10. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

10.1. В основе процессов управления информационной безопасностью лежат следующие требования:

10.1.1. Назначение и определение обязанностей администратора информационной безопасности Банка: администратор информационной безопасности назначается начальник Службы информационной безопасности приказом Председателя Правления Банка, внутренними документами Банка утверждаются цели и задачи его деятельности.

10.1.1.1. Определение области действия системы обеспечения информационной безопасности: в Банке проводится идентификация и классификация объектов информационной инфраструктуры на основании оценок их ценности в соответствии с тяжестью последствий потери свойств информационной безопасности для Банка. Процедуры идентификации, классификации и учета выполняются, регистрируются и контролируется начальником Департамента автоматизации банковских операций.

10.1.2. Выбор подхода к оценке рисков нарушения информационной безопасности.

10.1.2.1. Банком принимается методика оценки рисков нарушения информационной безопасности, определены критерии принятия риска нарушения информационной безопасности и уровень допустимого риска информационной безопасности.

10.1.2.2. Результаты выполнения оценки рисков нарушения информационной безопасности фиксируются перечнем недопустимых рисков нарушения информационной безопасности.

10.1.2.3. Разработка планов обработки рисков нарушения информационной безопасности: планы реализаций требований по обеспечению информационной безопасности, разрабатываемые начальником Службы информационной безопасности, содержат последовательность и сроки реализации и внедрения мер защиты информации для каждого из рисков нарушения информационной безопасности, который является недопустимым.

10.1.3. Разработка внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности: разработка (корректировка) внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности производится с учетом рекомендаций по 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».

10.1.4. Принятие руководством Банка решений о реализации и эксплуатации системы обеспечения информационной безопасности.

10.1.4.1. Решения о реализации и эксплуатации системы обеспечения информационной безопасности, планы внедрения утверждаются Правлением Банка.

10.1.4.2. В Банке фиксируются решения Председателя Правления Банка, связанные с назначением и распределением ролей для всех структурных подразделений.

10.1.4.3. Организация реализации планов обработки рисков нарушения информационной безопасности: в Банке организован постоянный контроль внедрения, эксплуатации, контроля и сопровождения эксплуатации защитных мер, предусмотренных планами реализации требований по обеспечению информационной безопасности.

10.1.5. Мониторинг системы обеспечения информационной безопасности и контроль за функционированием системы обеспечения информационной безопасности (контроль защитных мер), в том числе использование программ аудита.

10.1.5.1. Контроль за функционированием системы обеспечения информационной безопасности (включая контроль параметров конфигурации и настроек средств и механизмов защиты) осуществляется на основании проводимого мониторинга информационной безопасности, анализа функционирования системы обеспечения информационной безопасности, с учетом отчетности и результатов оценки системы обеспечения информационной безопасности.

Основными принципами контроля за функционированием обеспечения информационной безопасности являются: обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль, за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей

Результаты, полученные в ходе контроля путем проведения мониторинга, анализа функционирования системы обеспечения информационной безопасности и с учетом отчетности и результатов оценки системы обеспечения информационной безопасности, являются основой для совершенствования системы обеспечения информационной безопасности.

10.1.5.2. Начальником Службы информационной безопасности осуществляется сбор и хранение информации о действиях сотрудников Банка, событиях и параметрах, имеющих отношение к функционированию защитных мер.

10.1.5.3. Анализ функционирования системы обеспечения информационной безопасности: в Банке определяются, выполняются, регистрируются и контролируются процедуры анализа функционирования системы обеспечения информационной безопасности. При этом анализ функционирования включает в себя:

− анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению информационной безопасности требованиям
законодательства Российской Федерации, требованиям положений Банка России;

− анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению информационной безопасности требованиям положений настоящей Политики;

− оценку рисков в области информационной безопасности;

− проверку адекватности используемых мер защиты информации требованиям внутренних нормативных актов Банка;

− анализ непрерывности в технологических процессах обеспечения информационной безопасности, а также несогласованности в использовании мер защиты информации.

10.1.5.4. Принятие решений по тактическим и стратегическим улучшениям системы обеспечения информационной безопасности: для принятия решений, связанных с улучшениями системы обеспечения информационной безопасности, Банком учитываются результаты:

− аудитов/оценок соответствия информационной безопасности;

− мониторинга информационной безопасности и контроля защитных мер;

− анализа функционирования системы обеспечения информационной безопасности;

− обработки инцидентов информационной безопасности;

− выявления новых угроз и уязвимостей защиты информации;

− оценки рисков информационной безопасности;

− анализа перечня возможных для применения защитных мер;

− анализа успешных практик в области информационной безопасности, а также изменения: в законодательстве Российской Федерации, в нормативных актах Банка России, интересов, целей и задач Банка.

11. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Лицом, ответственным за обеспечение информационной безопасности является Председатель Правления, который осуществляет общее руководство системой обеспечения информационной безопасности в Банке.

11.2. **Председатель Правления** в целях обеспечения информационной безопасности выполняет следующие функции:

− организует процесс управления информационной безопасностью в Банке, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;

− обеспечивает условия и утверждает бюджет для эффективной реализации политики информационной безопасности;

− рассматривает информацию и отчеты о состоянии информационной безопасности Банка.

11.3. **Правление Банка** в целях обеспечения информационной безопасности выполняет следующие функции:

- утверждает Политику информационной безопасности, а также в случае пересмотра Политики.
- распределяет функции и ответственность Правления и работников Банка, в том числе исключающее конфликт интересов в рамках организационной структуры обеспечения информационной безопасности, а также предполагающее определение должностного лица (лица, его замещающего), ответственного за функционирование системы обеспечения информационной безопасности (с прямым подчинением Председателю Правления, или его заместителю) и не участвующего в совершении операций, сделок, организации бухгалтерского и управленческого учета, обеспечении функционирования информационных систем;
- участвует в вопросах развития системы обеспечения информационной безопасности;
- рассматривает отчеты по операционному риску с учетом риска информационной безопасности, предоставляемые Отделом управления рисками;

- участвует в решении вопросов управления операционным риском с учетом риска информационной безопасности Банка.

11.4. **Служба информационной безопасности выполняет следующие функции:**

11.4.1. В целях обеспечения информационной безопасности:

− разрабатывает политику информационной безопасности;

− разрабатывает нормативные, инструктивные и методические документы Банка по обеспечению информационной безопасности;

− разрабатывает требования по защите объектов информационной инфраструктуры в аспектах целостности, конфиденциальности и доступности на основе анализа рисков информационной безопасности;

− осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем от проектирования до снятия с эксплуатации;

− инициирует пересмотр внутренних организационных документов при изменении требований по защите информации, содержащихся в законодательных и нормативноправовых актах;

− обеспечивает управление ключевыми системами средств криптографической защиты информации;

− эксплуатирует специализированные средства обеспечения безопасности объектов информационной инфраструктуры и обеспечивает соответствие характеристик данных средств необходимому подразделениям Банка уровню доступности;

− обеспечивает выполнение и производит периодический контроль выполнения требований эксплуатационной документации на используемые специализированные средства обеспечения безопасности объектов информационной инфраструктуры;

− организует проведение единой антивирусной политики в Банке;

− проводит расследование инцидентов и фактов нарушений информационной безопасности и информирует руководство Банка о результатах проведенного расследования;

− организует обучение сотрудников Банка по вопросам информационной безопасности;

− осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности, информирует Председателя Правления об инцидентах информационной безопасности;

− организует проведение процедуры аудита (оценки соответствия) информационной безопасности в Банке;

− обеспечивает взаимодействие с уполномоченными государственными органами по вопросам лицензирования и сертификации;

− контролирует осуществление сотрудниками Банка мероприятий в области обеспечения информационной безопасности и защиты информации и выполнение других задач, возложенных на них внутренними нормативными документами Банка в области защиты информации;

− осуществляет планирование и контроль процессов обеспечения информационной безопасности в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

− разрабатывает предложения по совершенствованию процессов обеспечения информационной безопасности, в том числе в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

− осуществляет другие функции, связанные с обеспечение информационной безопасности, предусмотренных внутренними нормативными документами Банка.

11.4.2. В целях **управления риском** информационной безопасности:

− соблюдает процедуры управления операционным риском, установленных в подпунктах 2.1.1, 2.1.2. и 2.1.7. Положения Банка России 716-П в части идентификации, сбора и регистрации информации о событиях риска информационной безопасности;

− предоставляет информацию в Отдел управления рисками по событиям риска информационной безопасности для ведения базы событий по событиям операционного риска;

− участвует в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

− оценивает эффективность управления риском информационной безопасности;

− осуществляет мониторинг сигнальных и контрольных значений контрольных показателей уровня риска информационной безопасности;

− участвует в разработке внутренних документов в области управления риском информационной безопасности;

− информирует сотрудников Банка по вопросам, связанным с управлением риском информационной безопасности;

− осуществляет другие функции, связанные с управлением риском информационной безопасности, предусмотренные внутренними документами Банка.

Служба информационной безопасности составляет отчетность:

− отчеты по обеспечению информационной безопасности, включающие информацию о проведенных проверках и оценках в соответствии с п.6., п.7 и п.12 настоящей Политики, а также по событиям риска информационной безопасности, и направляет их Правлению Банка в срок не реже 1 раза в календарный год;

- специализированные отчеты по событиям риска информационной безопасности и направляет их в Отдел управления рисками (ежеквартально). Ответственный сотрудник Отдела управления рисками информирует Правление Банка о сведениях по событиям риска информационной безопасности в составе отчетов по операционному риску.

11.5. **Департамент автоматизации банковских операций**:

− обеспечивает выполнение требований по информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, систем управления базами данных, автоматизированных банковских систем;

− проводит обновление системного программного обеспечения, связанное с устранением критичных уязвимостей;

− обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, систем управления базами данных, автоматизированных банковских систем;

− обеспечивает требования по информационной безопасности при администрировании автоматизированных банковских систем.

11.6. **Подразделения Банка**:

− обеспечивают выполнение требований и процедур по информационной безопасности.

11.7. **Наблюдательный совет Банка**:

− участвует в решении вопросов управления риском информационной безопасности Банка в составе отчетов по управлению операционным риском, предоставляемым Отделом управления рисками.

12. ПРОВЕРКА И ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.1. Проверка и оценка информационной безопасности Банка проводится путем выполнения следующих процессов:

− мониторинга информационной безопасности и контроля защитных мер;

− оценки информационной безопасности;

− аудита информационной безопасности;

− анализа функционирования системы обеспечения информационной безопасности (в том числе со стороны руководства Банка).

12.2. Основными целями мониторинга информационной безопасности и контроля защитных мер являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели:

− контроль за реализацией положений внутренних документов по обеспечению информационной безопасности;

− выявление нештатных, в том числе злоумышленных действий в автоматизированной банковской системе;

− выявление инцидентов информационной безопасности.

12.3. Мониторинг и контроль защитных мер проводится сотрудниками Банка, ответственными за обеспечение информационной безопасности.

12.4. Основные цели проведения внутренних проверок системы обеспечения информационной безопасности:

– оценка текущего уровня защищённости информационной инфраструктуры;

– выявление и локализация уязвимостей в системе защиты;

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении объектов информационной инфраструктуры;

– оценка соответствия требованиям настоящей Политики;

– выработка рекомендаций по совершенствованию системы обеспечения информационной безопасности за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

12.5. Аудит информационной безопасности проводится с целью проверки выполнения требований по информационной безопасности нормативных актов Банка России, либо с целью проверки обоснованности и защищенности применяемых решений.

12.6. Аудит информационной безопасности – внешняя оценка выполнения требований к обеспечению защиты информации – осуществляющиеся один раз в два года, а также по требованию Банка России, с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации № 79 (далее – оценка соответствия).

12.7. Оценка соответствия осуществляется на основе:

– информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;

– анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям положений Банка России;

– результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации.

12.8. Банком в обязательном порядке обеспечивается проведение следующих оценок:

– оценка выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств осуществляется в соответствии с порядком, установленным в п.1.1 Положения Банка России № 719-П (ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры, оценка соответствия защиты информации);

– оценка выполнения требований, установленных в подпункте 3.2 пункта 3 и п.9 Положения Банка России № 683-П); (ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры и оценка соответствия уровню защиты информации);

– оценка соответствия в пределах выделенных сегментов вычислительной сети требований к защите информации в платежной системе Банка России проводится в соответствии с положениями ГОСТ Р 57580 (Положение Банка России № 747-П) .

Оценка соответствия защиты информации осуществляется в соответствии с национальным стандартом ГОСТ Р 57580 не реже одного раза в два года (п.1 Положения Банка России № 719-П, п.9 Положения Банка России № 683-П, п.19 Положение Банка России № 747-П).

12.9. Анализ функционирования системы обеспечения информационной безопасности проводится сотрудниками Банка, ответственными за обеспечение информационной безопасности, а также руководством Банка, в том числе на основании подготовленных для руководства документов (данных).

12.10. В число задач, решаемых при проведении проверок и аудитов информационной безопасности входят:

– сбор и анализ исходных данных об информационной инфраструктуре, необходимых для оценки состояния информационной безопасности;

– анализ существующей политики информационной безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);

– технико-экономическое обоснование мер защиты информации;

– проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности информационной инфраструктуры;

– разбор инцидентов информационной безопасности и минимизация возможного ущерба от их появления.

13. ОТВЕТСТВЕННОСТЬ ЗА НЕВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13.1. По степени опасности нарушения, связанные с несоблюдением локальных нормативных актов по обеспечению информационной безопасности Банка, делятся на две группы:

− нарушения, повлекшие за собой наступление нежелательных для Банка последствий (утечку или уничтожение информации).

− нарушения, в результате которых созданы предпосылки, способные привести к нежелательным для Банка последствиям (угроза уничтожения или утраты информации).

13.2. Нарушение требований локальных нормативных актов Банка по обеспечению информационной безопасности является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между Банком и сотрудниками и договорами, заключенными между Банком и контрагентами.

13.3. Степень ответственности за нарушение требований локальных нормативных актов в области информационной безопасности определяется исходя из размера ущерба, причиненного Банку.

13.4. Правление Банка несет ответственность за соблюдение требований положений настоящей Политики.

13.5. Руководители структурных подразделений Банка несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.

13.6. Каждый сотрудник Банка несет персональную ответственность за обеспечение информационной безопасности на своем рабочем месте.

13.7. Виды ответственности, предусмотренные отдельными федеральными законами об обращении с информацией ограниченного доступа:

– гражданско-правовая ответственность;

– дисциплинарная ответственность;

– уголовная ответственность;

– административная ответственность.

14. РЕАЛИЗАЦИЯ, КОНТРОЛЬ, ПЕРЕСМОТР НАСТОЯЩЕЙ ПОЛИТИКИ

14.1. За реализацию положений настоящей Политики и поддержание ее в актуальном состоянии отвечает начальник Службы информационной безопасности. Контроль за реализацией положений настоящей Политики и поддержанием её в актуальном состоянии возлагается на куратора информационной безопасности.

14.2. Для обеспечения актуальности настоящей Политики Служба информационной безопасности не реже 1 раза в год проводит анализ необходимости пересмотра требований настоящего Политики с учетом:

– обнаружения инцидентов информационной безопасности;

– обнаружения недостатков в рамках контроля системы защиты информации;

– изменения политики Банка в отношении:

• области применения системы обеспечения информационной безопасности;

• основных принципов и приоритетов в реализации системы обеспечения информационной безопасности: целевых показателей величины допустимого остаточного операционного риска, связанного с обеспечением информационной безопасности;

– изменения требований законодательства Российской Федерации, нормативно- правовых актов и методических документов Банка России, ФСБ России, ФСТЭК России, ФСФР и Роскомнадзора;

– пересмотра области применения процесса системы защиты информации: пересмотра состава и содержания организационных и технических мер защиты информации, применяемых в рамках системы обеспечения информационной безопасности;

– необходимости пересмотра на основе результатов оценки рисков информационной безопасности;

– изменения в составе основных объектов информационной инфраструктуры, которые могут повлиять на состав угроз безопасности информации. К таким элементам относятся:

• информационные технологии как совокупность приемов, способов и методов применения средств вычислительной техники при обработке защищаемых информационных активов;

- технические средства, осуществляющие обработку защищаемых информационных активов (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки защищаемых информационных активов, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов, другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации);
- программные средства (операционные системы, системы управления данными и т.п.);
- средства защиты информации;
- вспомогательные технические средства и системы.

15. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

15.1. Настоящая Политика является общедоступным документов для всех сотрудников, клиентов и контрагентов Банка.

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

15.3. 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.

ЛИСТ СОГЛАСОВАНИЯ

Стратегия управления рисками и капиталом
Коммерческий Банк «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью)

Должность	Ф.И.О.	Подпись
Зам. Председателя Правления	Суханова Е.В.	
Главный бухгалтер	Медникова Н.В.	
Начальник Юридического департамента	Скоринов Е.В.	
Начальник Отдела управления рисками	Машкова И.В.	
Начальник Службы информационной безопасности	Чуманов В.П.	