ООО «RAQAMLI BIZNES AGREGATOR»

«УТВЕРЖДАЮ»
Директор Толаганов А.А.

10 января 2023 год

Сведения о системе управления рисками, в том числе о требованиях к обеспечению сохранности денежных средств клиентов

ООО «RAQAMLI BIZNES AGREGATOR»

Ташкент 2022

1 Определение рисков информационной безопасности

1.1 Общее описание определения рисков информационной безопасности

Риск представляет собой комбинацию последствий, вытекающих из нежелательного события, и вероятности возникновения события. Определение рисков количественно или качественно описывает риски и даёт возможность руководителям расставлять риски в соответствии с приоритетами согласно воспринимаемой серьёзности или другим установленным критериям.

Определение риска состоит из следующих мероприятий:

- идентификации рисков в соответствии с 1.2; -
анализа рисков в соответствии с 1.3; -
оценивания рисков в соответствии с 1.4.

Определение рисков определяет ценность информационных активов, идентифицирует применимые угрозы и уязвимости, которые существуют (или могут существовать), идентифицирует существующие средства управления и их влияние на идентифицированные риски, определяет потенциальные последствия и, наконец, расставляет определенные риски в соответствии с приоритетами и классифицирует их по критериям оценивания рисков, определенным при установке контекста.

Определение риска часто проводится, используя две (или более) итерации. Сначала проводится высокоуровневое определение для идентификации потенциально высоких рисков, гарантирующих дальнейшую оценку. Следующая итерация может включать дальнейшее углублённое рассмотрение потенциально высоких рисков, обнаруженных при первоначальной итерации. В тех случаях, когда данные действия предоставляют недостаточную информацию для оценки рисков, проводится дальнейший детальный анализ с использованием иного метода и применительно только к определенным частям области действия рисков.

Выбор собственного подхода к определению рисков на основе задач и цели определения рисков зависит от самой организации.

1.2 Идентификация рисков

1.2.1 Введение в идентификацию рисков

Целью идентификации рисков является прогнозирование возможных инцидентов, влекущих потенциальный ущерб, и получение представления о том, каким образом данный ущерб мог быть получен. Шаги, описанные ниже, определяют входные данные для мероприятий по анализу рисков.

1.2.2 Определение активов

Активом является что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите. При определении активов следует иметь в виду, что информационная система состоит не только из аппаратных и программных средств.

Определение активов следует осуществлять на соответствующем уровне детализации, обеспечивающем достаточную информацию для определения рисков. Уровень детализации, используемый при определении активов, влияет на общий объем информации, собранной во время определения рисков. Этот уровень может быть более детализирован при дальнейших итерациях определения рисков.

Для каждого актива должен быть определён владелец, чтобы обеспечить ответственность и учет за каждый актив. Владелец актива может не обладать правами собственности на актив, но он несёт соответствующую ответственность за его производство, разработку, обслуживание, использование и безопасность. Чаще всего владелец актива является наиболее подходящим лицом, способным определить реальную ценность актива для организации. Информация об определении ценности активов приведена в 1.3.2.

Границей пересмотра является периметр активов организации, определённый как подлежащий управлению посредством процесса управления рисками информационной безопасности.

1.2.3 Определение угроз

Угроза может быть причиной нанесения вреда активам, таким как информация, процессы и системы, а, следовательно, и организациям. Угрозы могут быть природного происхождения или результатом действий людей, они могут быть случайными или умышленными. Должны быть определены и случайные и умышленные источники угроз. Угроза может проистекать как из самой организации, так и извне. Угрозы должны определяться в общем и по типу (например, неавторизованные действия, физический ущерб, технические сбои), а затем, где это уместно, отдельные угрозы определяются внутри общего класса. Это означает, что ни одна угроза, включая неожиданные, не будет упущена, но объем требуемой работы ограничен.

Некоторые угрозы могут влиять на несколько активов. В таких случаях они могут быть причиной различных воздействий, в зависимости от того, на какие активы оказывается воздействие.

Входные данные для определения и измерения вероятности возникновения угроз (1.2.2.3) могут быть получены от владельцев активов или пользователей, персонала отдела кадров, руководства организации и

специалистов по информационной безопасности, экспертов по физической безопасности, юридического отдела и других структур, включая правоохранительные органы, метеорологические службы, страховые компании, национальные правительственные учреждения. При рассмотрении угроз должны учитываться аспекты среды и культуры.

Внутренний опыт, полученный в результате инцидентов, и прошлые определения угроз должны быть учтены в текущем определение. Целесообразно учитывать иные реестры угроз (возможно, специфичные для организации или бизнеса), чтобы заполнить перечень общих угроз, где это уместно. Реестры и статистику угроз можно получить от промышленных организаций, национальных правительств, правоохранительные органы, страховых компаний и т.д.

Используя реестры угроз или результаты прежних определений угроз, не следует забывать о том, что происходит постоянная смена значимых угроз, особенно, если изменяются деловая среда или информационные системы.

1.2.4 Определение существующих средств управления

Определение существующих средств управления должно быть осуществлено во избежание ненужной работы или расходов, например, при дублировании средств управления. Кроме того, во время определения существующих средств управления следует провести проверку, удостоверяющую, что средства управления функционируют правильно - существующие отчёты по раннее проведенным аудитам СУИБ должны уменьшить время, затрачиваемое на эту задачу. Если средства управления не работают, как ожидалось, это может стать причиной уязвимости. Следует уделить внимание ситуации, когда операции выбранных средств управления требуют дополнительные средства управления для эффективного рассмотрения определяемых рисков. В СУИБ, в соответствии с O‘z DSt ISO/IEC 27001, это поддерживается измерением эффективности средств управления. Один из способов оценить действие средств управления - посмотреть, как оно уменьшает вероятность угроз и простоту использования уязвимости или воздействие инцидента. Анализы со стороны руководства и отчёты по аудиту также обеспечивают информацию об эффективности существующих средств управления.

Средства управления, которые планируется внедрить в соответствии с планами реализации обработки риска, должны учитываться тем же самым способом, который уже был реализован.

Существующие или планируемые средства управления могут быть определены как неэффективные, недостаточные или необоснованные. Если их посчитали необоснованными или недостаточными, средства управления

необходимо проверить, чтобы определить стоит ли их удалить, заменить другими, более подходящими, или продолжить их использование, например, по причинам отсутствия бюджета на внедрение новых средств управления.

Для определения существующих или планируемых средств управления рекомендуются следующие мероприятия:

- пересмотр документов, содержащих информацию о средствах управления (например, планы обработки рисков). Если процессы управления информационной безопасностью задокументированы должным образом, то все существующие или планируемые средства управления и состояние их реализации должны быть доступны;
- проверка средств управления на предмет их внедрения в рассматриваемый информационный процесс или информационную систему силами пользователей и ответственных за информационную безопасность (например, администратор по информационной безопасности, комендант здания или руководитель работ);
- обход здания с проведением осмотра физических средств управления, сравнение реализованных средств управления с перечнем тех, которые должны быть, и проверка реализованных средств управления на предмет правильной и эффективной работы;
- рассмотрение результатов внутренних аудитов.

1.2.5 Определение уязвимостей

Уязвимости могут быть определены в следующих областях:

- организация работ;
- процессы и процедуры;
- установленный порядок управления;
- персонал;
- физическая среда;
- конфигурация информационной системы;
- аппаратные средства, программное обеспечение и средства телекоммуникаций;
- зависимость от внешних сторон.

Наличие уязвимости не причиняет вреда само по себе, так как необходимо наличие угрозы, которая будет реализована посредством ее. Уязвимость, на которую не воздействует определенная угроза, может не требовать внедрения средства управления, но должна быть выявлена и подвергаться мониторингу на предмет изменений. Следует отметить, что неверно реализованное, используемое или неправильно функционирующее средство управления само может быть уязвимостью. Средство управления

может быть эффективным или неэффективным в зависимости от среды, в которой оно функционирует. И наоборот, угроза, для которой не существует уязвимость, может не приводить к риску.

Уязвимости могут быть связаны со свойствами актива, которые могут использоваться способом и с целью, отличающимися от тех, которые планировались при приобретении или создании актива. Уязвимости, возникающие из различных источников, подлежат рассмотрению, например, те которые являются внешними или внутренними по отношению к активу.

1.2.6 Определение последствий

Последствием может быть потеря эффективности, неблагоприятные условия работы, потеря бизнеса, ущерб, нанесённый репутации и т.д.

Эти действия определяют ущерб для организации или последствия для организации, которые могут быть обусловлены сценарием инцидента. Сценарий инцидента – это описание угрозы, которая использует определённую уязвимость или набор уязвимостей в случае инцидента информационной безопасности (O‘z DSt ISO/IEC 27002, раздел 13).

Воздействие сценариев инцидентов следует определять, используя критерии воздействия, определённые в процессе деятельности, связанной с установлением контекста. Оно может затронуть один или большее количество активов или часть актива. Поэтому активам может назначаться ценность в зависимости от их финансовой стоимости и последствий для бизнеса в случае их порчи или компрометации. Последствия могут быть временными или постоянными, как в случае разрушения активов.

Примечание - Происхождение сценариев инцидентов, как «недостатков безопасности», приведено в O‘z DSt ISO/IEC 27001.

Организации должны определять практические последствия сценариев инцидентов на основе (но не ограничиваясь):

- времени на расследование и восстановление;
- потери (рабочего) времени;
- упущенной возможности;
- охраны труда и безопасности;
- финансовых затрат на специфические навыки, необходимые для устранения неисправности;
- репутации и престижа.

1.3 Анализ рисков

1.3.1 Методологии анализа рисков

Анализ рисков может быть осуществлён с различной степенью детализации в зависимости от критичности активов, распространённости

известных уязвимостей и предыдущих инцидентов, касавшихся организации. Методология анализа рисков может быть качественной или количественной, или их комбинацией в зависимости от обстоятельств. На практике чаще вначале используется качественная оценка для получения общих сведений об уровне риска и выявления основных рисков. Позднее может возникнуть необходимость в осуществлении более специфичного или количественного анализа основных рисков, поскольку обычно выполнение качественного анализа по сравнению с количественным является менее сложным и менее затратным.

Форма анализа должна согласовываться с критериями оценки риска, разработанными как часть установления контекста. Далее подробно описываются методологии анализа:

a) качественный анализ риска. Качественный анализ использует шкалу квалификационных свойств для описания масштаба потенциальных последствий (например, «низкое», «среднее» и «высокое») и вероятности возникновения этих последствий. Преимущество качественного анализа заключается в простоте его понимания всем персоналом, имеющим к нему отношение, а недостатком является зависимость от субъективного выбора шкалы.

Такие шкалы могут быть адаптированы или скорректированы таким образом, чтобы удовлетворять обстоятельствам, а для разных рисков могут использоваться разные описания. Качественный анализ может использоваться:

- как предварительное рассмотрение деятельности по проверке для определения рисков, требующих более детального анализа;
- там, где этот вид анализа является соответствующим для принятия решения;
- там, где числовые данные или ресурсы являются неадекватными для количественного анализа рисков.

Качественный анализ должен использовать фактическую информацию и данные, где возможно;

b) количественный анализ риска. Количественный анализ риска использует шкалу с числовыми значениями (а не наглядные шкалы, используемые в качественном анализе) применительно к последствиям и вероятности, применяя данные из различных источников. Качество анализа зависит от точности и полноты числовых значений и от обоснованности используемых моделей. В большинстве случаев количественный анализ использует данные по инцидентам за прошлый период, преимущество которого заключается в том, что он может быть напрямую связан с целями

информационной безопасности и проблемами организации. Недостатком количественного анализа является нехватка таких данных по новым рискам или по проблемам информационной безопасности. Недостатки количественного анализа могут иметь место тогда, когда фактические проверяемые данные недоступны, поэтому создаётся иллюзия ценности и точности определения риска.

Способ выражения последствий и вероятности и способы их объединения для обеспечения сведений об уровне риска изменяются в соответствии с типом риска и целью, для которой должны использоваться выходные данные определения риска. Неопределённость и изменяемость последствий и вероятности следует учитывать при анализе и сообщать о них эффективным образом.

1.3.2 Определения последствий

После определения всех пересматриваемых активов, ценность, присвоенная этим активам, должна учитываться при оценке последствий.

Значение влияния бизнеса может быть выражено в качественной или количественной формах, однако, любой метод присвоения денежного значения может, в общем, дать больше информации для принятия решений и, следовательно, сделает возможным более эффективный процесс принятия решений.

Определение ценности активов начинается с определения активов в соответствии с их критичностью относительно важности активов для осуществления бизнес-целей организации. Затем определяется ценность с использованием двух мер:

- восстановительной стоимости актива: стоимости очистки с целью восстановления и замены информации (если это возможно);
- последствий для бизнеса от ущерба или компрометации актива, например, возможные неблагоприятные последствия для бизнеса вследствие раскрытия, модификации, недоступности и/или разрушения информации и других информационных активов из-за невыполнения требований законодательных или нормативных актов.

Определение ценности может быть установлено из анализа влияния на бизнес. Ценность определяется последствиями для бизнеса, обычно значительно выше просто восстановительной стоимости и зависит от важности актива для организации при выполнении её бизнес-целей.

Оценивание активов является ключевым фактором оценки влияния сценария инцидента, поскольку инцидент может воздействовать более чем на один актив (например, зависимые активы) или только на часть актива.

Различные угрозы и уязвимости могут иметь различное воздействие на активы, например, потеря конфиденциальности, целостности и доступности. В связи с этим оценка последствий является связанной с определением ценности активов или делается исходя из анализа влияния на бизнес.

Последствия или влияние бизнеса могут определяться путём моделирования результатов события или набора событий, или экстраполяции экспериментальных исследований или данных за прошедший период.

Последствия могут иметь денежное выражение, могут быть выражены техническими или человеческими критериями воздействия, или другими критериями, значимыми для организации. В отдельных случаях для определения последствий, связанных с различным временем, местами, группами или ситуациями, требуется больше чем одно цифровое значение.

Последствия, связанные со временем или финансами, должны измеряться посредством того же подхода, который используется в отношении вероятности угрозы и уязвимости. Должна поддерживаться последовательность количественного или качественного подхода.

1.3.3 Определение вероятности инцидента

После определения сценариев инцидентов необходимо оценить вероятность каждого сценария и возникающее воздействие, используя качественные или количественные методы оценки. Здесь нужно учитывать тот факт, как часто возникают угрозы и насколько легко могут быть использованы уязвимости, рассматривая:

- опыт и применимую статистику вероятности угроз;
- мотивацию и возможности, которые будут меняться с течением времени, и доступные для потенциальных нарушителей ресурсы, а также ощущение привлекательности и уязвимости активов потенциальным нарушителем - для источников умышленных угроз;
- географические факторы, например, близость к химическому или нефтеперерабатывающему заводу, возможность экстремальных погодных условий и факторы, которые могут оказывать влияние на ошибки персонала и сбои оборудования - для источников случайных угроз;
- отдельные уязвимости и их совокупность;
- существующие средства управления и то, отдельные уязвимости и их совокупность.

Например, у информационной системы может быть уязвимость к угрозам маскарадинг личности пользователя и злоупотреблению ресурсами. Уязвимость, связанная с маскарадингом личности пользователя, может быть высокой из-за отсутствия аутентификации пользователей. С другой стороны,

вероятность злоупотребления ресурсами может быть низкой несмотря на отсутствие аутентификации пользователей, потому что способы злоупотребления ресурсами ограничены.

В зависимости от того, требуется ли точность, активы могут быть сгруппированы или может возникать необходимость разбиения активов на элементы и связывания сценариев с элементами. Например, для географических местоположений характер угроз одним и тем же типам активов может меняться или может различаться эффективность существующих средств управления.

1.3.4 Уровень определения рисков

При анализе риска присваиваются значения вероятности и последствиям риска. Эти значения могут быть качественными или количественными. Анализ риска основывается на оценённых последствиях и вероятности. Дополнительно он может учитывать стоимостные преимущества, заинтересованность причастных сторон и другие переменные, необходимые при оценивании риска. Измеренный риск является комбинацией вероятности сценария инцидента и его последствий.

1.4 Оценка рисков

Характер решений, относящихся к оценке рисков, и критерии оценки рисков, которые будут использованы для принятия этих решений, должны были быть определены при установлении контекста. Эти решения и контекст должны быть более детально пересмотрены на данном этапе при наличии дополнительной информации о конкретных определенных рисках. Для оценки рисков организации должны сравнивать измеренные риски (используя выбранные методы или подходы, рассматриваемые в приложении Е) с критериями оценки рисков, выбранными на этапе установления контекста.

Критерии оценки рисков, используемые для принятия решений, должны согласовываться с определённым внешним и внутренним контекстом управления рисками информационной безопасности и принимать в расчёт цели организации, мнения заинтересованных сторон и т.д. Решения, связанные с оценкой рисков, обычно основываются на приемлемом уровне рисков. Однако последствия, вероятность, степень уверенности в идентификации и анализе рисков должны быть также учтены. Совокупность множества рисков низкого и среднего уровня может дать в итоге общий риск более высокого уровня.

При этом следует учесть следующее:

- свойства информационной безопасности: если один критерий неактуален для организации (например, потеря конфиденциальности), то все риски, влияющие на этот критерий, могут быть также неактуальными;
- значимость бизнес-процессов или деятельности, поддерживаемых конкретным активом или совокупностью активов: если процесс определён как имеющий низкую значимость, связанные с ним риски должны рассматриваться в меньшей степени, чем риски, влияющие на более важные процессы или действия.

Оценка рисков основывается на понимании сути рисков, полученном на этапе анализа рисков, для принятия решений о будущих действиях.
Решения должны включать в себя следующее:

- должна ли быть предприняты какие-либо действия;
- приоритеты при обработке риска, учитывающие измеренные уровни рисков.

2 Обработка рисков информационной безопасности

2.1 Общее описание обработки рисков

Для обработки рисков имеется четыре варианта: модификация рисков (2.2), сохранение рисков (2.3), предотвращение рисков (2.4) и распределение рисков (2.5).

На рисунке 3 показаны мероприятия по обработке рисков в рамках процесса управления рисками информационной безопасности.

Высокоуровневое представление процесса управления рисками определено в ISO 31000 [3] и показано на рисунке 1.

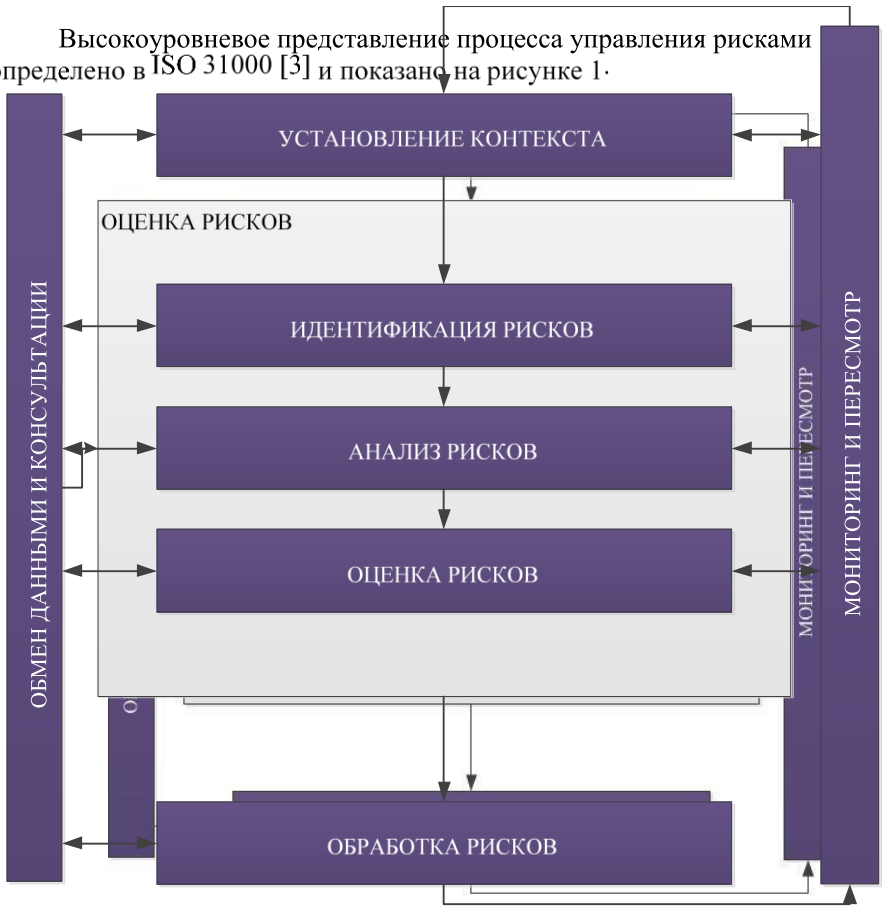

Рисунок 1 – Процесс управления рисками

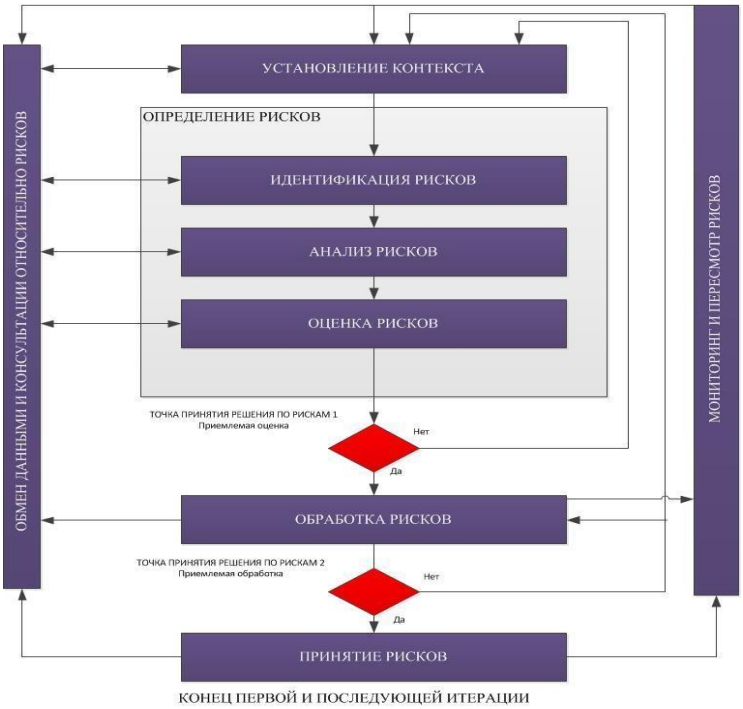

Рисунок 2 – Иллюстрация процесса управления рисками информационной безопасности

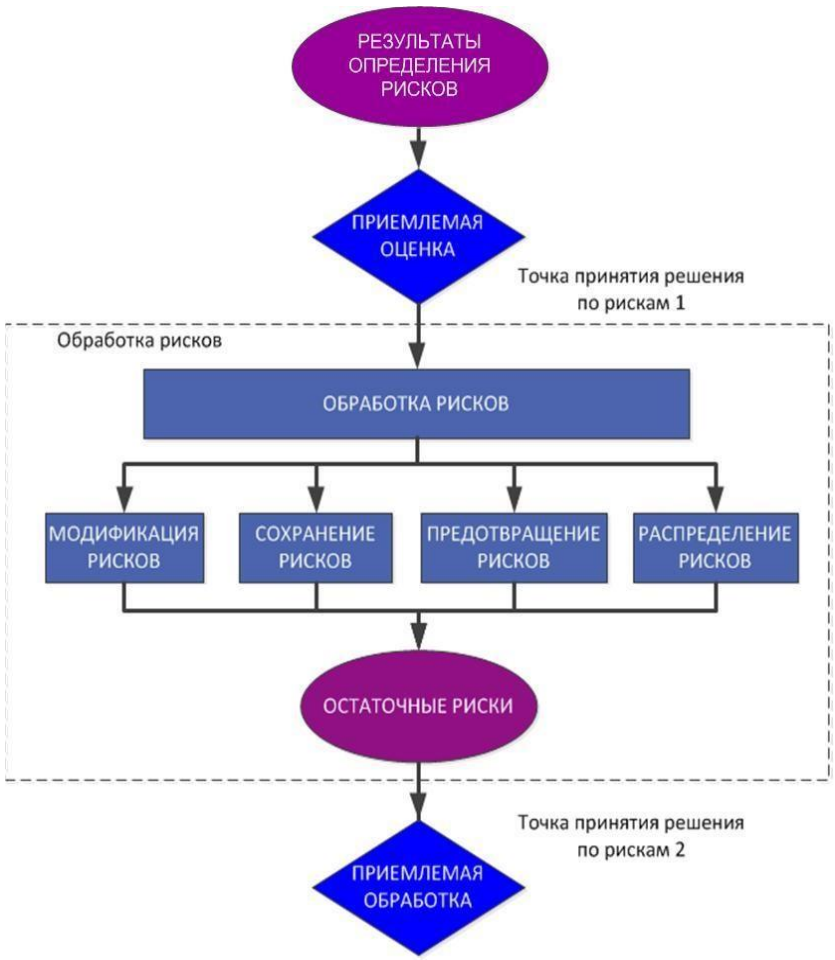

Рисунок 3 – Мероприятия по обработке риска

Варианты обработки риска должны выбираться на основе результатов определения риска, ожидаемой стоимости реализации этих вариантов и ожидаемой выгоды от этих вариантов.

Когда значительное снижение рисков может быть достигнуто при относительно небольших затратах, такие варианты должны реализовываться. Дальнейшие варианты улучшений могут быть неэкономичными и решение по их реализации должно быть изучено на предмет того, являются ли они оправданными.

В целом, неблагоприятные последствия рисков необходимо снижать до разумных пределов и независимо от каких-либо абсолютных критериев. Руководство должно рассматривать редкие, но серьёзные риски. В таких случаях может возникнуть необходимость реализации средств управления, которые являются необоснованными по строго экономическим причинам (например, средства управления непрерывностью бизнеса, рассматриваемые для охвата специфических высоких рисков).

Четыре варианта обработки рисков не являются взаимоисключающими. Иногда организация может получить значительную выгоду от объединения

вариантов, таких как снижение вероятности рисков, уменьшение их последствий и распределение или сохранение любых остаточных рисков.

Некоторые виды обработки рисков могут быть эффективными в отношении более чем одного риска (например, обучение и осведомлённость в части информационной безопасности). План обработки рисков должен чётко определять порядок приоритетов и временные рамки, при помощи которых должна реализовываться обработка отдельных рисков. Порядок приоритетов может устанавливаться с использованием различных методов, включая ранжирование рисков и анализ «затраты выгоды». В обязанности руководства входит принятие решения о балансе между затратами на реализацию средств управления и бюджетными отчислениями.

Определение существующих средств управления может обуславливать те существующие средства управления, которые превышают текущую потребность с точки зрения затрат, включая их поддержку. Если рассматривается удаление избыточных или ненужных средств управления (особенно, если расходы на поддержку этих средств управления велики), должны приниматься во внимание факторы информационной безопасности и стоимости. Поскольку средства управления оказывают влияние друг на друга, удаление избыточных средств управления может в итоге снизить эффективность использования всех оставшихся средств обеспечения безопасности. Кроме того, может быть дешевле оставить избыточные или ненужные средства управления, чем удалить их.

Варианты обработки риска должны учитывать:

- как риск осознается затрагиваемыми сторонами;
- наиболее соответствующие пути коммуникации с этими сторонами.

Установление контекста даёт информацию о правовых и регулирующих требованиях, которые организация должна соблюдать. Для организаций является риском несоблюдение указанных требований, в этой связи должны быть реализованы варианты обработки для ограничения этой возможности. Все ограничения - организационные, технические, структурные и др., которые определяются в процессе мероприятий, связанных с установлением контекста, следует принимать во внимание при обработке рисков.

После того как был определён план обработки рисков, необходимо определить остаточные риски. Это включает обновление или повторную операцию определения рисков, принимая во внимание ожидаемый эффект от предполагаемой обработки рисков. Если остаточные риски попрежнему не будут удовлетворять критериям принятия рисков организации, может возникнуть необходимость дальнейшей итерации обработки рисков, прежде чем перейти к принятию рисков.

2.2 Модификация рисков

Должны быть выбраны соответствующие и обоснованные средства управления для того, чтобы удовлетворять требованиям, определенным с помощью определения рисков и процесса обработки рисков. Такой выбор должен учитывать критерии принятия рисков, а также правовые, регулирующие и договорные требования. Этот выбор должен также учитывать стоимость и время для реализации средств управления, технические, культурные аспекты и аспекты среды. Зачастую можно снизить общие расходы на владение системой с помощью соответствующим образом выбранных средств управления информационной безопасностью.

В целом, средства управления могут обеспечивать один или несколько из следующих видов защиты: коррекция, устранение, предупреждение, уменьшение воздействия, сдерживание, обнаружение, восстановление, мониторинг и информированность. Во время выбора средств управления важно сравнивать стоимость приобретения, реализации, администрирования, функционирования, мониторинга и поддержки средств управления по отношению к ценности защищаемых активов. Кроме того необходимо учитывать рентабельность инвестиций с точки зрения снижения рисков и потенциал для использования новых деловых возможностей, предоставляемых определёнными средствами управления. Дополнительно следует обратить внимание на специализированные навыки, которые могут потребоваться для определения и реализации новых средств управления или модификации существующих.

В O‘z DSt ISO/IEC 27002 даётся подробная информация по выбору средств управления.

Существует много ограничений, влияющих на выбор средств управления. Технические ограничения, такие как требования к производительности, вопросы управляемости (требования эксплуатационной поддержки) и совместимости могут препятствовать использованию определённых средств управления или могут стимулировать человеческий фактор, аннулируя средство управления, вызывая ложное чувство безопасности или даже увеличивая риск не обладания никаким средством управления (например, требование по использованию сложных паролей без соответствующего обучения, что может привести к записи паролей пользователями). Более того, может произойти так, что средства управления будут влиять на производительность. Руководство должно работать над нахождением решения, которое удовлетворяет требованиям производительности и в то же время гарантирует достаточную информационную безопасность. Результатом этого шага является перечень

возможных средств управления с их стоимостью, выгодой и приоритетом реализации.

При выборе средств управления и в процессе их реализации должны приниматься в расчёт различные ограничения. Типичными ограничениями считаются:

- временные ограничения;
- финансовые ограничения;
- технические ограничения;
- эксплуатационные ограничения;
- культурные ограничения;
- этические ограничения;
- ограничения, связанные с окружающей средой;
- правовые ограничения;
- простота использования;
- кадровые ограничения;
- ограничения, касающиеся интеграции новых и существующих средств управления.

2.3 Сохранение рисков

Решение сохранить риск, не предпринимая дальнейших действий, следует принимать в зависимости от оценки риска. Если уровень риска соответствует критериям принятия риска, то нет необходимости реализовывать дополнительные средства управления и риск может быть сохранен.

2.4 Предотвращение рисков

Когда определенные риски считаются слишком высокими или расходы на реализацию других вариантов обработки рисков превышают выгоду, может быть принято решение о полном предотвращении рисков путём аннулирования запланированных или существующих действий, или совокупности действий или изменения условий, при которых проводятся эти действия. Например, в отношении рисков, вызываемых природными факторами, наиболее экономически выгодной альтернативой может быть физическое перемещение средств обработки информации туда, где эти риски не существуют или находятся под контролем.

2.5 Распределение рисков

Распределение рисков включает в себя решение разделить определённые риски с внешними сторонами. Распределение рисков может

создавать новые риски или модифицировать существующие определенные риски. Поэтому может быть необходима дополнительная обработка рисков.

Распределение может быть осуществлено посредством страхования последствий или с помощью заключения договора субподряда с партнёром, чья роль будет заключаться в проведении мониторинга информационной системы и осуществлении немедленных действий по прекращению инцидента, прежде чем он приведёт к определённому уровню ущерба.

Следует отметить, что возможно распределение ответственности по управлению рисками, но обычно невозможно распределять ответственность за воздействие. При неблагоприятном воздействии клиенты обычно считают виноватой организацию.

3 Принятие рисков информационной безопасности

Планы обработки рисков должны описывать то, как обрабатываются оцененные риски в соответствии с критериями принятия рисков. Важно, чтобы ответственные из числа руководства пересматривали и поддерживали предлагаемые планы обработки рисков и вытекающие из них остаточные риски, а также регистрировали все условия, связанные с поддержкой принятых решений.

Критерии принятия рисков могут быть более многогранным аспектом, чем просто определение того, находятся ли остаточные риски выше или ниже единого порогового значения.

В некоторых случаях уровень остаточных рисков может не соответствовать критериям принятия рисков, поскольку применяемые критерии не учитывают превалирующие обстоятельства. Например, может быть доказано, что необходимо принимать риски по причине привлекательности выгод, связанных с ними, или потому что расходы, связанные со снижением рисков, очень высоки. Такие обстоятельства показывают, что критерии принятия рисков являются неадекватными и должны быть по возможности пересмотрены. Однако не всегда возможно пересмотреть критерии принятия рисков своевременно. В таких случаях лицам, принимающим решения, возможно придется принять риски, которые не соответствуют стандартным критериям принятия. Если это необходимо, лицо, принимающее решение, должно явным образом прокомментировать риски и включить обоснование для решения, превышающего стандартный критерий принятия рисков.

4 Обмен данными и консультации относительно рисков информационной безопасности

Обмен данными относительно рисков представляет собой деятельность, связанную с достижением соглашения о том, как осуществлять управление рисками путём обмена и/или совместного использования данных о рисках между лицами, принимающими решения, и другими заинтересованными сторонами. Данная информация включает данные о наличии, характере, форме, вероятности, серьёзности, обработке и приемлемости рисков, а также другие необходимые данные. Эффективный обмен данными между заинтересованными сторонами имеет большое значение, поскольку он может оказывать существенное влияние на решения, которые должны быть приняты. Обмен данными будет обеспечивать уверенность в том, что лица, отвечающие за управление рисками, и лица, имеющие законный интерес, понимают основу, на которой принимаются решения, и необходимость определённых действий. Обмен данными относительно рисков является двунаправленным.

Восприятие рисков может варьироваться в зависимости от различий в предпосылках, понятиях и потребностях, вопросов и озабоченности заинтересованных сторон, которые связаны с рисками или обсуждаемыми проблемами. Заинтересованные стороны, вероятно, выносят суждения о принятии рисков на основе своего восприятия. Поэтому очень важно, чтобы восприятие рисков и выгод заинтересованными сторонами могло быть определено и задокументировано, а лежащие в основе причины были чётко поняты и учтены.

Обмен данными относительно рисков должен осуществляться с целью достижения следующего:

- обеспечение доверия к результатам управления рисками организации;
- сбор данных о рисках;
- совместное использование результатов определение рисков и представление плана обработки рисков;
- предотвращение или снижение возникновения и последствий нарушений информационной безопасности из-за отсутствия взаимопонимания между принимающими решения лицами и заинтересованными сторонами;
- поддержка принятия решений;
- получение новых знаний в области информационной безопасности;

- координация с другими сторонами и планирование реагирования для уменьшения последствий какого-либо инцидента;
- выработка чувства ответственности по отношению к рискам у лиц, принимающих решения, и заинтересованных сторон; - повышение осведомлённости.

Организация должна разрабатывать планы обмена данными относительно рисков как для обычного функционирования, так и для чрезвычайных ситуаций. Следовательно, деятельность по обмену данными должна выполняться непрерывно.

Координация лиц, принимающих окончательные решения, и иных заинтересованных сторон может быть достигнута посредством формирования соответствующего комитета, где могут проходить обсуждения вопросов о рисках, их приоритетах и выработке решений по обработке и принятию рисков.

Важно сотрудничать с соответствующим отделом по связям с общественностью или коммуникациям в организации, чтобы координировать все задачи, связанные с обменом данными относительно рисков. Это критически важно в кризисных ситуациях, например, при реагировании на определённые инциденты.

5 Мониторинг и повторный анализ рисков информационной безопасности

5.1 Мониторинг и повторный анализ факторов рисков

Вся информация о рисках, полученная в результате действий по управлению рисками (рисунок 2).

Риски и их факторы (т.е. ценность активов, воздействия, угрозы, уязвимости, вероятность возникновения) должны подвергаться мониторингу и пересмотру с целью определения любых изменений в контексте организации на ранней стадии и пересмотра всей картины риска.

Риски не статичны. Угрозы, уязвимости, вероятность или последствия могут изменяться неожиданно, без каких-либо признаков, поэтому для обнаружения таких изменений необходим непрерывный мониторинг. Это может быть организовано с использованием внешних сервисов, которые предоставляют информацию о новых угрозах или уязвимостях.

Организации должны быть уверены в проведении непрерывного мониторинга следующих факторов:

- новые активы, которые были включены в область действия управления рисками;
- необходимая модификация ценности активов, например, вследствие изменившихся деловых требований;

- новые угрозы, которые могут быть активными вне и внутри организации, и вследствие этого ещё не оцененные;
- вероятность того, что новые или увеличившиеся уязвимости могут способствовать реализации угроз посредством этих уязвимостей;
- идентифицированные уязвимости для определения тех, которые становятся подверженными новым или повторно возникающим угрозам;
- неприемлемый уровень риска следует из объединения повышенного воздействия или последствия оценённых угроз, уязвимостей и рисков;
- инциденты информационной безопасности.

Новые угрозы, уязвимости или изменения в вероятности или последствиях могут влиять на увеличение уровня рисков, которые ранее были оценены как низкие. Процесс пересмотра низких и принятых рисков должен рассматривать каждый риск отдельно, а также все эти риски как совокупное целое, чтобы оценивать их потенциальное суммарное воздействие. Если риски не попадают в категорию низких или приемлемых рисков, они должны обрабатываться с использованием одного или нескольких вариантов, рассмотренных в разделе 2.

Факторы, влияющие на вероятность и последствия существующих угроз, могут изменяться, как могут изменяться факторы, влияющие на применимость или стоимость различных вариантов обработки. Главные изменения, влияющие на организацию, должны служить основанием для более специфического пересмотра. Следовательно, мероприятия по мониторингу рисков должны регулярно повторяться и выбранные варианты обработки рисков должны периодически пересматриваться.

Результаты мероприятий по мониторингу рисков могут быть входными данными к другим мероприятиям по пересмотру рисков. Организация должна пересматривать все риски регулярно, а также в случае значительных изменений в соответствии с O‘z DSt ISO/IEC 27001.

5.2 Мониторинг, пересмотр и улучшение процессов управления рисками

Вся информация о рисках, полученная в результате действий по управлению рисками (рисунок 2).

Процесс управления рисками информационной безопасности должен постоянно подвергаться мониторингу, пересмотру и улучшению соответствующим образом.

Постоянный мониторинг и пересмотр необходимы для обеспечения уверенности в том, что контекст, результат определения рисков и обработки

рисков, а также планы по управлению остаются уместными и соответствующими обстоятельствам.

Организация должна быть уверена в том, что процесс управления рисками информационной безопасности и связанные с ним действия остаются соответствующими при текущих обстоятельствах и соблюдаются. Руководство должно быть уведомлено о любых согласованных улучшениях процесса или действиях, необходимых для улучшения соответствия процессу, чтобы обеспечить уверенность в том, что не существует ни одного риска или элемента риска, упущенного или недооценённого и что необходимые действия и решения, предпринимаются для получения реалистичного представления о рисках и способности реагировать на них.

Кроме того, организация должна регулярно проверять, что критерии, используемые для измерения рисков и его элементов, по-прежнему остаются действительными и согласуются с деловыми целями, стратегиями и политиками и что изменения делового контекста принимается во внимание на адекватном уровне во время процесса управления рисками информационной безопасности. Мониторинг и пересмотр должен быть направлен (но не ограничиваться) на следующее:

- правовой контекст и контекст окружающей среды;
- контекст конкуренции;
- подход к определению рисков;
- ценность и категории активов;
- критерии воздействия;
- критерии оценивания рисков;
- критерии принятия рисков;
- полную стоимость владения активами; - необходимые ресурсы.

Организация должна быть уверена в том, что ресурсы определения и обработки рисков были постоянно доступны для пересмотра рисков, рассмотрения новых или изменившихся угроз или уязвимостей и соответствующего уведомления руководства.

Результатами мониторинга управления рисками может быть модификация или дополнение подхода, методологии или инструментальных средств, используемых в зависимости от следующего:

- определенных изменений;
- итерации определения рисков;
- цели процесса управления рисками информационной безопасности (например, непрерывность бизнеса, устойчивость к инцидентам, совместимость);

- объекта процесса управления рисками информационной безопасности (например, организация, бизнес-подразделение, информационный процесс, его техническая реализация, приложение, подключение к сети Интернет).

Постоянная актуальность процесса управления рисками информационной безопасности для деловых целей организации.

6. Сведения о системе управления рисками, используемой Платежной организацией

6.1. Под системой управления рисками в Платежной организации понимается комплекс мероприятий, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков для обеспечения финансовой устойчивости, и стабильного функционирования. Для эффективного управления рисками Платежная организация разработала политику управления рисками, которая состоит из:

- выявление, измерение, контроль и мониторинг рисков;
- оценка эффективности их применения;
- контроль за совершением всех денежных операций;
- разработка и практическая реализация мер по предотвращению и минимизации рисков.

6.2. Основная задача регулирования рисков в Платежной организации — это поддержание приемлемых соотношений прибыльности с показателями безопасности и ликвидности в процессе управления активами и пассивами Платежной организации, т.е. минимизация потерь. Процесс управления рисками в Платежной организации включает в себя:

- предвидение рисков, определение их вероятных размеров и последствий;
- разработка и реализация мероприятий по предотвращению или минимизации связанных с ними потерь.

6.3. Все это предполагает разработку собственной стратегии управления рисками таким образом, чтобы своевременно и последовательно использовать все возможности развития Платежной организации и одновременно удерживать риски на приемлемом и управляемом уровне.

6.4. Система управления рисками характеризуется такими элементами как мероприятия и способы управления. Мероприятия по управлению рисками включают в себя: определение организационной структуры управления рисками, обеспечивающей контроль за выполнением агентами и субагентами Платежной организации требований к управлению рисками, установленных правилами управления рисками Платежной организации; доведение до органов управления Платежной организации

соответствующей информации о рисках; определение показателей и порядка обеспечения бесперебойности функционирования Платежной организации; определение методик анализа рисков; определение порядка обмена информацией, необходимой для управления рисками; определения порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур; определение порядка обеспечения защиты информации в Платежной организации.

6.5. Требования, предъявляемые к хранению информации о реквизитах картах и об операциях, совершенных с их использованием. Организация обязана обеспечить соблюдение следующих основных требований, предъявляемых к хранению информации о реквизитах карт и об операциях, совершенных с их использованием:

- Не хранить ни при каких обстоятельствах:

Полное содержание любой из дорожек магнитной полосы, находящейся на обратной стороне карты; Card validation code – 3-х-значное число, напечатанное на панели для подписи, расположенной на карте;

- Хранить только ту часть информации о карте, которая существенна для бизнеса (т.е имя держателя карты, номер карты, срок действия карты).
- Обеспечить защиту хранящейся в Организации информации о реквизитах карт и об операциях, совершенных с их использованием в соответствии с требованиями PCI DSS (Payment Card Industry Data Security Standart).
- Хранить все материалы, содержащие информацию о реквизитах картах и об операциях, совершенных с их использованием в безопасном месте, доступ к которому имеют только уполномоченные лица.
- Уничтожить или очистить все носители информации, содержащие устаревшие данные об операциях, совершенных с использованием карт.

6.6. Управления рисками в Платежной организации определяются такими способами как управление очередностью исполнения распоряжений должностными лицами; осуществление расчета, в пределах, предоставленных агентами Платежной организации денежных средств; осуществление расчетов в Платежной организации до конца рабочего дня; обеспечение