|  |  |
| --- | --- |
|  | **УТВЕРЖДЕНА**  Правлением АО «Urfu Bank» Протокол № 32232 от 26.05.2023 г. |

ПОЛИТИКА

# ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «Urfu Bank»

**Екатеринбург 2023**

# ОГЛАВЛЕНИЕ

Оглавление

[1. ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc136371051)

[2. ОБЛАСТЬ ПРИМЕНЕНИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 4](#_Toc136371052)

[3. ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ 6](#_Toc136371053)

[4. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 6](#_Toc136371054)

[5. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ **Ошибка! Закладка не определена.**](#_Toc136371055)

[6. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 9](#_Toc136371056)

[7. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 11](#_Toc136371057)

[8. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 14](#_Toc136371058)

[9. РЕАЛИЗАЦИЯ, КОНТРОЛЬ, ПЕРЕСМОТР НАСТОЯЩЕЙ ПОЛИТИКИ 14](#_Toc136371059)

[10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 15](#_Toc136371060)

# ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Политика информационной безопасности АО «URFU BANK» (далее – Политика) разработана в соответствии с требованиями законодательства Российской Федерации и нормативных документов Банка России.
  2. Настоящая Политика устанавливает принципы построения системы управления информационной безопасностью АО «URFU BANK» (далее – Банк) на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.
  3. Требования информационной безопасности предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.
  4. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна для применения всеми сотрудниками и руководством Банка, а также пользователями его информационных ресурсов.
  5. Требования настоящей Политики могут развиваться другими внутренними нормативными документами Банка, которые дополняют и уточняют ее.
  6. В случае изменения действующего законодательства и иных нормативны актов настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае отдел информационной безопасности инициирует внесение соответствующих изменений.
  7. 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 09.06.2012 г. № 382-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 09.01.2019 г. № 672-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 9 организаций. Базовый состав организационных и технических мер».  
  
 **1.8.** 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).

**1.9.** 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 10 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.

# 2. ОБЛАСТЬ ПРИМЕНЕНИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

**2.2.** 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, самооценки) 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;

Настоящая Политика не распространяется на организацию и порядок защиты информации, составляющей государственную тайну.

# 3. ПЕРИОД ДЕЙСТВИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

Настоящая Политика является локальным нормативным документом постоянного действия.

Настоящая Политика утверждается, изменяется и признается утратившей силу в АО «Urfu Bank» решением Совета директоров АО «Urfu Bank» и вводится в действие в АО «Urfu Bank» приказом АО «Urfu Bank».

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

|  |  |
| --- | --- |
| ***АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ (АСУ)*** | Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами. |
| ***КОМПЬЮТЕРНАЯ АТАКА*** | Действия, направленные на реализацию угроз несанкционированного доступа к ИТ-активу, воздействия на него или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств. |
| ***ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*** | Состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Компании. |
| ***ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (ИТ- ИНФРАСТРУКТУРА)*** | Совокупность компонентов информационных технологий, в том числе аппаратное (системы обработки и хранения данных, оборудование рабочего места, периферия и т.д.), системное программное и инженерное обеспечение, сети, специализированные помещения. |
| ***ИНФОРМАЦИОННАЯ СИСТЕМА (ИС)*** | Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. |
| ***ИНФОРМАЦИОННАЯ СРЕДА*** | Совокупность разной информации вместе с ИТ- инфраструктурой, а также субъектами, которые занимаются сбором, использованием и распространением информации. |
| ***ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКА- ЦИОННАЯ СЕТЬ*** | Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. |
| ***ИНФОРМАЦИЯ*** | Сведения (сообщения, данные) независимо от формы их представления. |
| ***ИТ-АКТИВ*** | Идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Компании. |
| ***ИТ-ПРОСТРАНСТВО*** | Совокупность объектов (информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура), вступающих друг с другом в информационное взаимодействие, а также сами информационные технологии, обеспечивающие данное взаимодействие. |
| ***КОМПАНИЯ*** | Группа юридических лиц различных организационно-правовых форм, включая ПАО «НК «Роснефть», в отношении которых последнее выступает в качестве основного или преобладающего (участвующего) общества. |

|  |  |
| --- | --- |
| ***МОБИЛЬНОЕ ТЕХНИЧЕСКОЕ СРЕДСТВО*** | Съемные машинные носители информации, портативные вычислительные устройства и устройства связи с возможностью обработки информации (переносные персональные компьютеры  - ноутбуки, нетбуки, планшетные компьютеры, а также мобильные телефоны, смартфоны, умные часы/браслеты, цифровые камеры, звукозаписывающие устройства и иные средства). |
| ***ОБЩЕСТВО ГРУППЫ (ОГ)*** | Хозяйственное общество, прямая и (или) косвенная доля владения ПАО «НК «Роснефть» акциями или долями в уставном капитале которого составляет 20 процентов и более. |
| ***ПОДКОНТРОЛЬНОЕ ПАО «НК «РОСНЕФТЬ» ОБЩЕСТВО ГРУППЫ*** | Общество Группы, в котором ПАО «НК «Роснефть» имеет право прямо и/или косвенно (через подконтрольных ему лиц) распоряжаться в силу участия в таком Обществе Группы и (или) на основании договоров доверительного управления имуществом, и (или) простого товарищества, и (или) поручения, и (или) акционерного соглашения, и (или) иного соглашения, предметом которого является осуществление прав, удостоверенных акциями (долями) такого Общества Группы, более 50 процентами голосов в высшем органе управления, либо назначать (избирать) единоличный исполнительный орган и/или более 50 процентов состава коллегиального органа управления. |
| ***ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ*** | Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ. |
| ***ПРОИЗВОДСТВЕННАЯ СИСТЕМА*** | Совокупность компонентов информационных технологий, обеспечивающих автоматизацию решения задач планирования и управления различными видами производственной деятельности и производственных процессов. |
| ***РИСК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ- РИСК)*** | Сочетание вероятности реализации угрозы информационной безопасности и последствий её реализации, оказывающих негативное влияние на достижение целей Компании. |
| ***СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ*** | Структурное подразделение ПАО НК «Роснефть» или Общества Группы с самостоятельными функциями, задачами и ответственностью в рамках своих компетенций, определенных в Положении о структурном подразделении. |
| ***УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***  ***(УГРОЗА)*** | Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива. |
| ***УЯЗВИМОСТЬ ИТ-АКТИВА*** | Недостаток (слабость) ИТ-актива в целом, который(ая) может быть использован(а) для реализации угроз информационной безопасности. |
| ***ЦИФРОВИЗАЦИЯ*** | Применение прорывных технологий, трансформирующих операционные процессы за счет замещения или дополнения человека на базе использования качественно новой аналитики, искусственного интеллекта, мобильных и носимых устройств, роботизации, интеграционных технологических платформ. |

# 5. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

Основными объектами защиты системы информационной безопасности в Банке являются информационные ресурсы, содержащие:

* коммерческую тайну;
* банковскую тайну;
* персональные данные физических лиц (сотрудников и клиентов);
* сведения ограниченного доступа;
* открыто распространяемую информацию, необходимую для работы Банка, независимо от формы и вида ее представления.

Особые объекты защиты, имеющие высокую важность для Банка:

* банковский платежный технологический процесс;
* банковский информационный технологический процесс;
* платежная информация;
* информация, отнесенная к защищаемой в соответствии с Положением Банка России от 09.06.2012 № 382-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 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России»;
* иная значимая для Банка информация, разглашение или модификация которой может привести к негативным последствиям для Банка;
* носители защищаемой информации, в т. ч. информационные ресурсы, речевая информация, документы на физических носителях информации, определенные как защищаемые нормативно-распорядительными документами Банка.

# ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**6.1.** 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.

**6.2.** 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.

**6.3.** 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 в соответствии с Положением Банка России 382-П и оценки соответствия национальному стандарту Российской Федерации ГОСТ Р 57580.1-2017;

− реализация четырех групп процессов (которые составляют систему менеджмента информационной безопасности), в целях реализации и поддержания должного уровня 12 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.

**6.4.** Основополагающие принципы, на которых основывается 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.

# МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**7.1.** 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.

**7.2.** 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.

**7.3.** 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.

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

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

− определение возможных негативных последствий от реализации угроз безопасности информации;

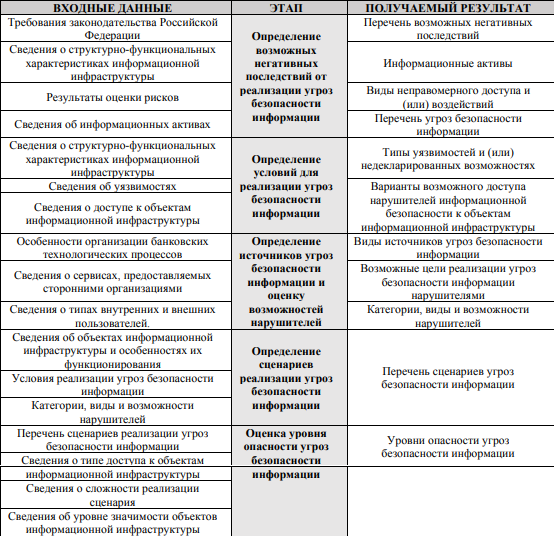
− определение условий для реализации угроз безопасности информации;

− 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



**7.6.** 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.

**7.7.** 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.

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

**7.9.** 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

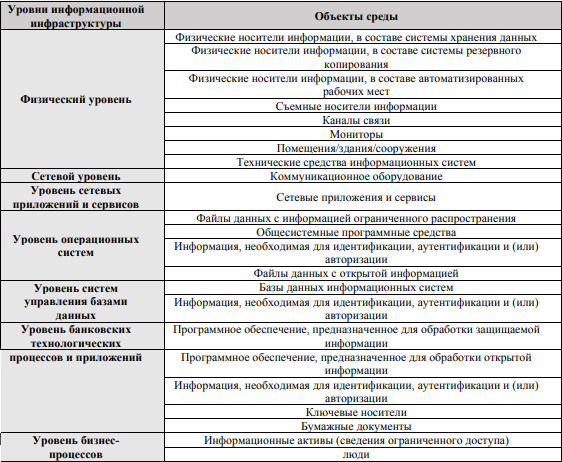


Таблица 3 – Способы реализации угроз безопасности информации



# УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. 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.

8.2. 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.

8.3. 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.

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

# РЕАЛИЗАЦИЯ, КОНТРОЛЬ, ПЕРЕСМОТР НАСТОЯЩЕЙ ПОЛИТИКИ

9.1. За реализацию положений настоящей Политики и поддержание ее в актуальном состоянии отвечает начальник отдела автоматизации и информационного сопровождения. Контроль за реализацией положений настоящей Политики и поддержанием её в актуальном состоянии возлагается на куратора информационной безопасности.

9.2. Для обеспечения актуальности настоящей Политики осуществляется ее плановый (регулярный) и внеплановый пересмотр.

9.2.1. Плановый пересмотр проводится с периодичностью не реже чем один раз в год. 9.2.2. Внеплановый пересмотр должен осуществляться в случаях:

– 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 базами данных и т.п.);

средства защиты информации;

вспомогательные технические средства и системы.

9.3. В Банке разрабатываются нормативно-методические документы по обеспечению информационной безопасности, определяющие порядок выполнения требований положений настоящей Политики.

9.4. Порядок пересмотра настоящей Политики:

− специалист по информационной безопасности и начальник отдела автоматизации и информационного сопровождения Банка собирают предложения по изменению настоящей Политики от заинтересованных сторон в следующих случаях:

• поступило обоснованное предложение пересмотреть настоящую Политику;

• в случае, предусмотренном п. 10.2.2. настоящей Политики;

• по указанию руководства Банка или куратора по информационной безопасности;

− специалист по информационной безопасности и начальник отдела автоматизации и информационного сопровождения Банка составляют проект документа;

− выполняется процедура согласования;

− документ направляется на утверждение Правления Банка.

# ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

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

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

10.3. 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.