УТВЕРЖДЕНО
Решением Совета директоров
АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ»
Протокол заседания Совета директоров
от 27 августа 2025 г.№ 27/08/2025-1 СД

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ»

МОСКВА
2025

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ» (далее – Политика) определяет высокоуровневые цели и задачи обеспечения информационной безопасности АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ» (далее – РНКО), включая способы контроля реализации требований политики информационной безопасности, а также определяет содержание, назначение и требования к деятельности РНКО по обеспечению информационной безопасности.

1.2. Настоящая Политика устанавливает принципы построения системы управления информационной безопасностью РНКО на основе систематизированного изложения целей, процессов и процедур информационной безопасности РНКО, обеспечивая их конфиденциальность, целостность и доступность.

1.3. Требования информационной безопасности предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.4. Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации и ключевыми отраслевыми стандартами в области информационной безопасности:

– Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», введенным в действие Распоряжением РНКО России от 17.05.2014 № Р-399;

– Стандартом РНКО России РС БР ИББС-2.0-2007 «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», введенным в действие Распоряжением РНКО России от 28.04.2007 № Р-348;

– Национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», введенным в действие Приказом Росстандарта от 08.08.2017 № 822-ст;

– Национальным стандартом Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения», введенным в действие Приказом Росстандарта от 22.12.2022 № 1548-ст;

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности»;

– Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Федеральным законом от 27.07. 2006 № 152-ФЗ "О персональных данных";

– Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Положением Банка России от 17.08.2023 № 821-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» (далее – Положение №821-П);

– Положением Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России»;

– Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее – Положение № 716-П);

– Положением Банка России от 30 января 2025 г. № 851-П "Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" (далее – Положение № 851-П);

– «Условия по защите информации», утвержденные Банком России и применяемые при обмене финансовыми сообщениями в системе передачи финансовых сообщений (СПФС);

– другими нормативными и правовыми актами.

1.5. Настоящая Политика распространяется на все структурные подразделения РНКО и обязательна для применения всеми работниками и руководством РНКО, а также пользователями его информационных ресурсов.

Политика распространяется на все информационные ресурсы РНКО, а также на бизнес-процессы, в рамках которых осуществляется их совместное использование. Положения Политики также могут распространяться на подрядные организации и партнеров в рамках договорных обязательств при их взаимодействии с информационными активами РНКО.

1.6. Требования настоящей Политики могут развиваться другими внутренними нормативными документами РНКО, которые дополняют и уточняют её.

1.7. В случае изменения действующего законодательства и иных нормативны актов Российской Федерации настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Служба информационной безопасности инициирует внесение соответствующих изменений.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационный актив (ИА) – информация (в электронном виде, на материальных носителях) с реквизитами, позволяющими ее идентифицировать, и имеющая ценность для достижения поставленных перед РНКО или его подразделениями целей. Основными характеристиками информационных активов, рассматриваемых в рамках обеспечения информационной безопасности, являются конфиденциальность, целостность и доступность.

Информационная безопасность (ИБ) – состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.
Безопасность информации определяется отсутствием недопустимого риска, связанного с несанкционированными и непреднамеренными воздействиями на информацию и (или) на другие ресурсы и информационной системы, используемые в РНКО.

Информационная система – совокупность программно-аппаратных комплексов РНКО, применяемых для обеспечения бизнес-процессов РНКО.

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

- нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности РНКО;
- нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних нормативных документов РНКО в области обеспечения информационной безопасности, нарушение или возможное нарушение в выполнении процессов системы обеспечения информационной безопасности РНКО;

– нарушение или возможное нарушение в выполнении технологических и бизнес-процессов процессов РНКО.

Инциденты защиты информации - инциденты, приведшие к фактической реализации риска информационной безопасности, в том числе киберриска, обусловленные источниками риска информационной безопасности, в том числе инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных в соответствии с Положением № 821-П и Положением № 851-П;

События риска информационной безопасности (далее – СОИБ) - инциденты защиты информации, вследствие которых возникли прямые и (или) непрямые потери РНКО, в базе событий операционного риска;

Киберриск - риск преднамеренных действий со стороны работников РНКО и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры РНКО в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими 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;

Конфиденциальная информация – информация с ограниченным доступом, в отношении которой РНКО установлен режим конфиденциальности.

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

Модель нарушителя – 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.

Пользователь информационной системы – физическое лицо, обладающее возможностью доступа к информационной системе РНКО.

Риск информационной безопасности - риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности кредитной организации. Риск информационной безопасности включает в себя:

- киберриск;
- другие виды риска информационной безопасности, связанных с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры.

Угроза информационной безопасности – угроза нарушения свойств информационной безопасности: доступности, целостности или конфиденциальности информационных активов РНКО, приводящая к возможности возникновения потерь (ущерба).

3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

3.1. Основными объектами защиты системы информационной безопасности в РНКО являются информационные ресурсы, содержащие:

– коммерческую тайну;
– банковскую тайну;

- персональные данные физических лиц (работников и клиентов);
- сведения ограниченного доступа;
- открыто распространяемую информацию, необходимую для работы РНКО, независимо от формы и вида ее представления.

3.2. Особые объекты защиты, имеющие высокую важность для РНКО:

- платежный технологический процесс;
- информационный технологический процесс;
- платежная информация;
- информация, отнесенная к защищаемой в соответствии с Положением Банка России от 17.08.2023 № 821-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 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России»;
- иная значимая для РНКО информация, разглашение или модификация которой может привести к негативным последствиям для РНКО;
- носители защищаемой информации, в т. ч. информационные ресурсы, речевая информация, документы на физических носителях информации, определенные как защищаемые нормативно-распорядительными документами РНКО.

4. ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Целью деятельности по обеспечению информационной безопасности РНКО является защита информационных активов РНКО, обеспечение их целостности, доступности и конфиденциальности, снижение уровня угроз информационной безопасности до приемлемого для РНКО значения.

4.2. Основные задачи деятельности по обеспечению информационной безопасности РНКО:

- организация выполнения требований законодательства Российской Федерации, нормативных актов Банка России и иных государственных органов в области информационной безопасности, внутренних нормативных документов РНКО по обеспечению информационной безопасности, в том числе по защите персональных данных, включая контроль реализации данных требований;
- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- исключение либо минимизация выявленных угроз;
- повышение уровня информационной безопасности РНКО;
- разработка и поддержание в актуальном состоянии нормативных документов РНКО в области информационной безопасности;
- предотвращение инцидентов информационной безопасности и минимизация возможного ущерба от инцидентов;
- внедрение, поддержка и при необходимости восстановление систем защиты информации;
- участие в расследованиях инцидентов информационной безопасности;
- участие и осуществление контроля выполнения требований информационной безопасности в ИТ-проектах РНКО;
- согласование и контроль предоставления доступа к информационным активам РНКО.

4.3. При обеспечении информационной безопасности РНКО руководствуется следующими принципами:

- системность – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности;
- комплексность – согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;
- непрерывность защиты – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем;
- своевременность – упреждающий характер мер обеспечения безопасности информации;
- преемственность и непрерывность совершенствования - постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и их систем защиты;
- разумная достаточность – соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения;
- персональная ответственность – возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий;
- разделение функций – отсутствие полномочий, позволяющих работнику РНКО единолично осуществлять выполнение критичных операций;
- минимизация полномочий – предоставление пользователям минимально возможных прав доступа в соответствии с должностными обязанностями, либо в соответствии с условиями договора, соглашения;
- гибкость системы защиты – возможность варьирования уровнем защищенности. Это свойство является важным для случаев, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования;
- эффективность применения средств защиты – затраты на внедрение и эксплуатацию механизмов защиты соизмеримы с возможным ущербом;
- специализация и профессионализм – привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области;
- осведомленность – все сотрудники РНКО должны быть информированы о требованиях по информационной безопасности, проходить регулярное обучение и аттестацию по вопросам информационной безопасности, создавать культуру безопасности.
- контроль – обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе проверок и экспертиз используемых систем и средств защиты информации, бизнес-процессов и деятельности работников РНКО.

5. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Источники угроз, уязвимости, используемые угрозами, методы и объекты атак, пригодные для реализации угрозы, а также описание потенциальных нарушителей определяются внутренним нормативным документом РНКО, регламентирующим построение моделей угроз и потенциального нарушителя информационных ресурсов.

5.2. Модель угроз содержит систематизированный перечень категорий защищаемой информации, источников актуальных угроз ИБ, уровней реализации угроз и объектов среды ИА, а также свойств ИБ, на которые направлена угроза.

5.3. Модель нарушителя содержит типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации, цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации, и возможные способы реализации угроз безопасности информации.

6. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

6.2. В РНКО в целях управления риском ИБ определено специализированное подразделение – Служба информационной безопасности с прямым подчинением Председателю Правления РНКО, ответственное за обеспечение ИБ и не участвующее в обеспечении функционирования информационных систем РНКО.

6.3. РНКО классифицирует события риска ИБ по источникам операционного риска в соответствии с классификатором (Далее – Классификатор СОР), приведенным в Приложении 2 к Порядку взаимодействия подразделений в целях учета событий операционного риска в АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ», а также по уязвимостям информационных систем и их компонентов, обусловленным недостатками процессов обеспечения защиты информации, способствующими реализации угрозы безопасности информации (совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации).

6.4. Риск ИБ является видом операционного риска, поэтому все события риска информационной безопасности с прямыми потерями в обязательном порядке заносятся в Базу событий операционного риска (далее – База СОР), порядок ведения которой описан в Порядке взаимодействия подразделений в целях учета событий операционного риска в АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ». В случае если РНКО ведет отдельную базу событий риска информационной безопасности, ответственный работник Службы информационной безопасности соблюдает все требования к ведению Базы СОР.

6.5. РНКО обеспечивает выявление, регистрацию и учет всех событий риска информационной безопасности с определением всех элементов классификации в соответствии Классификатором СОР, определяет суммы потерь в разрезе видов потерь с распределением по датам отражения в бухгалтерском учете, с раздельным учетом поступивших возмещений. В случае выявления событий риска информационной безопасности, связанных с не контролируемым РНКО распространением сведений, составляющих банковскую тайну, РНКО обеспечивает их регистрацию в базе СОР, включая описание указанных событий риска информационной безопасности.

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

- степени возможности реализации угроз безопасности информации выявленными и (или) предполагаемыми источниками угроз безопасности информации в результате их воздействия на информационные активы РНКО;
- степени тяжести последствий от потери свойств информационной безопасности для рассматриваемых типов информационных активов.

6.7. В целях эффективности управления риском ИБ в РНКО осуществляются следующие мероприятия:

- обеспечение выполнения порядка функционирования системы информационной безопасности, определенного внутренними нормативными документами РНКО, с

учетом требований Положения № 716-П (идентификации, сбора и регистрации информации о событиях риска ИБ и потерях, мониторинга риска ИБ);

- распределение функций и ответственности Правления РНКО (коллегиального исполнительного органа) и работников РНКО в части решения вопросов, связанных с управлением риском реализации информационных угроз, обеспечением операционной надежности и защиты информации, в том числе исключающее конфликт интересов;
- определение основных принципов функционирования системы обеспечения информационной безопасности и задачи управления риском ИБ;
- определение и поддержание допустимого уровня риска ИБ, разработка мероприятий, направленных на уменьшение негативного влияния риска ИБ.

6.8. Методами управления риском ИБ, с учетом требований Положения об управлении операционным риском в АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ», являются:

- применение защитных мер, позволяющих снизить величину риска ИБ до допустимого уровня;
- уход от риска ИБ (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);
- перенос риска ИБ на другие организации (например, путем страхования или передачи деятельности на аутсорсинг);
- осознанное принятие риска ИБ.

7. ФУНКЦИИ И ОТВЕТСТВЕННОСТЬ ПРАВЛЕНИЯ И РАБОТНИКОВ РНКО В РАМКАХ УПРАВЛЕНИЯ РИСКОМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. К компетенции Правления РНКО относятся следующие вопросы:

- обеспечение принятия внутренних нормативных документов, определяющих правила и процедуры управления риском ИБ;
- распределение полномочий и ответственности по управлению риском ИБ между руководителями подразделений, установление порядка взаимодействия и представления отчетности;
- определение потребности РНКО в ресурсах для обеспечения информационной безопасности РНКО и организация ресурсного (кадрового и финансового) обеспечения процессов системы управления риском ИБ;
- определение комплекса мероприятий, направленных на повышение качества системы управления риском ИБ и уменьшение негативного влияния риска ИБ;
- осуществление контроля за реализацией политики управления риском ИБ и соблюдения установленных значений сигнальных и контрольных значений контрольных показателей уровня риска ИБ.

7.2. На Службу информационной безопасности с учетом требований Положения № 716-П возложено выполнение следующих функций:

- соблюдение процедур управления риском ИБ в части идентификации, сбора и регистрации информации о событиях риска ИБ и потерях от риска ИБ;
- ведение базы событий риска ИБ;
- участие в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском ИБ и уменьшение негативного влияния риска ИБ;
- составление на регулярной основе отчетов по событиям риска ИБ и направление их Председателю Правления РНКО (ежеквартально) и в Службу управления рисками (ежемесячно не позднее 5го рабочего дня месяца, следующего за отчетным) для включения в отчеты ВПОДК для Совета директоров и Правления РНКО;
- разработка внутренних нормативных документов в области управления риском ИБ;

- информирование работников РНКО по вопросам, связанным с управлением риском ИБ.

8. ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ КОНТРОЛЯ ЗА ФУНКЦИОНИРОВАНИЕМ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Анализ функционирования СОИБ проводится ответственным работником **Службы информационной безопасности,** а также Правлением РНКО.

8.2. Основными целями проведения анализа функционирования СОИБ являются:

- оценка эффективности СОИБ;
- оценка соответствия СОИБ требованиям международного законодательства, законодательства РФ и требований Банка России;
- оценка соответствия СОИБ существующим и возможным угрозам информационной безопасности;
- оценка следования принципам информационной безопасности и выполнения требований по обеспечению информационной безопасности, закрепленным в Политике информационной безопасности, а также в иных внутренних документах РНКО.

Результаты, полученные в ходе анализа функционирования СОИБ, являются основой для совершенствования СОИБ.

8.3. Цели обработки рисков ИБ:

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

8.4. Управление рисками ИБ предполагает решение следующих задач:

- построение модели взаимодействия бизнес-процессов РНКО и информационных систем с целью выделения наиболее критичных ИА РНКО;
- построение модели нарушителя ИБ и модели угроз ИБ;
- оценка рисков реализации угроз ИБ, направленных на критичные ИА РНКО;
- выявление мер по снижению рисков угроз ИБ;
- разработка плана по снижению рисков ИБ;

8.5. Требования к анализу функционирования СОИБ:

8.5.1. Процедуры анализа функционирования СОИБ должны быть определены, выполняться, регистрироваться и контролироваться, к ним относятся:

- результаты мониторинга ИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудиторской проверки ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри РНКО (например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах);
- данные об изменениях вне РНКО (например, данные об изменениях в законодательстве РФ, изменениях в договорных обязательствах).

8.5.2. Анализ функционирования СОИБ должен включать в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению информационной безопасности в РНКО, требованиям законодательства РФ, требования международного законодательства, отраслевым стандартам, контрактным требованиям организации и т.д.;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ а РНКО, требованиям Политики информационной безопасности РНКО;
- оценку рисков в области ИБ, включая оценку уровня остаточного и допустимого риска, а также оценку адекватности модели угроз РНКО существующим угрозам информационной безопасности;

- проверку адекватности используемых мер защиты требованиям внутренних документов РНКО и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании мер защиты.

8.5.3. Анализ и оценка рисков ИБ основывается на:

- идентификации автоматизированных систем РНКО;
- идентификации информационных активов РНКО;
- ценности информационных активов для целей и задач РНКО;
- моделях угроз и нарушителей ИБ РНКО.

Требования к анализу СОИБ со стороны Правления:

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

- отчеты с результатами анализа функционирования СОИБ;
- отчеты с результатами аудитов информационной безопасности;
- документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
- документы, содержащие информацию о новых, выявленных уязвимостях и угрозах информационной безопасности;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ (например, изменения в законодательстве РФ);
- документы, содержащие информацию по выявленным инцидентам информационной безопасности;
- документы, подтверждающие выполнение требуемой деятельности по обеспечению информационной безопасности, например, выполнение планов обработки рисков;
- документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

9. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. Система менеджмента информационной безопасности РНКО основывается на осуществлении следующих основных процессов: планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование, соответствующих требованиям положениям международных стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла «планирование – реализация – проверка – совершенствование – планирование…», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности РНКО и повышение ее эффективности.

9.2. При планировании мероприятий по обеспечению информационной безопасности в РНКО осуществляется:

- определение и распределение ролей персонала РНКО, связанного с обеспечением информационной безопасности;
- оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности;
- выявление потенциальных угроз информационной безопасности, анализ причин их возникновения и прогнозирования их развития;
- построение моделей угроз и нарушителей информационной безопасности;
- оценка рисков информационной безопасности;

- рассмотрение и оценка различных вариантов решения задач по обеспечению информационной безопасности;
- поддержка в актуальном состоянии нормативно-методического обеспечения деятельности в сфере информационной безопасности.

9.3. В рамках реализации деятельности по обеспечению информационной безопасности в РНКО осуществляется:

- сбор информации о событиях информационной безопасности;
- выявление инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства РНКО информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним;
- повышение уровня знаний работников РНКО в вопросах обеспечения информационной безопасности;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения РНКО.

9.4. В целях проверки деятельности по обеспечению информационной безопасности в РНКО осуществляются;

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигураций систем и подсистем РНКО;
- контроль реализации и исполнения требований работниками РНКО действующих внутренних нормативных документов по обеспечению информационной безопасности РНКО;
- расследование и анализ инцидентов информационной безопасности.

9.5. В целях совершенствования деятельности по обеспечению информационной безопасности в РНКО осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности.

9.6. Политика информационной безопасности должна быть пересмотрена в следующих случаях:

- внесения изменений в законодательные акты РФ и нормативные акты РНКО России в области обеспечения информационной безопасности;
- изменения ключевых требований к защите информации;
- выявления недостатков настоящей Политики;
- принятия решения об улучшении системы ИБ.

10. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. В целях выполнения задач по обеспечению информационной безопасности РНКО, в РНКО определены следующие роли:

- ответственное подразделение (Служба информационной безопасности);
- работник РНКО.

10.2. Общее руководство обеспечением информационной безопасности РНКО осуществляет руководитель ответственного подразделения.

10.3. Основными функциями руководителя ответственного подразделения в вопросах информационной безопасности являются:

- согласование назначения ответственных лиц в области информационной безопасности;
- организация и контроль деятельности Службы информационной безопасности в РНКО.

10.4. Текущая деятельность и планирование деятельности по обеспечению информационной безопасности РНКО осуществляются и координируются Службой информационной безопасности.

10.5. РНКО при организации ресурсного (кадрового и финансового) обеспечения Службы информационной безопасности определяется минимально необходимая и достаточная численность работников Службы информационной безопасности, исходя из следующих показателей:

- уровень автоматизации процессов обеспечения операционной надежности и защиты информации;
- трудозатраты на выполнение задачи и функций обеспечения информационной безопасности;
- количество реализуемых процессов системы обеспечения информационной безопасности;
- масштаб выполнения управляемых процессов системы обеспечения информационной безопасности;
- прогноз возможного расширения состава задач и функций, возложенных на работников Службы информационной безопасности, в результате развития бизнес- и технологических процессов РНКО.

10.6. Работники Службы 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 области ИБ.

10.7. Состав задач, функции и требования, предъявляемые РНКО к работникам Службы информационной безопасности, определены в Положении о Службе информационной безопасности АО РНКО «ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ» и в должностных инструкциях указанных работников.

10.8. Основными задачами работников РНКО в рамках их участия в деятельности по обеспечению информационной безопасности РНКО являются:

- соблюдение требований информационной безопасности, установленных действующим законодательством, нормативными актами Российской Федерации и внутренними нормативными документами РНКО;
- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
- выявление и реагирование на инциденты информационной безопасности;
- информирование своего руководителя и Службы информационной безопасности о выявленной угрозе в информационной среде РНКО.

11. ТРЕБОВАНИЯ К СОЗДАНИЮ РЕСУРСНЫХ (КАДРОВЫХ И ФИНАНСОВЫХ) УСЛОВИЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Под ресурсным обеспечением информационной безопасности понимается процесс управления, обеспечивающий определение потребностей в ресурсах информационной безопасности и контроль эффективности использования ресурсов ИБ.

11.2. Основными целями реализации ресурсного обеспечения ИБ являются:

- обеспечение процессов системы ИБ финансовыми средствами;
- обеспечение РНКО кадровыми ресурсами, необходимыми и достаточными для реализации процессов системы обеспечения информационной безопасности;
- контроль эффективности использования ресурсов ИБ.

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

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

11.5. Определение потребности РНКО в кадровых ресурсах заключается в установлении необходимого и достаточного количества, а также требуемой компетенции работников, ответственных за обеспечение ИБ, выполняемой на основе:

- анализа задач и функций, возложенных на указанных работников;
- уровня автоматизации процессов СОИБ и централизации управления средствами автоматизации;
- прогноза возможного расширения состава задач и функций указанных работников в соответствии с планами совершенствования процессов СОИБ вследствие развития бизнес- процессов, совершенствования процессов информатизации, развития филиальной сети РНКО.

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

11.6. Основные внутренние нормативные документы РНКО в области информационной безопасности регламентируют:

- требования по обеспечению защиты информации, применяемой на стадиях жизненного цикла автоматизированных систем во время проектирования, разработки, тестирования, внедрения, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;
- требования по обеспечению защиты информации, применяемой при осуществлении доступа к объектам информационной инфраструктуры;
- требования по обеспечению защиты вычислительных сетей;
- требования по обеспечению контроля целостности и защищенности информационной инфраструктуры;
- требования по обеспечению защиты от утечек информации;
- требования к парольной защите;
- требования по обеспечению защиты информации, применяемой от воздействия вредоносного кода, приводящих к нарушению штатного функционирования средств вычислительной техники;
- требования по обеспечению защиты информации, применяемой при использовании информационно-телекоммуникационной сети Интернет;
- требования по обеспечению защиты информации, применяемой при использовании корпоративной электронной почты;
- требования к повышению осведомленности работников РНКО в области обеспечения защиты информации;
- требования по управлению инцидентами информационной безопасности и их обработку;
- требования по инвентаризации и классификации активов в РНКО;
- требования к обеспечению защиты информации, применяемые для защиты информации при использовании средств криптографической защиты информации;
- требования по обращению и хранению носителей ключевой информации;
- требования к обеспечению защиты информации на участке платежной системы Банка России;

- требования к разработке модели угроз и модели нарушителя информационной безопасности, а также разработке методики оценки рисков нарушения информационной безопасности;
- требования по защите при использовании технологии виртуализации;
- требования к порядку проверки усиленной квалифицированной электронной подписи и хранению электронных документов, подписанных усиленной квалифицированной электронной подписью;
- требования к порядку взаимодействия подразделений информационных технологий и Службы информационной безопасности;
- требования к условиям осуществления обмена электронными сообщениями (далее – ЭС) и (или) пакетами ЭС при взаимодействии между РНКО и Центральным Банком Российской Федерации;
- требования по определению перечня персональных данных, обрабатываемых РНКО, целей, принципов, сроков и способы такой обработки, порядок передачи, хранения и удаления персональных данных, ответственность на нарушение норм, регулирующих обработку персональных данных, а также другие требования, определенные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

12. ОТВЕТСТВЕННОСТЬ И КОНТРОЛЬ

12.1. Ответственность за поддержание положений настоящей Политики и внутренних нормативных документов РНКО в области ИБ в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы обеспечения информационной безопасности лежит на Службе информационной безопасности.

12.2. Ответственность работников РНКО за неисполнение настоящей Политики и внутренних нормативных документов РНКО в области ИБ определяется соответствующими положениями, включаемыми в договоры с работниками РНКО, а также положениями внутренних нормативных документов РНКО.

12.3. Общий контроль состояния информационной безопасности РНКО осуществляет Председатель Правления.

12.4. Текущий контроль соблюдения требований настоящей Политики осуществляет Служба информационной безопасности. Контроль осуществляется посредством проведения мониторинга и менеджмента инцидентов информационной безопасности РНКО, по результатам оценки информационной безопасности РНКО, а также в рамках иных контрольных мероприятий.

12.5. Подразделения РНКО, ответственные за организацию внутреннего контроля и аудита осуществляет контроль соблюдения настоящей Политики на основе проведения внутренних проверок информационной безопасности.

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1. Настоящая Политика вступает в силу с момента ее утверждения Правлением РНКО и действует до момента отмены или принятия нового документа.

13.2. Если при изменении законодательства Российской Федерации отдельные пункты Политики вступают в противоречие с ним, то эти пункты утрачивают силу, и до момента внесения изменений в документ работники РНКО руководствуются действующим законодательством Российской Федерации, при этом факт прекращения действия одного или нескольких пунктов не влияет на действие Политики в целом.

13.3. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте РНКО в информационно-телекоммуникационной сети «Интернет» по адресу: https://paymenttechno.com/