КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Руководитель Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019г.

М. П.

Методика оценки рисков информационной безопасности Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.МР.02.r01.19

г. Алматы
2019 г.

1. Область применения

Целью настоящего документа является описание методики оценки рисков информационной безопасности, и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Политика информационной безопасности ИС основывается на данных полученных в результате инвентаризации, классификации активов, анализа и оценки рисков информационной безопасности.

С целью совершенствования политики информационной безопасности информационных ИС, проводится ежегодный анализ и оценка рисков информационной безопасности.

Анализ и оценка рисков проводится в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 27002, СТ РК ISO/IEC 27005, СТ РК ИСО/МЭК 31010.

Пересмотр и переоценка рисков производится один раз в год.

При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое состояние. Ценность принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

Процесс определения ценности информации и ее потребности в защите является частью общего процесса классификации активов.

Для оценки ценности и критичности информации применяется метод экспертных оценок.

Настоящий документ содержит:

1) выбор методики оценки рисков, выполнение идентификации рисков;

2) описание методов по определению ценности и критичности информации;

3) описание порядка мониторинга, пересмотра и изменения рисков ИБ;

4) описание методов и последовательности по определению рисков информационной безопасности объекта аттестации;

5) описание метода и последовательности оценки выявленных рисков;

6) описание метода по обработке рисков;

7) описание метода и анализа угроз информационной безопасности и источники;

8) описание метода определения вероятности инцидента;

9) описание порядка обработки рисков с учетом корректировки, сохранение, избежание, разделение;

10) описание требований к периодичности пересмотра и переоценки рисков;

11) определение и оценку последствий в случае реализации риска;

12) определение ответственных лиц за ведение и обработку рисков;

13) описание порядка составления карты рисков;

14) описание порядка формирования плана обработки рисков по результатам оценки и анализа рисков.

5. Порядок обработки рисков с учетом корректировки, сохранения, избежания, разделения

На рисунке 1 иллюстрируется деятельность по обработке риска в рамках процесса менеджмента риска ИБ.

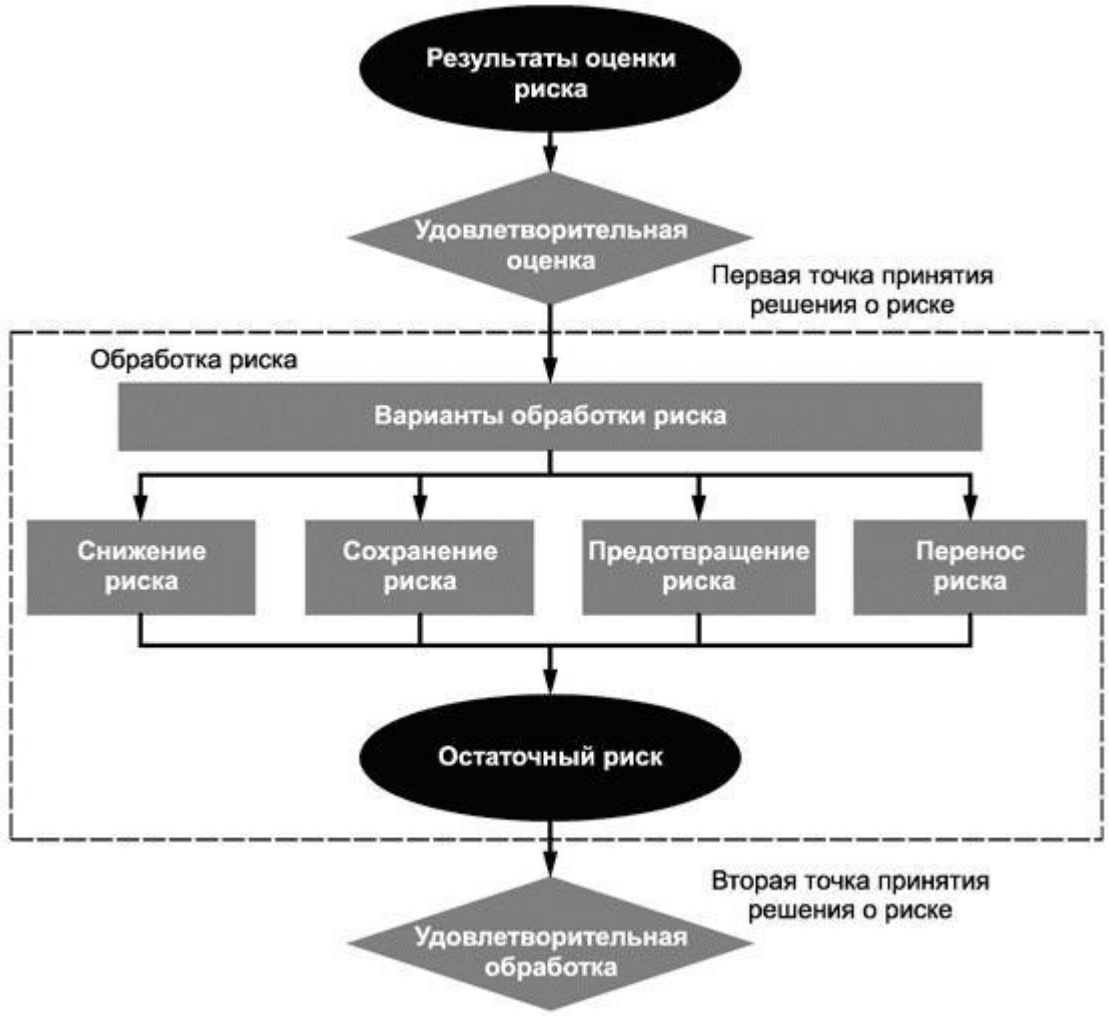

Рисунок 1. Порядок обработки рисков

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности.

Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Дополнительные варианты повышения эффективности могут быть неэкономичными, и необходимо принимать решение о целесообразности их применения.

Неблагоприятные последствия рисков необходимо снижать до разумных пределов независимо от каких-либо абсолютных критериев. Редкие, но серьезные риски должны рассматриваться руководством. В таких случаях может возникнуть необходимость реализации мер и средств контроля и управления, которые являются необоснованными по причинам затратности (например, меры и средства контроля и управления непрерывности бизнеса, для охвата высоких специфических рисков).

Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких, как снижение вероятности риска, уменьшение последствий и перенос или сохранение любого остаточного риска.

Некоторые варианты обработки риска могут быть эффективными для более чем одного риска (например, обучение и осведомленность в части ИБ). План обработки риска должен четко определять порядок приоритетов, при соблюдении которого должна реализовываться обработка отдельного риска. 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 мер и средств контроля и управления и бюджетными отчислениями.

При определении существующих мер и средств контроля и управления может быть установлено, что существующие меры и средства контроля и управления превышают текущую потребность в показателях сравнения затрат, включая поддержку. В случае удаления избыточных или ненужных мер и средств контроля и управления (особенно, если расходы на их поддержку велики) должны учитываться факторы ИБ и стоимости. Поскольку меры и средства контроля и управления оказывают влияние друг на друга, удаление избыточных мер и средств контроля и управления может в итоге снизить эффективность использования всех оставшихся мер и средств обеспечения безопасности. Кроме того, может быть менее затратным оставить избыточные или ненужные средства контроля, чем удалить их.

Установление контекста предоставляет информацию о законодательных и нормативных требованиях, которым необходимо следовать организации. Отказ от следования указанным требованиям является риском для организаций, поэтому должны быть рассмотрены варианты решений, ограничивающие эту возможность. Все ограничения - организационные, технические, структурные и др., которые определяются в течение деятельности, связанной с установлением контекста, следует учитывать в течение обработки риска.

После уточнения плана обработки риска необходимо определить остаточные риски. Это включает обновление или повторную операцию оценки риска с учетом ожидаемого эффекта от предполагаемой обработки риска. Если остаточные риски по-прежнему не будут удовлетворять критериям принятия риска организации, может возникнуть необходимость в дополнительной итерации обработки риска, прежде чем перейти к принятию риска.

a. Снижение риска

Должны быть выбраны соответствующие и обоснованные меры и средства контроля и управления, чтобы удовлетворять требованиям, определенным путем оценки и обработки рисков. Такой выбор должен учитывать критерии принятия рисков, а также законодательные, нормативные и договорные требования. При выборе должны также учитываться стоимость и время реализации мер и средств контроля и управления или технические аспекты, аспекты среды и культурные аспекты. С помощью соответствующим образом выбранных мер и средств

контроля безопасности зачастую можно снизить общие расходы владельца системы.

В целом меры и средства контроля и управления могут обеспечивать один или несколько из перечисленных видов защиты: исправление, исключение, предупреждение, уменьшение влияния, сдерживание, обнаружение, восстановление, мониторинг и информированность. Во время выбора мер и средств контроля и управления важно установить баланс между стоимостью приобретения, реализации, администрирования, функционирования, мониторинга и поддержки мер и средств контроля и управления и ценностью защищаемых активов. Кроме того, необходимо учитывать рентабельность инвестиций с точки зрения снижения риска, и потенциал для использования новых возможностей бизнеса, предоставляемых определенными мерами и средствами контроля и управления. Дополнительно следует обратить внимание на специализированные навыки, которые могут потребоваться для определения и реализации новых мер и средств контроля и управления или модификации существующих.

b. Сохранение риска

Решение сохранить риск, не предпринимая дальнейшего действия, следует принимать в зависимости от оценки риска.

Если уровень риска соответствует критериям принятия риска, то нет необходимости реализовывать дополнительные меры и средства контроля и управления, и риск может быть сохранен.

c. Предотвращение (избежания) риска

Отказ от деятельности или условия, вызывающего конкретный риск.

Если идентифицированные риски считаются слишком высокими или расходы на реализацию других вариантов обработки риска превышают выгоду, может быть принято решение о полном предотвращении риска путем отказа от планируемой или существующей деятельности, или их совокупности, или изменения условий, при которых осуществляется деятельность. Например, в отношении рисков, вызываемых природными факторами, наиболее экономически выгодной альтернативой может быть физическое перемещение средств обработки информации туда, где этого риска не существует или он контролируется.

d. Перенос (разделения) риска

Риск должен быть перенесен на сторону, которая может наиболее эффективно осуществлять менеджмент конкретного риска, в зависимости от оценки риска.

Перенос риска включает в себя решение разделить определенные риски с внешними сторонами. Перенос риска может создавать новые риски или модифицировать существующие идентифицированные риски. Поэтому может быть необходима дополнительная обработка риска.

Перенос может быть осуществлен путем страхования, которое будет поддерживать последствия, или путем заключения договора субподряда с партнером, чья роль будет заключаться в проведении мониторинга

информационной системы и осуществлении незамедлительных действий по прекращению атаки, прежде чем она приведет к определенному уровню ущерба.

Следует заметить, что может быть возможным перенести ответственность за менеджмент риска, но, как правило, невозможно перенести ответственность за ущерб. Клиенты обычно воспринимают неблагоприятное влияние ущерба как ошибку организации.

6. Описание метода и анализа угроз

Под анализом угроз следует понимать выявление и количественную оценку связи между активом, источником угрозы и уязвимостью актива перед угрозой (Exposure Factor, EF).

Для анализа угроз применяется метод экспертных оценок. В качестве экспертов выступает ответственный за обеспечение ИБ и системные администраторы ИС.

Эксперты, принимая во внимание текущее состояние защиты информации Проекта ИС, статистику Security Bulletins ведущих мировых производителей в области информационной безопасности и личный опыт выявляют и количественно оценивают связи между активом, источником угрозы и уязвимостью актива перед угрозой (Exposure Factor, EF).

После процесса инвентаризации и классификации всех активов Проекта ИС, ответственный за обеспечения ИБ проводит анализ существующих угроз ИС и составляет каталог угроз.

Для каждой угрозы в каталоге должно быть указано ее влияние на целостность, доступности и конфиденциальности информации ИС, источник угрозы (характеристика и потенциал нарушителя) и объект воздействия.

В качестве модели нарушителя (источник угроз) применяются следующие контрагенты:

- внутренний нарушитель с низким потенциалом;
- внутренний нарушитель со средним потенциалом;
- внутренний нарушитель с высоким потенциалом;
- внешний нарушитель с низким потенциалом;
- внешний нарушитель со средним потенциалом;
- внешний нарушитель с высоким потенциалом;
- природные явления.

а. Выбор методики оценки рисков, выполнение идентификации рисков

В качестве методики оценки рисков выбран метод экспертных оценок. Экспертное оценивание рисков — это процедура получения оценки на основе мнения специалистов (экспертов) с целью последующего принятия решения (выбора).

Обеспечение информационной безопасности это одна из ключевых задач современных ИС. Угрозу ИС могут представлять технические сбои, несогласованность данных в системах организации, безграничный доступ служащих к хранимой информации.

В своем понимании, риск — это возможность того, что произойдет какое-то негативное событие, имеющее свою оценку (размер возможного ущерба) и вероятность того, что он наступит.

Риск информационной безопасности (ИБ) представляет собой возможность нарушения ИБ с неблагоприятными последствиями для ИС. С методологической стороны верным подходом к решению проблем ИБ является обнаружение элементов информационных взаимоотношений и заинтересованности этих элементов, которые связаны с использованием информационных систем. Обратной стороной использования современных информационных технологий являются угрозы информационной безопасности организации.

Настоящая методика оценки рисков ИБ рассчитана для оценки автоматизированных ИС на соответствие требованиям и условиям нормативных документов. Целью настоящей методики ИБ является установление степени ИБ ИС по разным сферам контроля, которая выражена в численной форме, а также определение в наибольшей степени проблематичных областей со стороны информационной безопасности.

С учетом того, что оценка ИБ ИС представляет собой сложную научную задачу, которая требует принятия во внимание множества разных аспектов, то максимально подходящей методикой решения задачи оценки является использование методов многокритериальной оценки на основании иерархии признаков. Для создания общего рейтингового списка формируется единая шкала степеней информационной безопасности.

Данная методика оценки рисков информационной безопасности обладает комплексным характером, многофункциональна и приспособлена к разным видам объектов при организации информационной безопасности.

Например, если есть необходимость принимать во внимание более подробную информацию об определенных аппаратных, а также программных продуктах эксперт производит оценку влияния на многофункциональные области системы ИБ.

Для идентификации рисков применяется каталог угроз, разработанный «Государственным научно-исследовательским испытательным институтом проблем технической защиты информации. Федеральной службы по техническому и экспортному контролю» ФСТЭК России.

7. Описание метода определения вероятности инцидента (ARO)

Для определения вероятности инцидента применяется метод экспертных оценок. В качестве экспертов выступает ответственный за обеспечение ИБ и системные администраторы ИС.

Эксперты, принимая во внимание текущее состояние защиты информации Проекта ИС, статистику Security Bulletins ведущих мировых производителей в области информационной безопасности и личный опыт определяют для каждой угрозы вероятность ее реализации в течение года.

Оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая вероятность):

- низкая – не более трех раз в год;
- средняя – от четырех до восьми раз в год;
- высокая – девять и более раз в год;

При этом если оценки экспертов отличаются, то высчитывается средняя величина с округлением до целого в большую сторону.

Результаты оценки заносятся в таблицу предварительной оценки рисков.

8. Метод и последовательность по определению рисков

Для определения рисков применяется метод экспертных оценок. В качестве экспертов выступает ответственный за обеспечение ИБ и системные администраторы ИС. В качестве экспертов выступает ответственный за обеспечение ИБ и системные администраторы ИС.

Эксперты, принимая во внимание текущее состояние защиты информации Проекта ИС, статистику Security Bulletins ведущих мировых производителей в области информационной безопасности и личный опыт определяют риски информационной безопасности, как вероятность реализации угрозы в отношении активов ИС (Annual Rate of Occurrence, ARO).

Для каждого из идентифицированных рисков, следующих за оценкой рисков, принимается решение по обработке риска. Возможными вариантами решения для обработки риска могут быть:

a) применение подходящих мер контроля для уменьшения рисков;

b) сознательное и объективное принятие рисков при условии, что они соответствуют политике организации и критериям принятия рисков;

c) избежание рисков путём недопущения действий, вызывающих возникновение рисков;

d) передачу ассоциированных рисков другим сторонам.

Меры контроля выбираются с целью снижение рисков до приемлемого уровня, учитывая:

– требования и ограничения национальных и международных законодательств, и положений;

– организационные цели;

– эксплуатационные требования и ограничения;

– затраты на реализацию и эксплуатацию относительно снижаемых рисков и соответствия оставшихся рисков требованиям и ограничениям организации;

– необходимость сопоставления вложений в реализацию и эксплуатацию мер контроля с вероятным ущербом как следствием отказа в обеспечении безопасности.

Для управления рисками проводится инвентаризация, классификация активов и идентификация возможных угроз ИС.

Ответственный за обеспечение ИБ обязан составить и поддерживать в актуальном состоянии каталог угроз информационной безопасности ИС.

После проведения первичной оценки рисков, полученные значения подлежат систематизации по степени важности для выявления низких, средних и высоких рисков. Методика управления рисками подразумевает несколько способов действий.

Риск может принадлежать одной из категорий:

– низкий (low), т. е. руководство Организации согласно на риск и связанные с ним потери, поэтому работа информационной системы продолжается в обычном режиме;

– средний (middle) — с целью уменьшения величины риска будут приняты определенные меры;

– высокий (high) — риск очень высок и необходимо пересмотреть контрмеры для его уменьшения.

После ранжирования рисков определяются требующие первоочередного внимания; основным методом управления такими рисками является снижение, реже — передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа. Диапазон ранжирования рисков принимается исходя из проведенного расчета их качественных величин.

Таким образом, управление рисками сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Снижение величины риска достигается за счет уменьшения одной или нескольких составляющих (AV, EF, SLE) путем принятия определенных мер. В основном это возможно применительно к EF и SLE, так как AV (ценность актива) — фиксированный параметр.

Снижение параметра SLE, т. е. вероятности реализации угрозы, может быть достигнуто за счет технических или организационных мер.

Возникшие (оставшиеся) после применения методики управления риски называются остаточными.

Остаточные риски принимаются на усмотрение руководства Организации на основе карты рисков либо применяются дополнительные контрмеры по снижению рисков.

Обязанности по оценки рисков информационной безопасности возлагаются на ответственного за обеспечение ИБ.

Для установления пошаговой взаимозависимости между факторами воздействия (рисками) и вероятностью их реализации (с учетом аспектов уязвимости) должен использоваться утвержденный каталог угроз.

Для каждой угрозы в каталоге должно быть указано ее влияние на целостность, доступности и конфиденциальности информации ИС.

Последовательность определения рисков для активов ИС:

– определение ценности каждого актива с использованием классификаций в соответствии с требованиями Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

– определение консолидированной ценности активов ИС по отношению к угрозе;

– определение меры уязвимости ИС к угрозе;

– определение вероятности реализации выбранной угрозы по отношению к набору активов в течение года;

– определяется ожидаемый возможный ущерб от единичной реализации;

– определяются условные итоговые ожидаемые потери от конкретной угрозы за год.

Результаты расчетов заносятся в таблицу Предварительный перечень угроз, вероятность их реализации и оценка возможного ущерба ИС.

Далее подбираются меры снижения рисков от реализации угроз ИБ и повторно производится оценка и анализ рисков. Подбор и пересмотр мер обеспечения ИБ производится до тех пор, пока итоговые ожидаемые риски не перейдут в зеленую зону на карте рисков.

Если риски перешли в желтую зону, то решение принятия их остается за руководством Организации.

Следует отметить, что чем выше ранг угрозы в условиях существующих уязвимостей, тем выше вероятность возникновения риска, обусловленного данной угрозой, при этом необходимо опираться на перечень выявленных уязвимостей, соответствующих конкретной угрозе.

Такой метод позволяет сравнивать и ранжировать по приоритетности разные угрозы с различными воздействиями и вероятности возникновения угрозы.

Руководитель ИП и СОИБ, в случае если были выявлены максимальные риски, разрабатывает план обработки рисков, содержащий выбор оптимальных защитных мер, оценку их стоимости и эффективности, разработку предложений по принятию, избеганию или передачи части рисков. План обработки рисков предоставляется Директору ИП для рассмотрения и принятия соответствующих решений.

План обработки рисков разрабатывается согласно форме Приложения 3.

9. Описание метода по определению ценности и критичности информации

Обязанности по определению ценности информационных активов возлагаются на ответственного за обеспечение ИБ. Для оценки ценности информационных активов ИС применяется метод экспертных оценок. В качестве экспертов выступает ответственный за обеспечение ИБ и системные администраторы ИС.

Эксперты, принимая во внимание текущее состояние защиты информации Проекта ИС, статистику Security Bulletins ведущих мировых производителей в области информационной безопасности и личный опыт определяют ценность информации.

Ответственный за обеспечение ИБ используя классификацию информации, описанную в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации, подсчитывает баллы коэффициентов каждого информационного актива ИС.

Коэффициенты определяют ценность информации для Организации, и определения способов и методов ее защиты. В случае, если в рамках одной классификации информация принадлежит нескольким классам, баллы суммируются.

В рамках настоящей модели СМИБ информация рассматривается как актив (информационный актив) ИС. Критичность актива определяется методом экспертной оценки в соответствии с требованиями Правил идентификации, классификации и маркировки активов, связанных со средствами обработки информации и выражается в численном эквиваленте.

Результатом классификации относительной ценности актива является численная величина, получающаяся суммированием определенных классов актива.

Результаты суммирования баллов определяют ценность активов в следующих границах:

- низкая ценность актива: 0-9 баллов;
- средняя ценность актива: 10-19 баллов;
- высокая ценность актива: 20-30 баллов.

В виду многокомпонентности ИС, в настоящем документе применяется консолидированная ценность активов ИС (Consolidated Asset Value, CAV), определяемая как величина средней ценности активов ИС, подверженных выбранной угрозе, с округлением в большую сторону (см. 9. Расчет информационных рисков).

10. Расчет информационных рисков

Настоящим документом утверждается следующий способ расчета информационных рисков используемой ИС.

Формула представляет собой произведение трех параметров:

– ценность актива (Asset Value, AV). Указанная величина характеризует ценность актива. При качественной оценке рисков ценность актива чаще всего ранжируется в диапазоне от 1 до 3, где 1 — низкая ценность актива, 2 — средняя ценность актива и 3 — максимальная ценность актива;

– консолидированная ценность активов ИС по отношению к угрозе (Consolidated Asset Value, CAV). В виду многокомпонентности ИС в настоящем документе применяется консолидированная ценность активов ИС, определяемая как величина средней ценности активов ИС, подверженных выбранной угрозе, с округлением в большую сторону;

– мера уязвимости набора активов к угрозе (Exposure Factor, EF). Этот параметр показывает, в какой степени тот или иной набор активов уязвим по отношению к рассматриваемой угрозе. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 — минимальная мера уязвимости (слабое воздействие), 2 — средняя (актив подлежит восстановлению), 3 — максимальная (актив требует полной замены после реализации угрозы);

– оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь (уровень риска):

– оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы (Single Loss Exposure, SLE) рассчитывается по формуле:

индивидуально для каждого актива SLE = AV x EF;
для ИС в целом SLE = CAV x EF;

– итоговые ожидаемые потери от конкретной угрозы за определенный период времени (Annual Loss Exposure, ALE) характеризуют величину риска и рассчитывается по формуле:

ALE = SLE x ARO.

Таким образом, конечная формула расчета рисков представляет собой произведение:

индивидуально для каждого актива ALE = ((AV x EF = SLE) x ARO);
для ИС в целом ALE = ((CAV x EF = SLE) x ARO).

Полученные результаты излагаются в табличной форме.

Параметры AV (CAV), EF, SLE, ARO определяются на основе экспертной оценки ответственным сотрудником по обеспечению информационной безопасности.

Краткосрочный период оценки: 1 неделя.

Долгосрочный период оценки: 1 год.

11. Составление карты рисков

По результатам проведенных расчетов составляется карта рисков состоящая из:

- каталога угроз;
- предварительного перечня угроз, вероятность их реализации и оценка возможного ущерба ИС (до применения мер защиты);
- окончательного перечня угроз, вероятность их реализации и оценка возможного ущерба ИС (после применения мер защиты);
- мер информационной безопасности, применяемые для снижения существующих рисков до приемлемого уровня;
- графической интерпретации оценки рисков.

Критерии допустимости рисков

Настоящий документ утверждает критерии допустимости или недопустимости рисков, в соответствии с которыми будет приниматься решение о приемлемости риска.

Для этого задаются две границы, определяющие: уровень чрезмерного риска (или предельно допустимый уровень риска) и уровень пренебрежимого риска.

Весь спектр значений рисков этими двумя границами разбивается на три области (см. таблицу 1):

1. красная – область недопустимого (чрезмерного) риска – **риски ранга «В»** («высокие риски»), являются очень критичными для Предприятия. Таким рискам необходимо уделять максимум внимания, их предотвращению должны быть посвящены значительные усилия и средства, т.е. высокие риски требуют незамедлительного планирования и реализации корректирующих действий для его перевода в категорию приемлемого или пренебрежимого риска;

2. желтая – область приемлемого риска – **риски ранга «С»** («средние риски»), являются достаточно серьёзными, которыми не стоит пренебрегать. Средние риски также требуют планирования и реализации корректирующих действий за разумный период времени; При принятии решений по управлению рисками в "желтой" области используется принцип *ALARA/ALARP* (по начальным буквам фразы *«as low as reasonable applicable / practicable»* – «настолько низкий, насколько это оправдано / практически обосновано»). Данный подход подразумевает максимально

возможное снижение риска, достигаемое за счет реально имеющихся ограниченных ресурсов, т.е принимаются только те меры, которые считаются разумными и доступными с практической точки зрения. Реализация данных мер не должна требовать неоправданно высоких материальных или трудовых затрат.

3. зеленая – область пренебрежимого риска – **риски ранга «Н»** («низкие риски»), являются обычными для Предприятия, для их мониторинга и предотвращения силы и средства распределяются в соответствии с принципом экономности – общая стоимость мероприятий по управлению риском не должна превышать потенциальных убытков, умноженных на вероятность реализации риска. Очень часто, в ходе оценки, такими рисками можно пренебречь.

Таблица 1. Матрица оценки уровня критичности информационных рисков

Вероятность возникновения инцидента ИБ (ARO)	Степень воздействия на активы (ALE)		
	Малый ущерб (1-8)	Средний ущерб (9-17)	Большой ущерб (18-27)
1 (низкая вероятность)	Н	Н	С
2 (средняя вероятность)	Н	С	В
3 (высокая вероятность)	Н	В	В

Для визуализации информации, полученной в процессе оценки рисков, используется **карта рисков**. Она строится на основе сведений из реестра рисков, их количественных характеристик, полученных в процессе оценки рисков.

Карта рисков (см. рисунок 1) представляет собой координатную плоскость с осями «последствия» и «вероятность». На ней отмечаются идентифицированные и измеренные риски. Они могут изображаться просто точками или же кругами, цвет и диаметр которых также несет заданную составителем дополнительную информацию о риске (например, вид риска по классификации или возможный разброс численных характеристик).

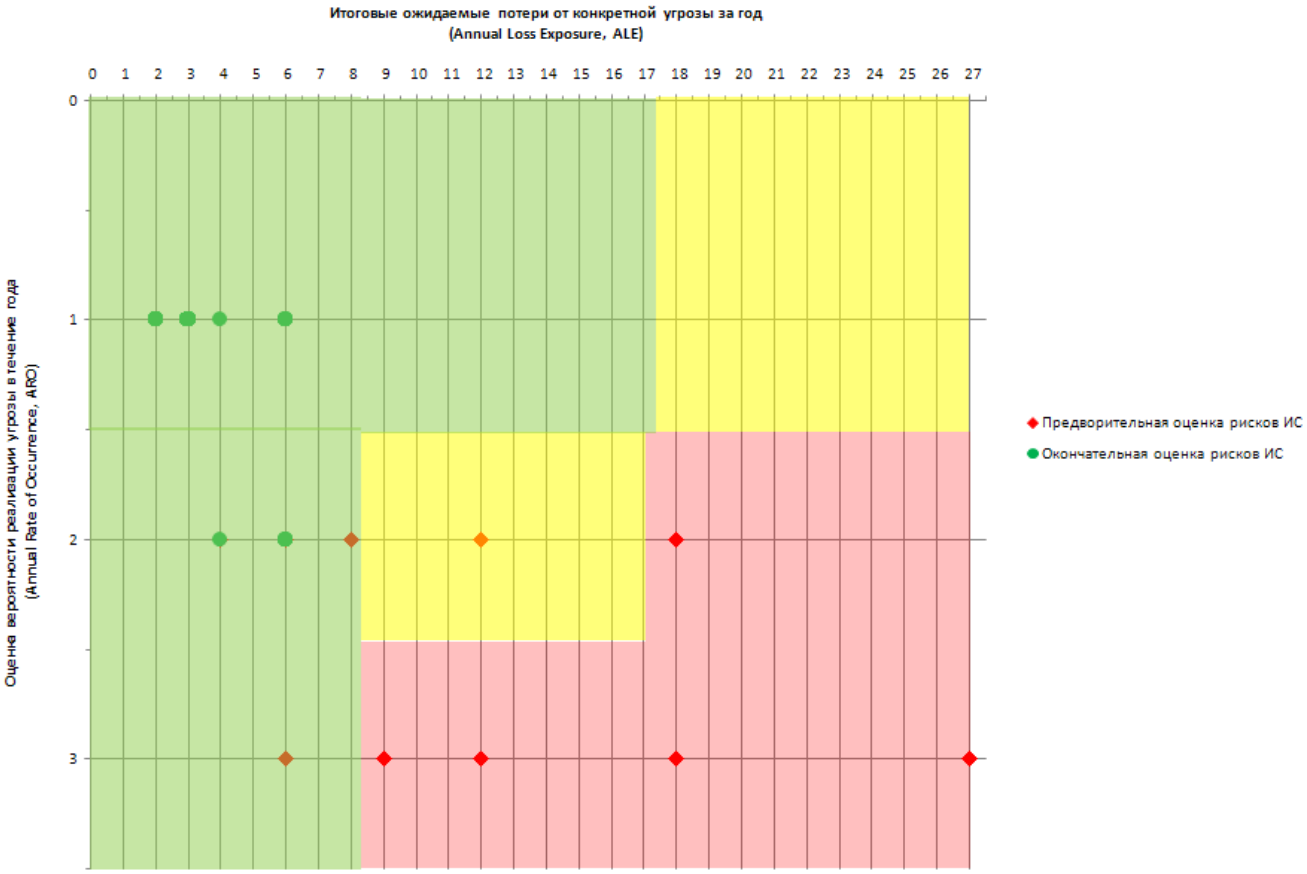

Рисунок 1. Пример построения карты рисков

Рекомендуемые контрмеры

Рекомендуемые контрмеры предназначены для нейтрализации последствий рисков, которые заключаются в достаточной степени уменьшения или устранения идентифицированных рисков, ранг которых оказался недопустимо высоким.

При планировании дополнительных регуляторов безопасности обязательно следует учитывать следующие факторы:

– совместимость с существующим аппаратно-программным обеспечением;

– соответствие действующему законодательству;

– соответствие практике Предприятия, его политике безопасности;

– воздействие на эксплуатационное окружение;

– безопасность и надежность.

При выборе мер защиты системный администратор и ответственный за обеспечение ИБ должны использовать программное обеспечение, серверное оборудования и методы контроля и мониторинга компонентов ИС, сотрудников и пользователей ИС. Выбранные методы и средства обеспечения безопасности должны быть утверждены руководством Организации и отражены в перечне активов ИС.

Рекомендуемые контрмеры являются результатом процесса оценки рисков и, одновременно, входными данными для процесса обработки рисков.

12. Порядок мониторинга

Кроме проводимой ежегодно плановой переоценки рисков, риски ИБ пересматриваются в случаях:

1) внесения существенных изменений в архитектуру и бизнес-процессы ИС ИП;
2) выявления уязвимостей, влияющих на вероятность реализации угроз, или указывающих на наличие неучтенных угроз или рисков;
3) выявление угроз и рисков, ранее не учтенных;
4) инцидентов ИБ, влияющих как на оценку ущерба, так и на оценку вероятности рисков ИБ.

13. Классификация угроз

Классификация угроз применяется только для удобства и упорядоченности применения методики оценки рисков.

Настоящим документом утверждается следующая классификация угроз информационных активов ИС:

- физические угрозы;
- нецелевое использование компьютерного оборудования и сети интернет сотрудниками организации;
- угрозы утечки конфиденциальной информации;
- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа;
- угрозы недоступности ИТ-сервисов и разрушения (утраты) информационных активов;
- угрозы нарушения целостности и несанкционированной модификации данных;
- угрозы антропогенных и природных катастроф;
- угрозы реализации уязвимостей ПО;
- юридические угрозы.

14. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,
b) исполнение настоящей Инструкции
c) за ведение и обработку рисков.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.