«УТВЕРЖДЕНО»
Приказом Директора ТОО «PrimePay»
№ 26 от 17.09.2024 г.

_____ / Добряков К.Е.

Правила
Системы электронных денег «PrimeWallet»

2024 г.

СОДЕРЖАНИЕ

1. Термины и определения

В настоящих Правилах Системы электронных денег «PrimeWallet» (далее – «Правила») используются термины и определения, предусмотренные Закона Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее – «Закон») и Правилами выпуска, использования и погашения электронных денег, а также требованиями к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан, утвержденными Постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 202, а также следующие понятия:

Банк-эмитент (Эмитент) – Банк второго уровня Республики Казахстан, с которым у ТОО «PrimePay» заключен договор, а также который осуществляет выпуск и погашение Электронных денег в Системе и обязуется обеспечить расчеты по Платежам, совершаемым Пользователями с их использованием в рамках Системы «PrimeWallet».

Владельцы электронных денег – Пользователи и Поставщик услуг, Агент.

Выпуск электронных денег – платежная услуга, предусматривающая выпуск Электронных денег Эмитентом электронных денег Оператору системы электронных денег путем обмена на равную по их номинальной стоимости сумму денег на основании договора между Эмитентом и Оператором;

Использование электронных денег – передача Электронных денег их Владельцем другому Участнику Системы в целях осуществления Платежа по гражданско-правовым сделкам и (или) иных операций, связанных с переходом права собственности на Электронные деньги в Системе;

Оператор Системы электронных денег (Оператор Системы, Оператор) – платежная организация ТОО «PrimePay», рег. номер № 02-21-113, обеспечивающая функционирование Системы электронных денег, а также сбор, обработку и передачу информации, формируемой при осуществлении операций с использованием Электронных денег в рамках Системы, а также определяющая правила функционирования Системы электронных денег;

Оферта – Публичная оферта об использовании Системы «PrimeWallet» ТОО «PrimePay», на условиях которой Оператор Системы заключает с Владельцами электронных денег – физическими лицами от имени Эмитента договоры об оказании услуг по обеспечению функционирования Системы, оказанию платежных услуг по приему и обработке платежей, совершаемых с использованием Электронных денег в Системе «PrimeWallet», в том числе по сбору, обработке и передачи Эмитенту информации, формируемой при осуществлении операций с использованием Электронных денег Эмитента в рамках Системы «PrimeWallet». Актуальная версия Оферты размещена на WEB-сайте Системы «PrimeWallet» по электронному адресу: https://primewallet.kz/

Платеж – операция по передаче Пользователем в адрес Эмитента информации для осуществления расчетов с использованием Электронных денег в целях погашения финансовых обязательств Пользователя перед Получателем платежа в Системе (исполнение обязательств Пользователя перед Поставщик услуг за приобретенные Товары или перевод Электронных денег другому Пользователю).

Пользователь – физическое лицо, обладающее надлежащей дееспособностью и/или правоспособностью в соответствии с действующим законодательством РК для совершения Платежа, совершившее конклюдентные действия, направленные на заключение Договора об оказании услуг посредством акцепта условий Оферты, и обладающее Аутентификационными данными для доступа к Системе для ее использования в целях управления Учетной записью Пользователя, осуществлению доступа к Электронным деньгам на Балансе Учетной записи Пользователя в целях совершения Платежей.

Поставщик услуг (далее-ПУ) – юридическое лицо, включая благотворительные организации, или индивидуальный предприниматель, являющийся Участником Системы, осуществляющий коммерческую деятельность (благотворительная организация, как и другие некоммерческие организации, занимается коммерческой деятельностью **постольку, поскольку это соответствует ее уставным целям)** и принимающий Электронные деньги от Пользователей в качестве оплаты по гражданско-правовым сделкам на основе договора, заключенного с Оператором;

Получатель Платежа (Получатель) – Пользователь, ПУ, Оператор Системы.

Поставщик услуг – юридическое лицо, включая благотворительные организации, или

индивидуальный предприниматель, являющийся Участником Системы, осуществляющий коммерческую деятельность (благотворительная организация, как и другие некоммерческие организации, занимается коммерческой деятельностью **постольку, поскольку это соответствует ее уставным целям**), с которым у Платежной организации заключен Договор на оказание платежных услуг по приему в его пользу наличных денег.

Учетная запись – Электронный кошелек Пользователя. Идентификатором Учетной записи Пользователя в учете Оператора Системы выступает Абонентский номер Пользователя. Идентификатором Учетной записи ПУ в учете Оператора Системы выступает id-номер ПУ, присваиваемый Оператором Системы.

Платежный агент – юридическое лицо и/или индивидуальный предприниматель, заключивший с Платежной организацией Договор на оказание платежных услуг с Платежным агентом;

Погашение электронных денег – осуществление Банком-Эмитентом перечисления идентифицированному Владельцу электронных денег, предъявившему их к погашению, равной (если иное не предусмотрено тарифами Оператора Системы) по их номинальной стоимости суммы денег на его банковский счет или выдачу ему наличных денег;

Система электронных денег «PrimeWallet» (Система «PrimeWallet», Система) – совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих осуществление Платежей и иных операций с использованием Электронных денег путем взаимодействия Оператора Системы с Банком-Эмитентом и (или) Владельцами Электронных денег;

Субагент – юридическое лицо или индивидуальный предприниматель, заключившие с Платежным агентом Договор на оказание платежных услуг;

Участники системы – Эмитент, Агент Эмитента, Платежный агент, Пользователь, ПУ.

Электронные деньги (ЭД) – безусловные и безотзывные денежные обязательства эмитента электронных денег, хранящиеся в электронной форме и принимаемые в качестве средства платежа в системе электронных денег другими участниками системы;

Электронный кошелек «PrimeWallet» (Электронный кошелек) – способ учета и хранения Электронных денег в Системе «PrimeWallet», обеспечивающий распоряжение ими;

WEB-сайт Системы/Оператора – https://primewallet.kz/

1. Общие положения

Правила Системы электронных денег «PrimeWallet» (далее – «Правила») являются внутренним нормативным документом Системы, регулирующим правила осуществления Участниками Системы деятельности в рамках Системы электронных денег «PrimeWallet».

Правила определяют:

- порядок выпуска, реализации, приобретения, погашения Электронных денег;
- порядок осуществления операций с использованием Электронных денег;
- технологию управления рисками в Системе;
- порядок урегулирования споров Участников Системы между собой, а также между Участниками Системы и лицами, не входящими в Систему.

2. Использование Электронных денег

2.1. Под «использованием электронных денег» в рамках Системы «PrimeWallet» понимается деятельность ТОО «PrimePay», зарегистрированного в реестре платежных организаций Национального Банка Республики Казахстан за № 02-21-113 от 09.12.2021 г., связанная с реализацией Электронных денег, а также с проведением расчетов с использованием Электронных денег.

Договор, заключаемый Оператором Системы с физическим лицом - владельцем Электронных денег, разрабатывается Оператором Системы самостоятельно с соблюдением настоящих Правил Системы и согласовывается с Эмитентом.

Договор, заключаемый Оператором Системы с ПУ на оказание платежных услуг по приему в

их пользу платежей с использованием Электронных денег в рамках Системы при оплате по гражданско-правовым сделкам разрабатывается Оператором Системы самостоятельно, с соблюдением настоящих Правил Системы и согласовывается с Эмитентом.

До момента заключения Оператором Системы с Поставщиком услуги соответствующего договора на оказание платежных услуг по приему в его пользу Электронных денег в качестве ПУ, Оператор Системы (при необходимости) осуществляет учитывает принятые в пользу такого Поставщика услуг Платежи на Электронном кошельке Платежной организации, как Агента Эмитента, с последующим предъявлением полученных Электронных денег к погашению Эмитенту и дальнейшим проведением расчетов с Поставщиком услуг.

Договор, заключаемый Оператором Системы с юридическим лицом или индивидуальным предпринимателем - Агентом Эмитента (в случае привлечения Эмитентом такового), разрабатывается Оператором Системы самостоятельно, с соблюдением настоящих Правил Системы и согласовывается с Эмитентом.

1.1. Общие вопросы выпуска Электронных денег

В рамках Системы «PrimeWallet» Банк-Эмитент осуществляет выпуск Электронных денег.

Выпуск Электронных денег осуществляется Банком-Эмитентом в пределах суммы денежных средств, предварительно внесенных Агентом Банка-Эмитента или физическим лицом Банку-Эмитенту, в соответствии с условиями заключенного между Оператором и таким Агентом Банка-Эмитента/физическим лицом договора.

Выпуская Электронные деньги, Банк-Эмитент принимает на себя безусловные и безотзывные денежные обязательства, хранящиеся в электронной форме и принимаемые в качестве средства платежа в Системе Электронных денег другими Участниками Системы и заменяющие в процессе их обращения требования торгово-сервисных предприятий и/или Владельцев электронных денег по оплате товаров или услуг, и в том числе денежные обязательства, составленные в электронной форме.

Выпуск Электронных денег в Системе производится в национальной валюте Республики Казахстан.

1.2. Общие вопросы реализации Электронных денег

В рамках Системы «PrimeWallet» Банк-Эмитент вправе осуществлять реализацию Электронных денег как самостоятельно, так и с привлечением Агентов на основании соответствующего договора между Банком-Эмитентом и Агентом Банка- Эмитента (если это не противоречит применимому законодательству Республики Казахстан).

Платежная организация ТОО «PrimePay» при оказании платежной услуги по реализации (распространению) Электронных денег в Системе выступает Агентом Эмитента, с целью приобретения Электронных денег у Эмитента и владельцев электронных денег - физических лиц. При реализации Электронных денег физическим лицам Платежная организация привлекает Платежных агентов/субагентов.

Реализация Электронных денег осуществляется путем внесения физическим лицом Банку-Эмитенту (либо его Агенту) наличных денежных средств, либо путем перечисления денежных средств в безналичном порядке на соответствующий счет Банка-Эмитента.

В момент реализации Электронных денег Владельцу электронных денег выдается квитанция в электронном виде, подтверждающая факт приобретения физическим лицом Электронных денег. Форма и способы выдачи квитанции при реализации Электронных денег устанавливается Публичной офертой об использовании Системы «PrimeWallet» ТОО «PrimePay». Содержание квитанции должно полностью соответствовать требованиям применимого законодательства Республики Казахстан.

Допускается реализация Электронных денег Агентами Банка-Эмитента через электронные терминалы, позволяющие совершать операции по приему наличных денежных средств, пункты приема денежных средств и иными способами, не противоречащими применимому законодательству Республики Казахстан на основании договора, заключенного между Оператором и Агентами Банка-Эмитента.

Электронные деньги считаются реализованными Владельцу электронных денег с момента отражения информации о доступном остатке Электронных денег в Электронном кошельке Владельца электронных денег.

1.3. Общие вопросы погашения Электронных денег

В рамках Системы «PrimeWallet» Банки-Эмитенты вправе осуществлять погашение Электронных денег, если это не противоречит применимому законодательству Республики Казахстан.

Погашение Электронных денег осуществляется Банком-Эмитентом при их предъявлении Владельцем Электронных денег к погашению. Банк-Эмитент погашает Электронные деньги путем перечисления равной по их номинальной стоимости (Если иное не предусмотрено тарифами Оператора) суммы денег на банковский счет, указанный идентифицированным Владельцем электронных денег, либо путем выдачи ему наличных денежных средств.

При погашении Электронных денег сумма денежных средств, выдаваемых (переводимых) Владельцу электронных денег, предъявившему Электронные деньги к погашению, должна соответствовать сумме Электронных денег, предъявленных к погашению.

Электронные деньги считаются погашенными Банком-Эмитентом с момента выдачи Владельцу, предъявившему Электронные деньги к погашению, соответствующей суммы наличных денежных средств или зачисления соответствующей суммы денежных средств на банковский счет, указанный Владельцем Электронных денег.

2. Расчеты с использованием электронных денег

2.1. Общие вопросы осуществления операций с использованием Электронных денег

Операции с использованием Электронных денег осуществляются Банком-Эмитентом в соответствии с положениями настоящих Правил, условиями договоров, заключенных Оператором с Агентами Банка-Эмитента, торгово-сервисными предприятиями, Офертой и нормами применимого законодательства Республики Казахстан.

Операции с использованием Электронных денег осуществляется на основании распоряжения Владельца электронных денег, переданного с использованием технических средств и методов, определенных Офертой.

Для обеспечения безопасности совершения операций с использованием Электронных денег Банк-Эмитент обязан использовать только те технические средства и методы, право на использование которых предоставлено ему Оператором Системы в момент присоединения Банка-Эмитента к Системе «PrimeWallet».

Распоряжение Владельца электронных денег о совершении операции с использованием Электронных денег должно содержать указание на сумму операции, конечного получателя Электронных денег и иные реквизиты, установленные Оператором Системы в договоре, заключенном с Владельцем электронных денег.

Операция с использованием Электронных денег осуществляется путем списания электронных денег с Баланса Учетной записи Владельца электронных денег в Системе, направившего соответствующего распоряжение, и их передачи указанному таким Владельцем электронных денег Получателю.

Осуществление операции с использованием Электронных денег сопровождается выдачей Владельцу электронных денег, направившему распоряжение о совершении соответствующей операции, торгового чека в форме электронной квитанции, подтверждающего факт осуществления операции с использованием Электронных денег. Форма и способы выдачи такой электронной квитанции в качестве подтверждающего документа устанавливаются Офертой. Содержание электронной квитанции, подтверждающей совершение операции с использованием Электронных денег, должно полностью соответствовать требованиям применимого законодательства Республики Казахстан к торговым чекам.

По запросу Владельца электронных денег Оператор обязан предоставить ему отчет, содержащий информацию обо всех операциях, совершенных таким Владельцем электронных денег по своей Учетной записи в Системе. Формат и сроки предоставления отчета определяются Офертой.

2.2. Оплата товаров (работ, услуг).

2.2.1. Общие вопросы оплаты товаров (работ, услуг).

Операции оплаты товаров (работ, услуг) с использованием Электронных денег могут совершаться в торгово-сервисном предприятии, осуществляющем реализацию товаров (работ, услуг) – ПУ, с которым у Оператора Сервиса заключен соответствующий Договор на оказание платежных услуг по приему в его пользу платежей с использованием Электронных денег.

Операции оплаты товаров (работ, услуг) осуществляются в пределах лимитов, устанавливаемых Законом и Офертой.

2.2.2. Требования к совершению операций оплаты товаров (услуг), погашения кредитных обязательств

При совершении операции оплаты товаров (услуг) ПУ, Оператор Системы обязан обеспечить выполнение следующих требований:

- выполнение проверки совершаемой операции на соответствие ограничениям по сумме допустимых операций, установленных действующим законодательством и Офертой для данного типа Учетной записи;
- выполнение авторизации операции, планируемой к совершению с использованием Электронных денег;
- формирование первичного документа по совершенной операции в электронной форме;
- предоставление Владельцу электронных денег подтверждающего документа, оформленного согласно требованиям применимого законодательства Республики Казахстан, по результатам осуществленной операции, в электронном виде.

3. Управление рисками

3.1. Общие положения управления рисками идентификация угроз и уязвимости автоматизированных информационных систем

Основными функциями Оператора Системы при обеспечении безопасности операций, осуществляемых Участниками Системы в связи с выпуском, реализацией и погашением Электронных денег, являются:

- идентификация угроз и уязвимости автоматизированных информационных систем;
- Оценка рисков информационной безопасности информационных систем;
- Обработка рисков информационной безопасности информационных систем.

Настоящий раздел Правил определяет порядок проведения оценки рисков информационной безопасности для автоматизированных информационных систем, а также методику обработки выявленных рисков.

Порядок распространяется на всех Участников Системы и их автоматизированные информационные системы, и является обязательной к исполнению Участниками Системы.

3.2. Идентификация угроз и уязвимостей

Идентификация угроз и уязвимостей автоматизированных информационных систем проводится коллегиально, с участием представителей Оператора Системы, Банка-Эмитента, чьи автоматизированные информационные системы проходят проверку, а также иных Участников Системы, взаимодействующие с автоматизированными информационными системами проверяемого Банка-Эмитента/Оператора.

Идентификация угроз и уязвимостей автоматизированных информационных систем проводится по мере выявления новых угроз и уязвимостей автоматизированных информационных систем, но не реже одного раза в год.

При идентификации угроз и уязвимостей обязательно должны быть учтены:

- сведения об инцидентах информационной безопасности, произошедших в автоматизированных информационных системах Банка-Эмитента;
- результаты выполнения утвержденных в Системе процедур проверок (сканирование уязвимостей, тесты на проникновение, мониторинг событий информационной безопасности и прочие);
- мнения заинтересованных Участников Систем;
- информация внешних специализированных баз знаний (новостные ленты и прочие).

По результатам процесса идентификации угроз и уязвимостей проверяемый Банк- Эмитент создает реестр выявленных угроз и уязвимостей.

3.3. Оценка рисков информационной безопасности

Оценка рисков информационной безопасности проводится комиссией по оценке рисков (далее - «Комиссия по оценке рисков») не реже одного раза в год, а также при возникновении существенных изменений, влияющих на результаты предыдущей оценки.

Комиссия по оценке рисков формируется из представителей Оператора Системы, Банка-Эмитента, а также иных Участников Системы, использующих и/или взаимодействующих с проверяемыми автоматизированными информационными системами, из числа специалистов, обладающих достаточной осведомленностью о ключевых используемых автоматизированных информационных системах, основных процессах и рисках.

Организацию работы, подготовку исходной информации, модерирование работы и председательство в Комиссии по оценке рисков осуществляет полномочный представитель Оператора Системы (далее - «Председатель Комиссии по оценке рисков»).

Оценка рисков информационной безопасности автоматизированных информационных систем производится в соответствии с процедурой, описанной в Приложении № 1 к настоящим Правилам.

Работа Комиссии по оценке рисков завершается формированием Отчета об оценке рисков, утверждаемого Председателем Комиссии по оценке рисков, который включает в себя рекомендации Комиссии по оценке рисков о доработках автоматизированных информационных систем Банка-Эмитента в части предотвращения угроз и устранения уязвимостей таких систем в части информационной безопасности.

3.4. Обработка рисков информационной безопасности

Значение приемлемого уровня риска информационной безопасности автоматизированных информационных систем Участников Системы устанавливается Оператором Системы.

Возможные варианты действий с выявленными рисками, прошедшими оценку:

- выбор и применение защитных мер, направленных на снижение рисков до приемлемого уровня;
- предотвращение рисков, путем исключения рискованных действий и/или оптимизации работы автоматизированных информационных систем;
- перенос рисков на третьих лиц, не являющихся Участниками Системы (например, страхование рисков информационной безопасности);
- принятие рисков, если их значение не превышает приемлемый уровень;
- принятие рисков, если стоимость реализации защитных мер превышает вероятный ущерб от реализации соответствующей угрозы.

При рассмотрении Отчета об оценке рисков Комиссия по оценке рисков принимает решение об обработке рисков: риски, не превышающие приемлемые уровни, принимаются; остальные снижаются, предотвращаются или переносятся.

На основании решения Комиссии по оценке рисков Оператор Системы разрабатывает, в отношении рисков, требующих проведения мероприятий, План обработки рисков информационной безопасности.

Разработанный и согласованный План обработки рисков подлежит выполнению Участником(ами) Системы в течение установленного Оператором Системы срока. По итогам выполнения Плана обработки рисков проводится повторная идентификация угроз и уязвимостей автоматизированных информационных систем соответствующего Участника Системы.

4. Урегулирование споров

4.1. Претензия Участника Системы

В случае возникновения у Участника Системы каких-либо претензий к Оператору Системы и/или иным Участниками Системы по любой спорной ситуации, связанной с осуществлением Участником Системы деятельности в рамках Системы «PrimeWallet», Участник Системы вправе направить Оператору Системы соответствующую претензию в письменной форме.

В случае если претензия Участника Системы связана с опротестованием совершенных с использованием Электронных денег операций в Системе, такая претензия может быть подана Участником Системы только в одном из следующих случаев:

- операция с использованием электронных денег не была осуществлена по вине одного из Участников Системы;
- операция с использованием электронных денег была заблокирована Оператором Системы в связи с подозрением на незаконность такой операции.

К направляемой Участником Системы претензии должны быть приложены документы, содержащие доказательства обстоятельств, послуживших поводом для направления претензии.

Претензия может быть направлена Участником Системы любым из следующих способов:

- в электронном виде, посредством электронного документооборота;
- заказным почтовым отправлением с уведомлением и описью вложения;
- нарочным, с проставлением отметки уполномоченного представителя Оператора Системы о получении претензии.

4.2. Рассмотрение претензии

Рассмотрение претензии Участника Системы осуществляется Оператором Системы в течение 10 (Десяти) рабочих дней с даты поступления к Оператору Системы соответствующей претензии от Участника Системы.

По результатам рассмотрения претензии Участника Системы Оператор Системы производит одно из следующих действий:

- в случае установления правомерности требований Участника Системы, заявленных в претензии (полностью или в части), предпринимает действия, направленные на удовлетворение требований Участника Системы по спорной ситуации;
- в случае установления неправомерности требований Участника Системы, заявленных в претензии, направляет Участнику Системы, от которого получена претензия, разъяснительную информацию в отношении спорной операции.

4.3. Порядок разрешения споров

В случае несогласия кого-либо из Участников Системы, интересы которого затронуты решением Согласительной комиссии, с решением Согласительной комиссии, такой Участник Системы в течение 30 (Тридцати) календарных дней после получения решения Согласительной комиссии вправе уведомить Оператора Системы о своем несогласии. В таком уведомлении о несогласии должны быть указаны спорные вопросы и причины несогласия.

Ни одна из сторон спорной ситуации не имеет права начинать судебное разбирательство в отношении любого спора, если не было представлено уведомление о несогласии с решением Согласительной комиссии, как описано выше.

Если ни одна из сторон спорной ситуации не представила уведомления о несогласии с решением Согласительной комиссии в пределах 30 (Тридцати) календарных дней после получения соответствующего решения Согласительной комиссии, то решение Согласительной комиссии становится окончательным и имеет обязательную силу для всех заинтересованных Участников Системы.

Если Оператором Системы от какой-либо из сторон спорной ситуации будет получено уведомление о несогласии, заинтересованные Участники Системы обязаны попытаться мирным путем урегулировать спор до начала судебного разбирательства. Однако, если Сторонами не согласовано иначе, судебное разбирательство может быть начато по истечении 45 (Сорока пяти) календарных дней с момента представления уведомления о несогласии: даже если не было предпринято попыток урегулировать спор мирным путем.

Любой спор, решение Согласительной комиссии по которому не стало окончательным и обязательным для всех заинтересованных Участников Системы, и если спорная ситуация не разрешена мирным путем, такая спорная ситуация подлежит окончательному разрешению в судебном порядке в соответствии с действующим законодательством Республики Казахстан.

При этом, ни один из Участников Системы в ходе судебного разбирательства: не может быть ограничен представлением доказательств или аргументов, которые ранее. выдвигались Согласительной комиссии для вынесения ею решения, или причинами несогласия, указанными в уведомлении о несогласии. Любое решение Согласительной комиссии может быть предъявлено в суде в качестве подтверждения или доказательства.

Приложение № 1:

Процедура Оценки рисков информационной безопасности автоматизированных информационных систем

Исходной информацией для проведения оценки рисков являются:

- перечень информационных систем, процессов и прочих активов, для которых проводится оценка рисков;
- актуальный Реестр угроз и уязвимостей;
- результаты предыдущей оценки рисков информационной безопасности.

В ходе проведения Оценки рисков информационной безопасности члены Комиссии по оценке рисков определяют набор угроз и уязвимостей, применимых к каждому из активов, и проводят их оценку с точки зрения степени вероятности реализации и степени тяжести последствий, основываясь на знаниях о реализованных защитных мерах и ценности актива. Отчетным документом по результатам собрания является Отчет об оценке рисков информационной безопасности.

Под определением степени вероятности реализации (СВР) нарушения информационной безопасности подразумевается значение в соответствии со шкалой ниже, определяющее потенциальную вероятность реализации угрозы для данного актива с учетом реализованных защитных мер.

Для выполнения оценки СВР угроз информационной безопасности проводится анализ возможности потери каждого из свойств информационной безопасности для информационных активов в результате воздействия выделенных источников угроз.

Основными факторами для оценки СВР угроз информационной безопасности являются: информация соответствующих моделей угроз, в частности:

данные о расположении источника угрозы относительно соответствующих типов объектов среды;

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

предположения о квалификации и (или) ресурсах источника угрозы; статистические данные о частоте реализации угрозы ее источником в прошлом; информация о способах реализации угроз информационной безопасности; информация о сложности обнаружения реализации угрозы рассматриваемым источником;

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

Для оценки СВР угроз информационной безопасности используется следующая качественная шкала степеней:

- крайне маловероятно- «1»;
- маловероятно - «2»;
- потенциально возможно - «3»;
- высокая вероятность реализации - «4»;
- реализуемо - «5».

При привлечении к оценке отдельных СВР угроз информационной безопасности нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СВР угроз информационной безопасности принимать равной экспертной оценке, определяющей наибольшую СВР угрозы информационной безопасности.

Для угроз, источником которых является человек, простота реализации угрозы путем эксплуатации уязвимости прямо пропорциональна необходимой для ее реализации квалификации злоумышленника.

Для определения степени тяжести последствий (СТП) нарушения информационной безопасности проводится анализ последствий потери каждого из свойств информационной безопасности для каждого из типов информационных активов в результате воздействия на соответствующие им типы объектов среды выделенных источников угроз.

Основными факторами для оценки СТП 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 информационной безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения информационной безопасности;

объем людских ресурсов, необходимых для восстановления свойств информационной безопасности 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;
- 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.

Для оценки СТП нарушения информационной безопасности вследствие реализации угроз информационной безопасности используется следующая качественная шкала степеней:

- незначительная - «1»;
- небольшая - «2»;
- существенная - «3»;
- серьезная - «4»;
- критическая - «5».

При привлечении к оценке отдельных СТП нарушения информационной безопасности нескольких экспертов и получении разных экспертных оценок рекомендуется итоговую, обобщенную оценку СТП нарушения информационной безопасности принимать равной экспертной оценке, определяющей наибольшую СТП нарушения информационной безопасности.

Каждый член Комиссии оглашает собственную субъективную оценку СВР и СТП угроз для рассматриваемого скоупа оценки рисков.

Результирующие оценки рассчитываются по формуле:

$$V_R = (V_1 + V_2 + ... + V_n) / n, \text{ где:}$$

V_R – результирующая оценка;

V_n – оценка, выданная i-ым членом Комиссии;

n – общее количество членов Комиссии.

Результирующие оценки фиксируются Председателем Комиссии в Отчете об оценке рисков информационной безопасности.

Риски рассчитываются по следующей формуле:

$$R = СВР \times СТП, \text{ где:}$$

R -

СВР - .степень вероятности реализации угрозы нарушения ИБ

СТП – степень тяжести последствий реализации угрозы нарушения ИБ;

Риски могут принимать значение от 1 до 25.

Полученный отчет об оценке рисков в рабочем порядке проходит согласование со всеми членами Комиссии, и утверждается Оператором Системы.